
Original Signature of Member

118TH CONGRESS
1ST SESSION

H.R.

To enact certain existing laws relating to domestic security as title 6, United States Code, “Domestic Security”, and to make technical amendments to improve the United States Code.

IN THE HOUSE OF REPRESENTATIVES

— —, 2023

—, — introduced the following bill; which was referred to the Committee on the Judiciary

A BILL

To enact certain existing laws relating to domestic security as title 6, United States Code, “Domestic Security”, and to make technical amendments to improve the United States Code.

1 *Be it enacted by the Senate and House of Representatives of the United*
2 *States of America in Congress assembled,*

1 **SECTION 1. TABLE OF CONTENTS.**

2 The table of contents for this Act is as follows:

- Sec. 1. Table of contents.
- Sec. 2. Purposes; conformity with original intent.
- Sec. 3. Enactment of title 6, United States Code.
- Sec. 4. Conforming amendments.
- Sec. 5. Conforming cross references.
- Sec. 6. Transitional and savings provisions.
- Sec. 7. Repeals.

3 **SEC. 2. PURPOSES; CONFORMITY WITH ORIGINAL INTENT.**

4 (a) PURPOSES.—The purposes of this Act are—

- 5 (1) to enact certain existing laws relating to domestic security as
- 6 title 6, United States Code, “Domestic Security”; and
- 7 (2) to make technical amendments to improve the United States
- 8 Code.

9 (b) CONFORMITY WITH ORIGINAL INTENT.—In the codification of laws
 10 by this Act, the intent is to conform to the understood policy, intent, and
 11 purpose of Congress in the original enactments, with such amendments and
 12 corrections as will remove ambiguities, contradictions, and other imperfec-
 13 tions, in accordance with section 205(c)(1) of House Resolution No. 988,
 14 93d Congress, as enacted into law by Public Law 93–554 (2 U.S.C.
 15 285b(1)).

16 **SEC. 3. ENACTMENT OF TITLE 6, UNITED STATES CODE.**

17 Certain existing laws of the United States relating to domestic security
 18 are enacted as title 6, United States Code, “Domestic Security”, as follows:

19 **TITLE 6—DOMESTIC SECURITY**

Subtitle I—Homeland Security Organization

Chap.	Sec.
101. General	10101
103. Department of Homeland Security	10301
105. Information Analysis	10501
107. Cybersecurity and Infrastructure Security	10701
109. Science and Technology in Support of Homeland Security	10901
111. Border Security	11101
113. National Emergency Management	11301
115. Transportation Security Administration	11501
117. Management	11701
119. Coordination With Other Entities	11901
121. Homeland Security Council	12101
123. Emergency Communications	12301

125.	Countering Weapons of Mass Destruction Office	12501
127.	Homeland Security Grants	12701
129.	Anti-Trafficking Training for Department Personnel	12901
Subtitle II—National Emergency Management		
201.	General	20101
203.	Emergency Management Capabilities	20301
205.	Comprehensive Preparedness System	20501
207.	Prevention of Fraud, Waste, and Abuse	20701
Subtitle III—Port Security and Accountability		
301.	General	30101
303.	Security of United States Seaports	30301
305.	Security of the International Supply Chain	30501
307.	Administration	30701
Subtitle IV—Transportation Security		
401.	General	40101
403.	Transportation Security Planning, Information Sharing, and Enhancements	40301
405.	Public Transportation Security	40501
407.	Surface Transportation Security	40701
409.	Air Transportation Security	40901

1 **Subtitle I—Homeland Security**
2 **Organization**
3 **Chapter 101—General**

Sec.
10101. Definitions.
10102. Construction; relationship to other laws.

4 **§ 10101. Definitions**

5 In this subtitle:

6 (1) AMERICAN HOMELAND; HOMELAND.—Each of the terms “Amer-
7 ican homeland” and “homeland” means the United States.

8 (2) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term “appro-
9 appropriate congressional committee” means a committee of the House of
10 Representatives or the Senate having legislative or oversight jurisdic-
11 tion under the Rules of the House of Representatives or the Senate,
12 respectively, over the matter concerned.

13 (3) ASSETS.—The term “assets” includes contracts, facilities, prop-
14 erty, records, unobligated or unexpended balances of appropriations,
15 and other funds or resources (other than personnel).

1 (4) CRITICAL INFRASTRUCTURE.—The term “critical infrastructure”
2 has the meaning given the term in subsection (e) of the Critical Infra-
3 structures Protection Act of 2001 (42 U.S.C. 5195e(e)).

4 (5) DEPARTMENT.—The term “Department” means the Department
5 of Homeland Security.

6 (6) EMERGENCY RESPONSE PROVIDERS.—The term “emergency re-
7 sponse providers” includes Federal, State, and local governmental and
8 nongovernmental emergency public safety, fire, law enforcement, emer-
9 gency response, emergency medical (including hospital emergency facili-
10 ties), and related personnel, agencies, and authorities.

11 (7) EMP.—The term “EMP” means an electromagnetic pulse
12 caused by a nuclear device or nonnuclear device, including an electro-
13 magnetic pulse caused by an act of terrorism.

14 (8) EXECUTIVE AGENCY.—The term “executive agency” means an
15 executive agency and a military department, as defined, respectively, in
16 sections 105 and 102 of title 5.

17 (9) FUNCTIONS.—The term “functions” includes authorities, powers,
18 rights, privileges, immunities, programs, projects, activities, duties, and
19 responsibilities.

20 (10) GMD.—The term “GMD” means a geomagnetic disturbance
21 caused by a solar storm or another naturally occurring phenomenon.

22 (11) INTELLIGENCE COMPONENT OF THE DEPARTMENT.—The term
23 “intelligence component of the Department” means an element or enti-
24 ty of the Department that collects, gathers, processes, analyzes, pro-
25 duces, or disseminates intelligence information within the scope of the
26 information sharing environment, including homeland security informa-
27 tion, terrorism information, and weapons of mass destruction informa-
28 tion, or national intelligence (as defined under section 3 of the National
29 Security Act of 1947 (50 U.S.C. 3003)), except—

30 (A) the United States Secret Service; and

31 (B) the Coast Guard, when operating under the direct authority
32 of the Secretary of Defense or Secretary of the Navy under section
33 103 of title 14, except that nothing in this paragraph shall affect
34 or diminish the authority and responsibilities of the Commandant
35 of the Coast Guard to command or control the Coast Guard as
36 an armed force or the authority of the Director of National Intel-
37 ligence with respect to the Coast Guard as an element of the intel-
38 ligence community (as defined under section 3 of the National Se-
39 curity Act of 1947 (50 U.S.C. 3003)).

1 (12) KEY RESOURCES.—The term “key resources” means publicly or
2 privately controlled resources essential to the minimal operations of the
3 economy and government.

4 (13) LOCAL GOVERNMENT.—The term “local government” means—

5 (A) a county, municipality, city, town, township, local public au-
6 thority, school district, special district, intrastate district, council
7 of governments (regardless of whether the council of governments
8 is incorporated as a nonprofit corporation under State law), re-
9 gional or interstate government entity, or agency or instrumen-
10 tality of a local government;

11 (B) an Indian tribe or authorized tribal organization, or in Alas-
12 ka a Native village or Alaska Regional Native Corporation; and

13 (C) a rural community, unincorporated town or village, or other
14 public entity.

15 (14) MAJOR DISASTER.—The term “major disaster” has the mean-
16 ing given the term in section 102 of the Robert T. Stafford Disaster
17 Relief and Emergency Assistance Act (42 U.S.C. 5122).

18 (15) PERSONNEL.—The term “personnel” means officers and em-
19 ployees.

20 (16) SECRETARY.—The term “Secretary” means the Secretary of
21 Homeland Security.

22 (17) STATE.—The term “State” means a State, the District of Co-
23 lumbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the
24 Northern Mariana Islands, or a possession of the United States.

25 (18) TERRORISM.—The term “terrorism” means an activity that—

26 (A) involves an act that—

27 (i) is dangerous to human life or potentially destructive of
28 critical infrastructure or key resources; and

29 (ii) is a violation of the criminal laws of the United States
30 or of a State or other subdivision of the United States; and

31 (B) appears to be intended—

32 (i) to intimidate or coerce a civilian population;

33 (ii) to influence the policy of a government by intimidation
34 or coercion; or

35 (iii) to affect the conduct of a government by mass destruc-
36 tion, assassination, or kidnapping.

37 (19) UNITED STATES.—The term “United States” means the States,
38 the District of Columbia, Puerto Rico, the Virgin Islands, Guam,
39 American Samoa, the Northern Mariana Islands, a possession of the
40 United States, and waters in the jurisdiction of the United States.

1 (20) VOLUNTARY PREPAREDNESS STANDARDS.—The term “vol-
2 untary preparedness standards” means a common set of criteria for
3 preparedness, disaster management, emergency management, and busi-
4 ness continuity programs, such as the American National Standards
5 Institute’s National Fire Protection Association Standard on Con-
6 tinuity, Emergency, and Crisis Management (ANSI/NFPA 1600).

7 **§ 10102. Construction; relationship to other laws**

8 (a) CONSTRUCTION; SEVERABILITY.—A provision of this subtitle held to
9 be invalid or unenforceable by its terms, or as applied to a person or cir-
10 cumstance, shall be construed so as to give it the maximum effect permitted
11 by law, unless the holding shall be one of utter invalidity or unenforceability,
12 in which event the provision shall be deemed severable from this subtitle and
13 shall not affect the remainder of the subtitle, or the application of the provi-
14 sion to other persons not similarly situated or to other, dissimilar cir-
15 cumstances.

16 (b) RELATIONSHIP TO OTHER LAWS.—

17 (1) NATIONAL SECURITY RESPONSIBILITIES.—Nothing in this sub-
18 title (or an amendment made by the Homeland Security Act of 2002
19 (Public Law 107–296, 116 Stat. 2135)) shall supersede any authority
20 of the Secretary of Defense, the Director of Central Intelligence, or
21 other agency head, as authorized by law and as directed by the Presi-
22 dent, with regard to the operation, control, or management of national
23 security systems, as defined by section 3552(b)(6) of title 44.

24 (2) ATOMIC ENERGY ACT OF 1954.—Nothing in this subtitle shall su-
25 persede any requirement made by or under the Atomic Energy Act of
26 1954 (42 U.S.C. 2011 et seq.). Restricted data or formerly restricted
27 data shall be handled, protected, classified, downgraded, and declas-
28 sified in conformity with the Atomic Energy Act of 1954 (42 U.S.C.
29 2011 et seq.).

30 (3) STANDARDS AND TECHNOLOGY ACT.—Nothing in this subtitle
31 (or an amendment made by the Homeland Security Act of 2002 (Pub-
32 lic Law 107–296, 116 Stat. 2135)) affects the authority of the Na-
33 tional Institute of Standards and Technology or the Department of
34 Commerce relating to the development and promulgation of standards
35 or guidelines under paragraphs (1) and (2) of section 20(a) of the Na-
36 tional Institute of Standards and Technology Act (15 U.S.C. 278g-
37 3(a)(1), (2)).

38 (4) IMMIGRATION AND NATIONALITY LAW.—Nothing in the definition
39 of “United States” in section 10101 of this title or another provision
40 of this subtitle shall be construed to modify the definition of “United

1 States” for the purposes of the Immigration and Nationality Act (8
2 U.S.C. 1101 et seq.) or any other immigration or nationality law.

3 **Chapter 103—Department of Homeland**
4 **Security**

Subchapter I—Organization

Sec.

- 10301. Establishment; mission; seal.
- 10302. Secretary and other officers.
- 10303. Office of Intelligence and Analysis.
- 10304. Cybersecurity and Infrastructure Security Agency.
- 10305. Directorate of Science and Technology.
- 10306. U.S. Customs and Border Protection.
- 10307. U.S. Immigration and Customs Enforcement.
- 10308. U.S. Citizenship and Immigration Services.
- 10309. Federal Emergency Management Agency.
- 10310. Transportation Security Administration.
- 10311. United States Secret Service.
- 10312. Coast Guard.
- 10313. Office for State and Local Government Coordination.
- 10314. Countering Weapons of Mass Destruction Office.
- 10315. Office of Counternarcotics Enforcement.
- 10316. Office of International Affairs.
- 10317. Office for National Capital Region Coordination.
- 10318. Office of Cargo Security Policy.
- 10319. Transportation Security Oversight Board.
- 10320. Special Assistant to the Secretary.
- 10321. Border Enforcement Security Task Force.
- 10322. Office for Domestic Preparedness.
- 10323. Social media working group.
- 10324. Office of Strategy, Policy, and Plans.
- 10325. Immigration Detention Ombudsman.
- 10326. Counter Threats Advisory Board.
- 10327. Economic security council.

Subchapter II—Functions

- 10341. In general.
- 10342. Trade and customs revenue functions.
- 10343. Military activities.
- 10344. Sensitive Security Information.
- 10345. Daily public report of covered contract awards.

Subchapter III—Acquisitions

- 10351. Personal services.
- 10352. Prohibition on contracts with corporate expatriates.
- 10353. Lead system integrator; financial interests.
- 10354. Requirements to buy certain items related to national security interests.

Subchapter IV—Human Resources Management

- 10361. Establishment of human resources management system.
- 10362. Labor-management relations.
- 10363. Use of counternarcotics enforcement activities in certain employee performance appraisals.
- 10364. Compliance with laws protecting equal employment opportunity and providing whistleblower protections.
- 10365. Use of protective equipment or measures by employees.
- 10366. Homeland Security Rotation Program.
- 10367. Rotational cybersecurity research program.
- 10368. Homeland Security Education Program.
- 10369. Annual employee award program.

Subchapter V—Cybersecurity

- 10381. Workforce assessment and strategy.
- 10382. Homeland Workforce Measurement Initiative.

Subchapter VI—Miscellaneous Provisions

- 10391. Advisory committees.
- 10392. Use of appropriated funds.

- 10393. Reports and consultation addressing use of appropriated funds.
- 10394. Buy America requirements.
- 10395. Horse adoption program.
- 10396. Future Years Homeland Security Program.
- 10397. Federal Law Enforcement Training Centers.
- 10398. Fees.
- 10399. Reports to Committee on Commerce, Science, and Transportation.
- 10400. Annual ammunition and weaponry reports.
- 10401. National identification system not authorized.
- 10402. Functions and authorities of Administrator of General Services not affected.
- 10403. Research and development pilot program.
- 10404. Protection of certain facilities and assets from unmanned aircraft.
- 10405. Homeland security critical domain research and development.
- 10406. Department of Homeland Security Nonrecurring Expenses Fund.
- 10407. Mentor firm-protege firm program.

Subchapter I—Organization

§ 10301. Establishment; mission; seal

(a) ESTABLISHMENT.—The Department of Homeland Security is an executive department of the United States within the meaning of title 5.

(b) MISSION.—

(1) IN GENERAL.—The primary mission of the Department is to—

(A) prevent terrorist attacks within the United States;

(B) reduce the vulnerability of the United States to terrorism;

(C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States;

(D) carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning;

(E) ensure that the functions of the agencies and subdivisions in the Department that are not related directly to securing the homeland are not diminished or neglected except by a specific explicit Act of Congress;

(F) ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland;

(G) ensure that the civil rights and civil liberties of persons are not diminished by efforts, activities, and programs aimed at securing the homeland; and

(H) monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever the connections, and otherwise contribute to efforts to interdict illegal drug trafficking.

(2) RESPONSIBILITY FOR INVESTIGATING AND PROSECUTING TERRORISM.—Except as specifically provided by law with respect to entities transferred to the Department under this subtitle, primary responsibility for investigating and prosecuting acts of terrorism shall be vested

1 not in the Department, but rather in Federal, State, and local law en-
2 forcement agencies with jurisdiction over the acts in question.

3 (c) SEAL.—The Department has a seal. The design of the seal is subject
4 to the approval of the President.

5 **§ 10302. Secretary and other officers**

6 (a) SECRETARY.—The Secretary of Homeland Security is the head of the
7 Department. The Secretary is appointed by the President, by and with the
8 advice and consent of the Senate.

9 (b) DEPUTY SECRETARY, UNDER SECRETARIES, ADMINISTRATOR, DI-
10 RECTORS, ASSISTANT SECRETARIES, AND GENERAL COUNSEL.—

11 (1) IN GENERAL.—Except as provided in paragraph (2), the Depart-
12 ment has the following officers, appointed by the President, by and
13 with the advice and consent of the Senate:

14 (A) Deputy Secretary of Homeland Security, who shall be the
15 Secretary's first assistant for purposes of subchapter III of chap-
16 ter 33 of title 5.

17 (B) Under Secretary for Science and Technology.

18 (C) Commissioner of U.S. Customs and Border Protection.

19 (D) Administrator of the Federal Emergency Management
20 Agency.

21 (E) Director of U.S. Citizenship and Immigration Services.

22 (F) Under Secretary for Management, who shall be 1st assist-
23 ant to the Deputy Secretary of Homeland Security for purposes
24 of chapter 33 of title 5.

25 (G) Director of U.S. Immigration and Customs Enforcement.

26 (H) Director of the Cybersecurity and Infrastructure Security
27 Agency.

28 (I) Not more than 12 Assistant Secretaries.

29 (J) General Counsel, who is the chief legal officer of the Depart-
30 ment.

31 (K) Under Secretary for Strategy, Policy, and Plans.

32 (2) ASSISTANT SECRETARIES.—If any of the Assistant Secretaries
33 referred to under paragraph (1)(I) is designated to be the Assistant
34 Secretary for Legislative Affairs or the Assistant Secretary for Public
35 Affairs, that Assistant Secretary shall be appointed by the President
36 without the advice and consent of the Senate.

37 (c) INSPECTOR GENERAL.—There is in the Department the Office of In-
38 spector General and an Inspector General at the head of the office, as pro-
39 vided in chapter 4 of title 5.

40 (d) COMMANDANT OF THE COAST GUARD.—To assist the Secretary in
41 the performance of the Secretary's functions, there is a Commandant of the

1 Coast Guard, who shall be appointed as provided in section 302 of title 14,
2 and who shall report directly to the Secretary. In addition to duties provided
3 in this subtitle and as assigned to the Commandant by the Secretary, the
4 duties of the Commandant shall include those required by section 102 of
5 title 14.

6 (e) CHIEF FINANCIAL OFFICER.—There is in the Department a Chief Fi-
7 nancial Officer, as provided in chapter 9 of title 31.

8 (f) CHIEF HUMAN CAPITAL OFFICER.—There is in the Department a
9 Chief Human Capital Officer.

10 (g) OTHER OFFICERS.—To assist the Secretary in the performance of the
11 Secretary's functions, there are the following officers, appointed by the
12 President:

13 (1) Director of the Secret Service.

14 (2) Chief Information Officer.

15 (3) Officer for Civil Rights and Civil Liberties.

16 (4) Assistant Secretary for the Countering Weapons of Mass De-
17 struction Office.

18 (5) Any Director of a Joint Task Force under section 11708 of this
19 title.

20 (h) ABSENCE, DISABILITY, OR VACANCY OF SECRETARY OR DEPUTY
21 SECRETARY AND FURTHER ORDER OF SUCCESSION.—

22 (1) ABSENCE, DISABILITY, OR VACANCY OF SECRETARY OR DEPUTY
23 SECRETARY.—

24 (A) UNDER SECRETARY FOR MANAGEMENT TO SERVE AS ACT-
25 ING SECRETARY.—Notwithstanding chapter 33 of title 5, the
26 Under Secretary for Management shall serve as the Acting Sec-
27 retary if by reason of absence, disability, or vacancy in office, nei-
28 ther the Secretary nor the Deputy Secretary is available to exer-
29 cise the duties of the Secretary.

30 (B) NOTIFICATION OF VACANCIES.—The Secretary shall notify
31 the Committee on Homeland Security and Governmental Affairs
32 of the Senate and the Committee on Homeland Security of the
33 House of Representatives of any vacancies that require notification
34 under sections 3345 through 3349d of title 5.

35 (2) FURTHER ORDER OF SUCCESSION.—Notwithstanding chapter 33
36 of title 5, the Secretary may designate other officers of the Department
37 in further order of succession to serve as Acting Secretary.

38 **§ 10303. Office of Intelligence and Analysis**

39 (a) IN GENERAL.—There is in the Department the Office of Intelligence
40 and Analysis. The Under Secretary for Intelligence and Analysis is the head
41 of the Office. The Under Secretary is appointed by the President, by and

1 with the advice and consent of the Senate, and serves as the Chief Intel-
2 ligence Officer of the Department.

3 (b) HOMELAND SECURITY INTELLIGENCE PROGRAM.—The Homeland Se-
4 curity Intelligence Program in the Department coordinates the intelligence
5 activities of the Office of Intelligence and Analysis that serve predominantly
6 department missions.

7 **§ 10304. Cybersecurity and Infrastructure Security Agency**

8 (a) IN GENERAL.—There is in the Department the Cybersecurity and In-
9 frastructure Security Agency (in this section referred to as the “Agency”).
10 Any reference to the National Protection and Programs Directorate of the
11 Department in a law, regulation, map, document, record, or other paper of
12 the United States shall be deemed to be a reference to the Agency.

13 (b) DIRECTOR.—

14 (1) IN GENERAL.—The Director of the Cybersecurity and Infrastruc-
15 ture Security Agency (in this section referred to as the “Director”) is
16 the head of the Agency. The Director reports to the Secretary.

17 (2) QUALIFICATIONS.—

18 (A) IN GENERAL.—The Director shall be appointed from among
19 individuals who have—

20 (i) extensive knowledge in at least 2 of the areas specified
21 in subparagraph (B); and

22 (ii) not fewer than 5 years of demonstrated experience in
23 efforts to foster coordination and collaboration between the
24 Federal Government, the private sector, and other entities on
25 issues related to cybersecurity, infrastructure security, or se-
26 curity risk management.

27 (B) SPECIFIED AREAS.—The areas specified in this subpara-
28 graph are the following:

29 (i) Cybersecurity.

30 (ii) Infrastructure security.

31 (iii) Security risk management.

32 (3) REFERENCE.—Any reference to an Under Secretary responsible
33 for overseeing critical infrastructure protection, cybersecurity, and any
34 other related program of the Department as described in section
35 103(a)(1)(H) of the Homeland Security Act of 2002 (Public Law 107–
36 296, 116 Stat. 2144), as amended by section 2(f)(5)(A) and (B) of the
37 Presidential Appointment Efficiency and Streamlining Act of 2011
38 (Public Law 112–166, 126 Stat. 1285) and section 2(g)(1) of the Cy-
39 bersecurity and Infrastructure Security Agency Act of 2018 (Public
40 Law 115–278, 132 Stat. 4176), as in effect on November 15, 2018,

1 in a law, regulation, map, document, record, or other paper of the
2 United States shall be deemed to be a reference to the Director.

3 (e) DEPUTY DIRECTOR.—The Agency has a Deputy Director of Cyberse-
4 curity and Infrastructure Security who shall—

5 (1) assist the Director in the management of the Agency; and

6 (2) report to the Director.

7 (d) PRIVACY OFFICER.—The Agency has a Privacy Officer with primary
8 responsibility for privacy policy and compliance for the Agency.

9 (e) CYBERSECURITY DIVISION.—

10 (1) IN GENERAL.—There is in the Agency the Cybersecurity Divi-
11 sion.

12 (2) EXECUTIVE ASSISTANT DIRECTOR.—The Executive Assistant Di-
13 rector for Cybersecurity is the head of the Cybersecurity Division. The
14 Executive Assistant Director for Cybersecurity shall—

15 (A) be at the level of Assistant Director in the Department;

16 (B) be appointed by the President without the advice and con-
17 sent of the Senate; and

18 (C) report to the Director.

19 (3) REFERENCE.—Any reference to the Assistant Secretary for Cy-
20 bersecurity and Communications or Assistant Secretary for Cybersecu-
21 rity in a law, regulation, map, document, record, or other paper of the
22 United States shall be deemed to be a reference to the Executive As-
23 sistant Director for Cybersecurity.

24 (f) INFRASTRUCTURE SECURITY DIVISION.—

25 (1) IN GENERAL.—There is in the Agency the Infrastructure Secu-
26 rity Division.

27 (2) EXECUTIVE ASSISTANT DIRECTOR.—The Executive Assistant Di-
28 rector for Infrastructure Security is the head of the Infrastructure Se-
29 curity Division. The Executive Assistant Director for Infrastructure Se-
30 curity shall—

31 (A) be at the level of Assistant Director in the Department;

32 (B) be appointed by the President without the advice and con-
33 sent of the Senate; and

34 (C) report to the Director.

35 (3) REFERENCE.—Any reference to the Assistant Secretary for In-
36 frastructure Protection or Assistant Secretary for Infrastructure Secu-
37 rity in a law, regulation, map, document, record, or other paper of the
38 United States shall be deemed to be a reference to the Executive As-
39 sistant Director for Infrastructure Security.

40 (g) EMERGENCY COMMUNICATIONS DIVISION.—

1 (1) IN GENERAL.—There is in the Agency the Emergency Commu-
2 nications Division.

3 (2) EXECUTIVE ASSISTANT DIRECTOR.—

4 (A) IN GENERAL.—The Executive Assistant Director for Emer-
5 gency Communications (in this subsection referred to as the “Ex-
6 ecutive Assistant Director”) is the head of the Emergency Com-
7 munications Division. The Executive Assistant Director shall re-
8 port directly to the Director. All decisions of the Executive Assist-
9 ant Director that entail the exercise of significant authority shall
10 be subject to the approval of the Director.

11 (B) REFERENCE TO ASSISTANT DIRECTOR.—Any reference to
12 the Assistant Director for Emergency Communications in a law,
13 regulation, map, document, record, or other paper of the United
14 States shall be deemed to be a reference to the Executive Assist-
15 ant Director for Emergency Communications.

16 (h) NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION
17 CENTER.—There is in the Agency the National Cybersecurity and Commu-
18 nications Integration Center to carry out certain responsibilities of the Di-
19 rector. The head of the National Cybersecurity and Communications Inte-
20 gration Center shall report to the Executive Assistant Director for Cyberse-
21 curity.

22 (i) CHEMICAL FACILITY ANTI-TERRORISM STANDARDS PROGRAM.—
23 There is in the Agency the Chemical Facility Anti-Terrorism Standards
24 Program.

25 (j) JOINT CYBER PLANNING OFFICE.—

26 (1) DEFINITION OF CYBER DEFENSE OPERATION.—In this sub-
27 section, the term “cyber defense operation” means defensive activities
28 performed for a cybersecurity purpose.

29 (2) IN GENERAL.—There is in the Agency an office for joint cyber
30 planning (in this subsection referred to as the “Office”) to develop, for
31 public- and private-sector entities, plans for cyber defense operations,
32 including the development of a set of coordinated actions to protect, de-
33 tect, respond to, and recover from cybersecurity risks or incidents or
34 limit, mitigate, or defend against coordinated, malicious cyber oper-
35 ations that pose a potential risk to critical infrastructure or national
36 interests.

37 (3) HEAD OF OFFICE.—A senior official of the Agency selected by
38 the Director is the head of the Office.

39 (4) COMPOSITION.—The Office shall be composed of—

40 (A) a central planning staff; and

1 (B) appropriate representatives of Federal departments and
2 agencies, including—

- 3 (i) the Department;
- 4 (ii) United States Cyber Command;
- 5 (iii) the National Security Agency;
- 6 (iv) the Federal Bureau of Investigation;
- 7 (v) the Department of Justice; and
- 8 (vi) the Office of the Director of National Intelligence.

9 (5) PLANNING AND EXECUTION.—In leading the development of
10 plans for cyber defense operations pursuant to paragraph (2), the head
11 of the Office shall—

12 (A) coordinate with relevant Federal departments and agencies
13 to establish processes and procedures necessary to develop and
14 maintain ongoing coordinated plans for cyber defense operations;

15 (B) leverage cyber capabilities and authorities of participating
16 Federal departments and agencies, as appropriate, in furtherance
17 of plans for cyber defense operations;

18 (C) ensure that plans for cyber defense operations are, to the
19 greatest extent practicable, developed in collaboration with rel-
20 evant private-sector entities, particularly in areas in which the en-
21 tities have comparative advantages in limiting, mitigating, or de-
22 fending against a cybersecurity risk or incident or coordinated,
23 malicious cyber operation;

24 (D) ensure that plans for cyber defense operations, as appro-
25 priate, are responsive to potential adversary activity conducted in
26 response to United States offensive cyber operations;

27 (E) facilitate the exercise of plans for cyber defense operations,
28 including by developing and modeling scenarios based on an un-
29 derstanding of adversary threats to, vulnerability of, and potential
30 consequences of disruption or compromise of critical infrastruc-
31 ture;

32 (F) coordinate with and, as necessary, support relevant Federal
33 departments and agencies in the establishment of procedures, de-
34 velopment of additional plans, including for offensive and intel-
35 ligence activities in support of cyber defense operations, and cre-
36 ation of agreements necessary for the rapid execution of plans for
37 cyber defense operations when a cybersecurity risk or incident or
38 malicious cyber operation has been identified; and

39 (G) support public- and private-sector entities, as appropriate,
40 in the execution of plans developed pursuant to this subsection.

1 (6) CONSULTATION.—In carrying out its responsibilities described in
2 paragraph (5), the Office shall regularly consult with appropriate rep-
3 resentatives of non-Federal entities, such as—

4 (A) State, local, federally recognized Tribal, and territorial gov-
5 ernments;

6 (B) Information Sharing and Analysis Organizations, including
7 information sharing and analysis centers;

8 (C) owners and operators of critical information systems;

9 (D) private entities; and

10 (E) other appropriate representatives or entities, as determined
11 by the Secretary.

12 (7) INTERAGENCY AGREEMENTS.—The Secretary and the head of a
13 Federal department or agency referred to in paragraph (4) may enter
14 into agreements for the purpose of detailing personnel on a reimburs-
15 able or non-reimbursable basis.

16 (k) CYBERSECURITY ADVISORY COMMITTEE

17 (1) IN GENERAL.—There is in the Agency the Cybersecurity Advi-
18 sory Committee, established by the Secretary.

19 (2) MEMBERSHIP.—

20 (A) APPOINTMENT.—The Director shall appoint the members of
21 the Cybersecurity Advisory Committee.

22 (B) COMPOSITION.—The Cybersecurity Advisory Committee
23 shall consist of not more than 35 individuals and shall satisfy the
24 following criteria:

25 (i) Consist of subject matter experts.

26 (ii) Be geographically balanced.

27 (iii) Include representatives of State, local, and Tribal gov-
28 ernments and of a broad range of industries, which may in-
29 clude the following:

30 (I) Defense.

31 (II) Education.

32 (III) Financial services and insurance.

33 (IV) Healthcare.

34 (V) Manufacturing.

35 (VI) Media and entertainment.

36 (VII) Chemicals.

37 (VIII) Retail.

38 (IX) Transportation.

39 (X) Energy.

40 (XI) Information technology.

41 (XII) Communications.

1 (XIII) Other relevant fields identified by the Director.

2 (C) LIMITATION ON REPRESENTATION.—Not fewer than 1
3 member nor more than 3 members may represent a category
4 under subparagraph (B)(iii).

5 (D) PUBLICATION OF MEMBERSHIP LIST.—The Cybersecurity
6 Advisory Committee shall publish its membership list on a publicly
7 available website not less than once per fiscal year and shall up-
8 date the membership list as changes occur.

9 (E) TERM OF OFFICE.—

10 (i) IN GENERAL.—The term of each member of the Cyber-
11 security Advisory Committee shall be 2 years, except that a
12 member may continue to serve until a successor is appointed.

13 (ii) REAPPOINTMENT.—A member of the Cybersecurity Ad-
14 visory Committee may be reappointed for an unlimited num-
15 ber of terms.

16 (iii) REMOVAL.—The Director may review the participation
17 of a member of the Cybersecurity Advisory Committee and at
18 any time remove the member at the discretion of the Direc-
19 tor.

20 (F) PROHIBITION ON COMPENSATION.—The members of the Cy-
21 bersecurity Advisory Committee may not receive pay or benefits
22 from the United States Government by reason of their service on
23 the Cybersecurity Advisory Committee.

24 (G) CHAIRPERSON.—The Cybersecurity Advisory Committee
25 shall select from among its members—

26 (i) a member to serve as chairperson of the Cybersecurity
27 Advisory Committee; and

28 (ii) a member to serve as chairperson of each subcommittee
29 of the Cybersecurity Advisory Committee established under
30 paragraph (4).

31 (H) MEETINGS.—

32 (i) IN GENERAL.—The Director shall require the Cyberse-
33 curity Advisory Committee to meet not less frequently than
34 semiannually, and may convene additional meetings as nec-
35 essary.

36 (ii) PUBLIC MEETINGS.—At least one of the meetings re-
37 ferred to in clause (i) shall be open to the public.

38 (iii) ATTENDANCE.—The Cybersecurity Advisory Com-
39 mittee shall maintain a record of the individuals present at
40 each meeting.

41 (I) ACCESS TO CLASSIFIED INFORMATION.—

1 (i) IN GENERAL.—Not later than 60 days after the date on
2 which a member is first appointed to the Cybersecurity Advi-
3 sory Committee and before the member is granted access to
4 any classified information, the Director shall determine, for
5 the purposes of the Cybersecurity Advisory Committee, if the
6 member should be restricted from reviewing, discussing, or
7 possessing classified information.

8 (ii) MANAGING ACCESS.—Access to classified materials
9 shall be managed in accordance with Executive Order No.
10 13526 of December 29, 2009 (50 U.S.C. 3161 note), or any
11 subsequent corresponding Executive Order.

12 (iii) PROTECTING INFORMATION.—A member of the Cyber-
13 security Advisory Committee shall protect all classified infor-
14 mation in accordance with the applicable requirements for the
15 particular level of classification of the information.

16 (iv) RULE OF CONSTRUCTION.—Nothing in this subpara-
17 graph shall be construed to affect the security clearance of a
18 member of the Cybersecurity Advisory Committee or the au-
19 thority of a Federal agency to provide a member of the Cy-
20 bersecurity Advisory Committee access to classified informa-
21 tion.

22 (3) DUTIES.—

23 (A) IN GENERAL.—The Cybersecurity Advisory Committee shall
24 advise, consult with, report to, and make recommendations to the
25 Director, as appropriate, on the development, refinement, and im-
26 plementation of policies, programs, planning, and training per-
27 taining to the cybersecurity mission of the Agency.

28 (B) RECOMMENDATIONS.—

29 (i) IN GENERAL.—The Cybersecurity Advisory Committee
30 shall develop, at the request of the Director, recommendations
31 for improvements to advance the cybersecurity mission of the
32 Agency and strengthen the cybersecurity of the United
33 States.

34 (ii) RECOMMENDATIONS OF SUBCOMMITTEES.—Rec-
35 ommendations agreed on by subcommittees established under
36 paragraph (4) for any year shall be approved by the Cyberse-
37 curity Advisory Committee before the Cybersecurity Advisory
38 Committee submits to the Director the annual report under
39 subparagraph (D) for that year.

40 (C) PERIODIC REPORTS.—The Cybersecurity Advisory Com-
41 mittee shall periodically submit to the Director—

- 1 (i) reports on matters identified by the Director; and
2 (ii) reports on other matters identified by a majority of the
3 members of the Cybersecurity Advisory Committee.

4 (D) ANNUAL REPORT.—

- 5 (i) IN GENERAL.—The Cybersecurity Advisory Committee
6 shall submit to the Director an annual report providing infor-
7 mation on the activities, findings, and recommendations of
8 the Cybersecurity Advisory Committee, including its sub-
9 committees, for the preceding year.

- 10 (ii) PUBLICATION.—Not later than 180 days after the date
11 on which the Director receives an annual report for a year
12 under clause (i), the Director shall publish a public version
13 of the report describing the activities of the Cybersecurity Ad-
14 visory Committee and such related matters as would be in-
15 formative to the public during that year, consistent with sec-
16 tion 552(b) of title 5.

- 17 (E) FEEDBACK.—Not later than 90 days after receiving any
18 recommendation submitted by the Cybersecurity Advisory Com-
19 mittee under subparagraph (B), (C), or (D), the Director shall re-
20 spond in writing to the Cybersecurity Advisory Committee with
21 feedback on the recommendation. The response shall include—

- 22 (i) with respect to a recommendation with which the Direc-
23 tor concurs, an action plan to implement the recommenda-
24 tion; and

- 25 (ii) with respect to a recommendation with which the Di-
26 rector does not concur, a justification for why the Director
27 does not plan to implement the recommendation.

- 28 (F) CONGRESSIONAL NOTIFICATION.—Not less frequently than
29 once per year after January 1, 2021, the Director shall provide
30 to the Committee on Homeland Security and Governmental Affairs
31 and the Committee on Appropriations of the Senate and the Com-
32 mittee on Homeland Security, the Committee on Energy and Com-
33 merce, and the Committee on Appropriations of the House of Rep-
34 resentatives a briefing on feedback from the Cybersecurity Advi-
35 sory Committee.

- 36 (G) GOVERNANCE RULES.—The Director shall establish rules
37 for the structure and governance of the Cybersecurity Advisory
38 Committee and all subcommittees established under paragraph
39 (4).

- 40 (4) SUBCOMMITTEES.—

1 (A) IN GENERAL.—The Director shall establish subcommittees
2 in the Cybersecurity Advisory Committee to address cybersecurity
3 issues, which may include the following:

- 4 (i) Information exchange.
- 5 (ii) Critical infrastructure.
- 6 (iii) Risk management.
- 7 (iv) Public and private partnerships.

8 (B) MEETINGS AND REPORTING.—Each subcommittee shall
9 meet not less frequently than semiannually, and submit to the Cy-
10 bersecurity Advisory Committee for inclusion in the annual report
11 required under paragraph (3)(D) information, including activities,
12 findings, and recommendations, regarding subject matter consid-
13 ered by the subcommittee.

14 (C) QUALIFICATION OF MEMBERS.—The chairperson of the Cy-
15 bersecurity Advisory Committee shall appoint members to sub-
16 committees and shall ensure that each member appointed to a sub-
17 committee has subject matter expertise relevant to the subject
18 matter of the subcommittee.

19 (l) CYBERSECURITY EDUCATION AND TRAINING PROGRAMS

20 (1) IN GENERAL.—There is in the Agency the Cybersecurity Edu-
21 cation and Training Assistance Program (in this subsection referred to
22 as “CETAP”).

23 (2) PURPOSE.—The purpose of CETAP shall be to support the ef-
24 fort of the Agency in building and strengthening a national cybersecu-
25 rity workforce pipeline capacity through enabling elementary and sec-
26 ondary cybersecurity education, including by—

- 27 (A) providing foundational cybersecurity awareness and literacy;
- 28 (B) encouraging cybersecurity career exploration; and
- 29 (C) supporting the teaching of cybersecurity skills at the ele-
30 mentary and secondary education levels.

31 (3) DUTIES.—In carrying out CETAP, the Director shall—

- 32 (A) ensure that the program—
 - 33 (i) creates and disseminates cybersecurity-focused curricula
34 and career awareness materials appropriate for use at the ele-
35 mentary and secondary education levels;
 - 36 (ii) conducts professional development sessions for teachers;
 - 37 (iii) develops resources for the teaching of cybersecurity-fo-
38 cused curricula described in clause (i);
 - 39 (iv) provides direct student engagement opportunities
40 through camps and other programming;

- 1 (v) engages with State educational agencies and local edu-
2 cational agencies to promote awareness of the program and
3 ensure that offerings align with State and local curricula;
- 4 (vi) integrates with existing post-secondary education and
5 workforce development programs at the Department;
- 6 (vii) promotes and supports national standards for elemen-
7 tary and secondary cyber education;
- 8 (viii) partners with cybersecurity and education stakeholder
9 groups to expand outreach; and
- 10 (ix) engages in any other activity the Director determines
11 necessary to meet the purpose described in paragraph (2);
12 and

13 (B) enable the deployment of CETAP nationwide, with special
14 consideration for underserved populations or communities.

15 (4) BRIEFINGS.—

16 (A) IN GENERAL.—Not later than 1 year after the establish-
17 ment of CETAP, and annually thereafter, the Secretary shall brief
18 the Committee on Homeland Security and Governmental Affairs
19 of the Senate and the Committee on Homeland Security of the
20 House of Representatives on the program.

21 (B) CONTENTS.—Each briefing conducted under subparagraph
22 (A) shall include—

- 23 (i) estimated figures on the number of students reached
24 and teachers engaged;
- 25 (ii) information on outreach and engagement efforts, in-
26 cluding the activities described in paragraph (3)(A)(v);
- 27 (iii) information on any grants or cooperative agreements
28 made pursuant to paragraph (6), including how any of the
29 grants or cooperative agreements are being used to enhance
30 cybersecurity education for underserved populations or com-
31 munities;
- 32 (iv) information on new curricula offerings and teacher
33 training platforms; and
- 34 (v) information on coordination with post-secondary edu-
35 cation and workforce development programs at the Depart-
36 ment.

37 (5) MISSION PROMOTION.—The Director may use appropriated
38 amounts to purchase promotional and recognition items and marketing
39 and advertising services to publicize and promote the mission and serv-
40 ices of the Agency, support the activities of the Agency, and recruit and
41 retain Agency personnel.

1 (6) GRANTS AND COOPERATIVE AGREEMENTS.—The Director may
2 award financial assistance in the form of grants or cooperative agree-
3 ments to States, local governments, institutions of higher education (as
4 the term is defined in section 101 of the Higher Education Act of 1965
5 (20 U.S.C. 1001)), nonprofit organizations, and other non-Federal en-
6 tities as determined appropriate by the Director for the purpose of
7 funding cybersecurity and infrastructure security education and train-
8 ing programs and initiatives to—

- 9 (A) carry out the purposes of CETAP; and
10 (B) enhance CETAP to address the national shortfall of cyber-
11 security professionals.

12 (m) INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING INITIA-
13 TIVE

14 (1) IN GENERAL.—

15 (A) ESTABLISHMENT.—There is in the Agency the Industrial
16 Control Systems Cybersecurity Training Initiative (in this sub-
17 section referred to as the “Initiative”).

18 (B) PURPOSE.—The purpose of the Initiative is to develop and
19 strengthen the skills of the cybersecurity workforce related to se-
20 curing industrial control systems.

21 (2) REQUIREMENTS.—In carrying out the Initiative, the Director
22 shall—

23 (A) ensure the Initiative includes—

24 (i) virtual and in-person trainings and courses provided at
25 no cost to participants;

26 (ii) trainings and courses available at different skill levels,
27 including introductory level courses;

28 (iii) trainings and courses that cover cyber defense strate-
29 gies for industrial control systems, including an under-
30 standing of the unique cyber threats facing industrial control
31 systems and the mitigation of security vulnerabilities in in-
32 dustrial controlssystems technology; and

33 (iv) appropriate consideration regarding the availability of
34 trainings and courses in different regions of the United
35 States;

36 (B) engage in—

37 (i) collaboration with the national laboratories of the De-
38 partment of Energy in accordance with section 1908 of this
39 title;

40 (ii) consultation with Sector Risk Management Agencies;
41 and

1 (iii) as appropriate, consultation with private sector entities
2 with relevant expertise, such as vendors of industrial control
3 systems technologies; and

4 (C) consult, to the maximum extent practicable, with commer-
5 cial training providers and academia to minimize the potential for
6 duplication of other training opportunities.

7 (3) REPORTS.—Not later than December 23, 2023, and annually
8 thereafter, the Secretary shall submit to the Committee on Homeland
9 Security of the House of Representatives and the Committee on Home-
10 land Security and Governmental Affairs of the Senate a report on the
11 Initiative. Each report shall contain the following:

12 (A) A description of the courses provided under the Initiative.

13 (B) A description of outreach efforts to raise awareness of the
14 availability of the courses.

15 (C) The number of participants in each course.

16 (D) Voluntarily provided information on the demographics of
17 participants in the courses, including by sex, race, and place of
18 residence.

19 (E) Information on the participation in the courses of workers
20 from each critical infrastructure sector.

21 (F) Plans for expanding access to industrial control systems
22 education and training, including expanding access to women and
23 underrepresented populations, and expanding access to different
24 regions of the United States.

25 (G) Recommendations regarding how to strengthen the state of
26 industrial control systems cybersecurity education and training.

27 **§ 10305. Directorate of Science and Technology**

28 There is in the Department the Directorate of Science and Technology.
29 The Under Secretary for Science and Technology is the head of the Direc-
30 torate.

31 **§ 10306. U.S. Customs and Border Protection**

32 (a) DEFINITIONS.—In this section, the terms “commercial operations”,
33 “customs and trade laws of the United States”, “trade enforcement”, and
34 “trade facilitation” have the meanings given the terms in section 2 of the
35 Trade Facilitation and Trade Enforcement Act of 2015 (19 U.S.C. 4301).

36 (b) IN GENERAL.—There is in the Department an agency known as U.S.
37 Customs and Border Protection.

38 (c) COMMISSIONER.—

39 (1) HEAD OF U.S. CUSTOMS AND BORDER PROTECTION.—The Com-
40 missioner of U.S. Customs and Border Protection (in this section re-

1 ferred to as the “Commissioner”) is the head of U.S. Customs and
2 Border Protection.

3 (2) COMMITTEE REFERRAL OF NOMINATION.—As an exercise of the
4 rulemaking power of the Senate, a nomination for the Commissioner
5 submitted to the Senate for confirmation and referred to a committee
6 shall be referred to the Committee on Finance.

7 (d) DEPUTY COMMISSIONER.—U.S. Customs and Border Protection has
8 a Deputy Commissioner. The Deputy Commissioner shall assist the Com-
9 missioner in the management of U.S. Customs and Border Protection.

10 (e) U.S. BORDER PATROL.—

11 (1) IN GENERAL.—There is in U.S. Customs and Border Protection
12 the U.S. Border Patrol.

13 (2) CHIEF.—The Chief of the U.S. Border Patrol is the head of the
14 U.S. Border Patrol. The Chief of the U.S. Border Patrol shall report
15 to the Commissioner.

16 (3) DUTIES.—The U.S. Border Patrol shall—

17 (A) serve as the law enforcement officer of U.S. Customs and
18 Border Protection with primary responsibility for interdicting indi-
19 viduals attempting to illegally enter or exit the United States or
20 goods being illegally imported into or exported from the United
21 States at a place other than a designated port of entry;

22 (B) deter and prevent illegal entry of terrorists, terrorist weap-
23 ons, persons, and contraband; and

24 (C) carry out other duties and powers prescribed by the Com-
25 missioner.

26 (f) OFFICE OF AIR AND MARINE OPERATIONS.—

27 (1) IN GENERAL.—There is in U.S. Customs and Border Protection
28 an Office of Air and Marine Operations.

29 (2) ASSISTANT COMMISSIONER.—An Assistant Commissioner is the
30 head of the Office of Air and Marine Operations. The Assistant Com-
31 missioner shall report to the Commissioner.

32 (3) DUTIES.—The Office of Air and Marine Operations shall—

33 (A) serve as the law enforcement office in U.S. Customs and
34 Border Protection with primary responsibility to detect, interdict,
35 and prevent acts of terrorism and the unlawful movement of peo-
36 ple, illicit drugs, and other contraband across the borders of the
37 United States in the air and maritime environment;

38 (B) conduct joint aviation and marine operations with U.S. Im-
39 migration and Customs Enforcement;

40 (C) conduct aviation and marine operations with international,
41 Federal, State, and local law enforcement agencies, as appropriate;

- 1 (D) administer the Air and Marine Operations Center; and
- 2 (E) carry out other duties and powers the Commissioner pre-
- 3 scribes.

4 (4) AIR AND MARINE OPERATIONS CENTER.—

5 (A) IN GENERAL.—There is in the Office of Air and Marine Op-

6 erations an Air and Marine Operations Center.

7 (B) EXECUTIVE DIRECTOR.—The Executive Director is the

8 head of the Air and Marine Operations Center. The Executive Di-

9 rector shall report to the Assistant Commissioner of the Office of

10 Air and Marine Operations.

11 (C) DUTIES.—The Air and Marine Operations Center shall—

- 12 (i) manage the air and maritime domain awareness of the
- 13 Department;
- 14 (ii) monitor and coordinate the airspace for Unmanned
- 15 Aerial Systems operations of the Office of Air and Marine
- 16 Operations;
- 17 (iii) detect, identify, and coordinate a response to threats
- 18 to national security in the air domain;
- 19 (iv) provide aviation and marine support to other Federal,
- 20 State, tribal, and local agencies; and
- 21 (v) carry out other duties and powers prescribed by the As-
- 22 sistant Commissioner.

23 (g) OFFICE OF FIELD OPERATIONS.—

24 (1) IN GENERAL.—There is in U.S. Customs and Border Protection

25 an Office of Field Operations.

26 (2) EXECUTIVE ASSISTANT COMMISSIONER.—An Executive Assistant

27 Commissioner is the head of the Office of Field Operations. The Execu-

28 tive Assistant Commissioner shall report to the Commissioner.

29 (3) DUTIES.—The Office of Field Operations shall coordinate the en-

30 forcement activities of U.S. Customs and Border Protection at United

31 States air, land, and sea ports of entry to—

- 32 (A) deter and prevent terrorists and terrorist weapons from en-
- 33 tering the United States at those ports of entry;
- 34 (B) conduct inspections at those ports of entry to safeguard the
- 35 United States from terrorism and illegal entry of persons;
- 36 (C) prevent illicit drugs, agricultural pests, and contraband
- 37 from entering the United States;
- 38 (D) in coordination with the Commissioner, facilitate and expedite
- 39 the flow of legitimate travelers and trade;
- 40 (E) administer the National Targeting Center;

1 (F) coordinate with the Executive Assistant Commissioner with
2 respect to the trade facilitation and trade enforcement activities of
3 U.S. Customs and Border Protection; and

4 (G) carry out other duties and powers the Commissioner pre-
5 scribes.

6 (4) NATIONAL TARGETING CENTER.—

7 (A) IN GENERAL.—There is in the Office of Field Operations
8 a National Targeting Center.

9 (B) EXECUTIVE DIRECTOR.—An Executive Director is the head
10 of the National Targeting Center. The Executive Director shall re-
11 port to the Executive Assistant Commissioner of the Office of
12 Field Operations.

13 (C) DUTIES.—The National Targeting Center shall—

14 (i) serve as the primary forum for targeting operations in
15 U.S. Customs and Border Protection to collect and analyze
16 traveler and cargo information in advance of arrival in the
17 United States;

18 (ii) identify, review, and target travelers and cargo for ex-
19 amination;

20 (iii) coordinate the examination of entry and exit of trav-
21 elers and cargo;

22 (iv) develop and conduct commercial risk assessment tar-
23 geting with respect to cargo destined for the United States;

24 (v) coordinate with the Transportation Security Adminis-
25 tration, as appropriate;

26 (vi) issue Trade Alerts pursuant to section 111(b) of the
27 Trade Facilitation and Trade Enforcement Act of 2015 (19
28 U.S.C. 4318(b)); and

29 (vii) carry out other duties and powers the Executive As-
30 sistant Commissioner prescribes.

31 (5) ANNUAL REPORT ON STAFFING.—

32 (A) IN GENERAL.—Not later than March 25 of each year, the
33 Executive Assistant Commissioner shall submit to the appropriate
34 congressional committees a report on the staffing model for the
35 Office of Field Operations, including information on how many su-
36 pervisors, front-line U.S. Customs and Border Protection officers,
37 and support personnel are assigned to each Field Office and port
38 of entry.

39 (B) FORM.—The report required under subparagraph (A) shall,
40 to the greatest extent practicable, be submitted in unclassified
41 form, but may be submitted in classified form, if the Executive As-

1 sistant Commissioner determines that a classified form is appro-
2 priate and informs the Committee on Homeland Security and the
3 Committee on Ways and Means of the House of Representatives
4 and the Committee on Homeland Security and Governmental Af-
5 fairs and the Committee on Finance of the Senate of the rea-
6 soning for a classified report.

7 (h) OFFICE OF INTELLIGENCE.—

8 (1) IN GENERAL.—There is in U.S. Customs and Border Protection
9 an Office of Intelligence.

10 (2) ASSISTANT COMMISSIONER.—An Assistant Commissioner is the
11 head of the Office of Intelligence. The Assistant Commissioner shall re-
12 port to the Commissioner.

13 (3) DUTIES.—The Office of Intelligence shall—

14 (A) develop, provide, coordinate, and implement intelligence ca-
15 pabilities into a cohesive intelligence enterprise to support the exe-
16 cution of the duties and responsibilities of U.S. Customs and Bor-
17 der Protection;

18 (B) collect and analyze advance traveler and cargo information;

19 (C) establish, in coordination with the Chief Intelligence Officer
20 of the Department, as appropriate, intelligence-sharing relation-
21 ships with Federal, State, local, and tribal agencies and intel-
22 ligence agencies;

23 (D) conduct risk-based covert testing of U.S. Customs and Bor-
24 der Protection operations, including for nuclear and radiological
25 risks; and

26 (E) carry out other duties and powers the Commissioner pre-
27 scribes.

28 (i) OFFICE OF INTERNATIONAL AFFAIRS.—

29 (1) IN GENERAL.—There is in U.S. Customs and Border Protection
30 an Office of International Affairs.

31 (2) ASSISTANT COMMISSIONER.—An Assistant Commissioner is the
32 head of the Office of International Affairs. The Assistant Commis-
33 sioner shall report to the Commissioner.

34 (3) DUTIES.—The Office of International Affairs, in collaboration
35 with the Office of Policy of the Department, shall—

36 (A) coordinate and support U.S. Customs and Border Protec-
37 tion's foreign initiatives, policies, programs, and activities;

38 (B) coordinate and support U.S. Customs and Border Protec-
39 tion's personnel stationed abroad;

40 (C) maintain partnerships and information sharing agreements
41 and arrangements with foreign governments, international organi-

1 zations, and United States agencies in support of U.S. Customs
2 and Border Protection duties and responsibilities;

3 (D) provide necessary capacity building, training, and assistance
4 to foreign border control agencies to strengthen global supply
5 chain and travel security, as appropriate;

6 (E) coordinate mission support services to sustain U.S. Customs
7 and Border Protection’s global activities;

8 (F) coordinate with customs authorities of foreign countries
9 with respect to trade facilitation and trade enforcement;

10 (G) coordinate U.S. Customs and Border Protection’s engage-
11 ment in international negotiations;

12 (H) advise the Commissioner with respect to matters arising in
13 the World Customs Organization and other international organiza-
14 tions on matters relating to the policies and procedures of U.S.
15 Customs and Border Protection;

16 (I) advise the Commissioner regarding international agreements
17 to which the United States is a party as the agreements relate to
18 the policies and procedures of U.S. Customs and Border Protec-
19 tion; and

20 (J) carry out other duties and powers the Commissioner pre-
21 scribes.

22 (j) OFFICE OF PROFESSIONAL RESPONSIBILITY.—

23 (1) IN GENERAL.—There is in U.S. Customs and Border Protection
24 an Office of Professional Responsibility.

25 (2) ASSISTANT COMMISSIONER.—An Assistant Commissioner is the
26 head of the Office of Professional Responsibility. The Assistant Com-
27 missioner shall report to the Commissioner.

28 (3) DUTIES.—The Office of Professional Responsibility shall—

29 (A) investigate criminal and administrative matters and mis-
30 conduct by officers, agents, and other employees of U.S. Customs
31 and Border Protection;

32 (B) manage integrity-related programs and policies of U.S. Cus-
33 toms and Border Protection;

34 (C) conduct research and analysis regarding misconduct of offi-
35 cers, agents, and other employees of U.S. Customs and Border
36 Protection; and

37 (D) carry out other duties and powers the Commissioner pre-
38 scribes.

39 (k) OFFICE OF TRADE.—

40 (1) DEFINITIONS.—In this subsection, the terms “customs and trade
41 laws of the United States”, “trade enforcement”, and “trade facilita-

1 tion” have the meanings given the terms in section 2 of the Trade Fa-
2 cilitation and Trade Enforcement Act of 2015 (19 U.S.C. 4301).

3 (2) IN GENERAL.—There is in U.S. Customs and Border Protection
4 an Office of Trade.

5 (3) EXECUTIVE ASSISTANT COMMISSIONER.—An Executive Assistant
6 Commissioner is the head of the Office of Trade. The Executive Assist-
7 ant Commissioner shall report to the Commissioner.

8 (4) DUTIES.—The Office of Trade shall—

9 (A) direct the development and implementation, pursuant to the
10 customs and trade laws of the United States, of policies and regu-
11 lations administered by U.S. Customs and Border Protection;

12 (B) advise the Commissioner with respect to the impact on
13 trade facilitation and trade enforcement of any policy or regulation
14 otherwise proposed or administered by U.S. Customs and Border
15 Protection;

16 (C) coordinate and cooperate with the Executive Assistant Com-
17 missioner for the Office of Field Operations with respect to the
18 trade facilitation and trade enforcement activities of U.S. Customs
19 and Border Protection carried out at the land borders and ports
20 of entry of the United States;

21 (D) direct the development and implementation of matters relat-
22 ing to the priority trade issues identified by the Commissioner in
23 the joint strategic plan on trade facilitation and trade enforcement
24 required under section 105 of the Trade Facilitation and Trade
25 Enforcement Act of 2015 (19 U.S.C. 4314);

26 (E) otherwise advise the Commissioner with respect to the de-
27 velopment and implementation of the joint strategic plan;

28 (F) direct the trade enforcement activities of U.S. Customs and
29 Border Protection;

30 (G) oversee the trade modernization activities of U.S. Customs
31 and Border Protection, including the development and implemen-
32 tation of the Automated Commercial Environment computer sys-
33 tem authorized under section 13031(f)(5) of the Consolidated Om-
34 nibus Budget and Reconciliation Act of 1985 (19 U.S.C.
35 58c(f)(5)) and support for the establishment of the International
36 Trade Data System under the oversight of the Department of
37 Treasury pursuant to section 411(d) of the Tariff Act of 1930 (19
38 U.S.C. 1411(d));

39 (H) direct the administration of customs revenue functions as
40 otherwise provided by law or delegated by the Commissioner; and

1 (I) prepare an annual report to be submitted to the Committee
2 on Finance of the Senate and the Committee on Ways and Means
3 of the House of Representatives not later than March 1 of each
4 calendar year that includes—

5 (i) a summary of the changes to customs policies and regu-
6 lations adopted by U.S. Customs and Border Protection dur-
7 ing the preceding calendar year; and

8 (ii) a description of the public vetting and interagency con-
9 sultation that occurred with respect to each change.

10 (5) TRANSFER OF ASSETS, FUNCTIONS, AND PERSONNEL.—The
11 Commissioner may transfer any assets, functions, or personnel in U.S.
12 Customs and Border Protection to the Office of Trade. Not less than
13 90 days prior to the transfer, the Commissioner shall notify the Com-
14 mittee on Finance of the Senate, the Committee on Homeland Security
15 and Government Affairs of the Senate, the Committee on Ways and
16 Means of the House of Representatives, and the Committee on Home-
17 land Security of the House of Representatives of the specific assets,
18 functions, or personnel to be transferred, and the reason for the trans-
19 fer.

20 (1) OTHER AUTHORITIES.—

21 (1) IN GENERAL.—The Secretary may establish such other offices or
22 positions of Assistant Commissioners (or other similar officers or offi-
23 cials) as the Secretary determines necessary to carry out the missions,
24 duties, functions, and authorities of U.S. Customs and Border Protec-
25 tion.

26 (2) NOTIFICATION.—If the Secretary exercises the authority pro-
27 vided under paragraph (1), the Secretary shall notify the Committee
28 on Homeland Security of the House of Representative and the Com-
29 mittee on Homeland Security and Governmental Affairs of the Senate
30 not later than 30 days before exercising the authority

31 (m) RESCUE BEACONS.—In carrying out section 11102(b)(8), the Com-
32 missioner shall purchase, deploy, and maintain not more than 250 self-
33 powering, 911 cellular relay rescue beacons along the southern border of the
34 United States at locations determined appropriate by the Commissioner to
35 mitigate migrant deaths.

36 (n) AUTHORITY OF OTHER FEDERAL AGENCIES NOT AFFECTED.—Noth-
37 ing in subsections (a) through (j), (l), and (m) may be construed as affect-
38 ing in any manner the authority, existing on February 23, 2016, of any
39 other Federal agency or component of the Department.

1 **§ 10307. U.S. Immigration and Customs Enforcement**

2 There is in the Department an agency known as U.S. Immigration and
3 Customs Enforcement. The Director of U.S. Immigration and Customs En-
4 forcement is the head of U.S. Immigration and Customs Enforcement. The
5 Director reports directly to the Secretary and shall have a minimum of 5
6 years professional experience in law enforcement and a minimum of 5 years
7 of management experience.

8 **§ 10308. U.S. Citizenship and Immigration Services**

9 There is in the Department an agency known as U.S. Citizenship and Im-
10 migration Services. The Director of U.S. Citizenship and Immigration Serv-
11 ices is the head of U.S. Citizenship and Immigration Services. The Director
12 of U.S. Citizenship and Immigration Services reports directly to the Deputy
13 Secretary of Homeland Security, shall have a minimum of 5 years of man-
14 agement experience, and shall be paid at the same level as the Director of
15 U.S. Immigration and Customs Enforcement.

16 **§ 10309. Federal Emergency Management Agency**

17 (a) ESTABLISHMENT.—There is in the Department the Federal Emer-
18 gency Management Agency. The Federal Emergency Management Agency
19 is a distinct entity in the Department.

20 (b) ADMINISTRATOR.—The Administrator of the Federal Emergency
21 Management Agency is the head of the Agency. The Administrator shall be
22 appointed by the President, by and with the advice and consent of the Sen-
23 ate, from among individuals who have—

24 (1) a demonstrated ability in and knowledge of emergency manage-
25 ment and homeland security; and

26 (2) not less than 5 years of executive leadership and management
27 experience in the public or private sector.

28 (c) DEPUTY ADMINISTRATORS.—The President may appoint, by and with
29 the advice and consent of the Senate, not more than 4 Deputy Administra-
30 tors to assist the Administrator in carrying out chapter 111 of this title.

31 (d) UNITED STATES FIRE ADMINISTRATOR.—The Administrator of the
32 United States Fire Administration shall have a rank equivalent to an assist-
33 ant secretary of the Department.

34 **§ 10310. Transportation Security Administration**

35 (a) ESTABLISHMENT.—There is in the Department the Transportation
36 Security Administration. The Administration is a distinct entity in the De-
37 partment.

38 (b) ADMINISTRATOR.—

39 (1) IN GENERAL.—The Administrator of the Transportation Security
40 Administration (in this section referred to as the “Administrator”) is
41 the head of the Administration. The Administrator shall be appointed

1 by the President, by and with the advice and consent of the Senate.
2 The Administrator shall be a citizen of the United States and have ex-
3 perience in a field directly related to transportation or security.

4 (2) TERM.—The term of office of an individual appointed as the Ad-
5 ministrator is 5 years.

6 (3) LIMITATION ON OWNERSHIP OF STOCKS AND BONDS.—The Ad-
7 ministrator may not own stock in or bonds of a transportation or secu-
8 rity enterprise or an enterprise that makes equipment that could be
9 used for security purposes.

10 (c) DEPUTY ADMINISTRATOR.—

11 (1) IN GENERAL.—There is in the Transportation Security Adminis-
12 tration a Deputy Administrator, who shall assist the Administrator in
13 the management of the Transportation Security Administration. The
14 Deputy Administrator shall be appointed by the President. The Deputy
15 Administrator shall be a citizen of the United States and have experi-
16 ence in a field directly related to transportation or security.

17 (2) ACTING ADMINISTRATOR.—The Deputy Administrator shall be
18 Acting Administrator during the absence or incapacity of the Adminis-
19 trator or during a vacancy in the office of Administrator.

20 (d) CHIEF COUNSEL.—There is in the Transportation Security Adminis-
21 tration a Chief Counsel, who shall advise the Administrator and other senior
22 officials on all legal matters relating to the responsibilities, functions, and
23 management of the Transportation Security Administration. The Chief
24 Counsel shall be a citizen of the United States.

25 (e) AIR CARGO SECURITY DIVISION.—

26 (1) ESTABLISHMENT.—The Administrator shall establish an air
27 cargo security division to carry out and engage with stakeholders re-
28 garding the implementation of air cargo security programs established
29 by the Transportation Security Administration.

30 (2) LEADERSHIP.—The air cargo security division shall be headed by
31 an individual in the executive service in the Transportation Security
32 Administration.

33 (3) STAFFING.—The air cargo security division shall be staffed by
34 not fewer than 4 full-time equivalents, including the head of the divi-
35 sion. The Administrator shall staff the air cargo security division with
36 existing Transportation Security Administration personnel.

37 (f) NATIONAL DEPLOYMENT OFFICE.—

38 (1) ESTABLISHMENT.—There is in the Transportation Security Ad-
39 ministration a National Deployment Office. An individual with super-
40 visory experience is the head of the National Deployment Office. The
41 Administrator shall designate the individual.

1 (2) DUTIES OF HEAD OF OFFICE.—The individual designated as the
2 head of the National Deployment Office shall be responsible for the fol-
3 lowing:

4 (A) Maintaining a National Deployment Force in the Transporta-
5 tion Security Administration, including transportation security
6 officers, supervisory transportation security officers, and lead
7 transportation security officers, to provide the Transportation Se-
8 curity Administration with rapid and efficient response capabilities
9 and augment the Department’s homeland security operations to
10 mitigate and reduce risk, including for the following:

11 (i) Airports temporarily requiring additional security per-
12 sonnel due to an emergency, seasonal demands, hiring short-
13 falls, severe weather conditions, passenger volume mitigation,
14 equipment support, or other reasons.

15 (ii) Special events requiring enhanced security, including
16 National Special Security Events, as determined by the Sec-
17 retary.

18 (iii) Response in the aftermath of a manmade disaster, in-
19 cluding a terrorist attack.

20 (iv) Other similar situations, as determined by the Admin-
21 istrator.

22 (B) Educating transportation security officers regarding how to
23 participate in the Transportation Security Administration’s Na-
24 tional Deployment Force.

25 (C) Recruiting officers to serve on the National Deployment
26 Force, in accordance with a staffing model to be developed by the
27 Administrator.

28 (D) Approving 1-year appointments for officers to serve on the
29 National Deployment Force, with an option to extend on request
30 of the officer and with the approval of the appropriate Federal Se-
31 curity Director.

32 (E) Training officers to serve on the National Deployment
33 Force.

34 (3) CAREER DEVELOPMENT.—The Administrator may consider serv-
35 ice in the National Deployment Force as a positive factor when evalu-
36 ating applicants for promotion in the Transportation Security Adminis-
37 tration.

38 (g) INDIVIDUALS RESPONSIBLE AND ACCOUNTABLE FOR SPECIFIC
39 AREAS.—

40 (1) IN GENERAL.—For each of the areas described in paragraph (2),
41 the Administrator shall appoint at least 1 individual who shall—

1 (A) report directly to the Administrator or the Administrator's
2 designated direct report; and

3 (B) be responsible and accountable for that area.

4 (2) AREAS.—The areas referred to in paragraph (1) are as follows:

5 (A) Aviation security operations and training, including risk-
6 based, adaptive security focused on—

7 (i) airport checkpoint and baggage screening operations;

8 (ii) workforce training and development programs; and

9 (iii) ensuring compliance with aviation security law, includ-
10 ing regulations, and other specialized programs designed to
11 secure air transportation.

12 (B) Surface transportation security operations and training, in-
13 cluding risk-based, adaptive security focused on—

14 (i) accomplishing security systems assessments;

15 (ii) reviewing and prioritizing projects for appropriated sur-
16 face transportation security grants;

17 (iii) operator compliance with surface transportation secu-
18 rity law, including regulations, and voluntary industry stand-
19 ards; and

20 (iv) workforce training and development programs, and
21 other specialized programs designed to secure surface trans-
22 portation.

23 (C) Transportation industry engagement and planning, includ-
24 ing the development, interpretation, promotion, and oversight of a
25 unified effort regarding risk-based, risk-reducing security policies
26 and plans (including strategic planning for future contingencies
27 and security challenges) between government and transportation
28 stakeholders, including airports, domestic and international air-
29 lines, general aviation, air cargo, mass transit and passenger rail,
30 freight rail, pipeline, highway and motor carriers, and maritime.

31 (D) International strategy and operations, including agency ef-
32 forts to work with international partners to secure the global
33 transportation network.

34 (E) Trusted and registered traveler programs, including the
35 management and marketing of the agency's trusted traveler initia-
36 tives, including the PreCheck Program, and coordination with
37 trusted traveler programs of other Department agencies and the
38 private sector.

39 (F) Technology acquisition and deployment, including the over-
40 sight, development, testing, evaluation, acquisition, deployment,

1 and maintenance of security technology and other acquisition pro-
2 grams.

3 (G) Inspection and compliance, including the integrity, effi-
4 ciency, and effectiveness of the agency's workforce, operations, and
5 programs through objective audits, covert testing, inspections,
6 criminal investigations, and regulatory compliance.

7 (H) Civil rights, liberties, and traveler engagement, including
8 ensuring that agency employees and the traveling public are treat-
9 ed in a fair and lawful manner consistent with Federal laws and
10 regulations protecting privacy and prohibiting discrimination and
11 reprisal.

12 (I) Legislative and public affairs, including communication and
13 engagement with internal and external audiences in a timely, accu-
14 rate, and transparent manner, and development and implementa-
15 tion of strategies in the agency to achieve congressional approval
16 or authorization of agency programs and policies.

17 (3) NOTIFICATION.—The Administrator shall submit to the appro-
18 priate committees of Congress—

19 (A) not later than 180 days after October 5, 2018, a list of the
20 names of the individuals appointed under paragraph (1); and

21 (B) an update of the list not later than 5 days after a new indi-
22 vidual is appointed under paragraph (1).

23 **§ 10311. United States Secret Service**

24 (a) IN GENERAL.—The United States Secret Service (in this section re-
25 ferred to as the “Secret Service”) is a distinct entity in the Department.
26 The Secretary succeeds to the functions, personnel, assets, and obligations
27 of the Secret Service, including the functions of the Secretary of the Treas-
28 ury relating to the Secret Service.

29 (b) NATIONAL COMPUTER FORENSICS INSTITUTE.—

30 (1) DEFINITIONS.—In this subsection:

31 (A) CYBERSECURITY THREAT.—The term “cybersecurity
32 threat” has the meaning given that term in section 10781 of this
33 title.

34 (B) INCIDENT.—The term “incident” has the meaning given
35 that term in section 10701 of this title.

36 (C) INFORMATION SYSTEM.—The term “information system”
37 has the meaning given that term in section 10781 of this title.

38 (2) IN GENERAL; MISSION.—There is through fiscal year 2028 in the
39 Secret Service a National Computer Forensics Institute (in this sub-
40 section referred to as the “Institute”). The Institute's mission shall be
41 to educate, train, and equip State, local, territorial, and Tribal law en-

1 enforcement officers, prosecutors, and judges, as well as participants in
2 the Secret Service's network of cyber fraud task forces who are Federal
3 employees, members of the uniformed services, or State, local, Tribal,
4 or territorial employees, regarding the investigation and prevention of
5 cybersecurity incidents, electronic crime and related cybersecurity
6 threats, including through the dissemination of homeland security in-
7 formation in accordance with relevant Federal law regarding privacy
8 civil rights, and civil liberties protections.

9 (3) CURRICULUM.—In furtherance of paragraph (2), all education
10 and training of the Institute shall be conducted in accordance with rel-
11 evant Federal law regarding privacy, civil rights, and civil liberties pro-
12 tections. Education and training provided pursuant to paragraph (2)
13 shall relate to the following:

14 (A) Investigating and preventing cybersecurity incidents, elec-
15 tronic crimes, and related cybersecurity threats, including relating
16 to instances involving illicit use of digital assets and emerging
17 trends in cybersecurity and electronic crime.

18 (B) Conducting forensic examinations of computers, mobile de-
19 vices, and other information systems.

20 (C) Prosecutorial and judicial considerations related to cyberse-
21 curity incidents, electronic crimes, related cybersecurity threats,
22 and forensic examinations of computers, mobile devices, and other
23 information systems.

24 (D) Methods to obtain, process, store, and admit digital evi-
25 dence in court.

26 (4) PRINCIPLES.—In carrying out the functions specified in sub-
27 section (b), the Institute shall ensure, to the extent practicable, that
28 timely, actionable, and relevant expertise and information related to cy-
29 bersecurity incidents, electronic crimes, and related cybersecurity
30 threats is shared with recipients of education and training provided
31 pursuant to paragraph (2). When selecting participants for the train-
32 ing, the Institute shall prioritize, to the extent reasonable and prac-
33 ticable, providing education and training to individuals from geographi-
34 cally-diverse jurisdictions throughout the United States, and the Insti-
35 tute shall prioritize, to the extent reasonable and practicable, State,
36 local, tribal, and territorial law enforcement officers, prosecutors,
37 judges, and other employees.

38 (5) PROVIDING COMPUTER EQUIPMENT, HARDWARE, SOFTWARE,
39 MANUALS, AND TOOLS.—The Institute may provide recipients of edu-
40 cation and training provided pursuant to paragraph (2) with computer
41 equipment, hardware, software, manuals, and tools for investigating

1 and preventing cybersecurity incidents, electronic crimes, and related
2 cybersecurity threats, and for forensic examinations of computers, mo-
3 bile devices, and other information systems.

4 (6) CYBER FRAUD TASK FORCES.—The Institute shall facilitate the
5 expansion of the network of Cyber Fraud Task Forces of the United
6 States Secret Service through the addition of recipients of education
7 and training provided pursuant to paragraph (2) educated and trained
8 by the Institute.

9 (7) EXPENSES.—The Director of the United States Secret Service
10 may pay for all or a part of the education, training, or equipment pro-
11 vided by the Institute, including relating to the travel, transportation,
12 and subsistence expenses of recipients of education and training pro-
13 vided pursuant to paragraph (2).

14 (8) Annual reports to congress.—

15 (A) IN GENERAL.— The Secretary shall include in the annual
16 report required under section 1116 of title 31 information regarding
17 the activities of the Institute, including, where possible, the fol-
18 lowing:

19 (i) An identification of jurisdictions with recipients of the
20 education and training provided pursuant to paragraph (2)
21 during that year.

22 (ii) Information relating to the costs associated with that
23 education and training.

24 (iii) Any information regarding projected future demand
25 for the education and training provided pursuant to para-
26 graph (2).

27 (iv) Impacts of the activities of the Institute on the capa-
28 bility of jurisdictions to investigate and prevent cybersecurity
29 incidents, electronic crimes, and related cybersecurity threats.

30 (v) A description of the nomination process for potential re-
31 cipients of the information and training provided pursuant to
32 paragraph (2).

33 (vi) Any other issues determined relevant by the Secretary.

34 (B) EXCEPTION.— Any information required under subpara-
35 graph (A) that is submitted as part of the annual budget sub-
36 mitted by the President to Congress under section 1105 of title
37 31 is not required to be included in the report required under sub-
38 paragraph (A).

39 (9) SAVINGS PROVISION.—All authorized activities and functions car-
40 ried out by the Institute at any location as of November 1, 2017, may
41 continue to be carried out at that location after November 1, 2017.

1 (c) USE OF PROCEEDS DERIVED FROM CRIMINAL INVESTIGATIONS.—

2 (1) IN GENERAL.—With respect to any undercover investigative oper-
3 ation of the Secret Service that is necessary for the detection and pros-
4 ecutio n of crimes against the United States—

5 (A) sums appropriated for the Secret Service, including unobli-
6 gated balances available from prior fiscal years, may be used for
7 purchasing property, buildings, and other facilities, and for leasing
8 space, in the United States, the District of Columbia, and the ter-
9 ritories and possessions of the United States, without regard to
10 sections 1341 and 3324 of title 31, section 8141 of title 40, and
11 section 3901, chapter 45, and sections 6301(a) and (b)(1) to (3)
12 and 6306(a) of title 41;

13 (B) sums appropriated for the Secret Service, including unobli-
14 gated balances available from prior fiscal years, may be used to
15 establish or to acquire proprietary corporations or business entities
16 as part of the undercover operation, and to operate the corpora-
17 tions or business entities on a commercial basis, without regard
18 to sections 9102 and 9103 of title 31;

19 (C) sums appropriated for the Secret Service, including unobli-
20 gated balances available from prior fiscal years and the proceeds
21 from the undercover operation, may be deposited in banks or other
22 financial institutions, without regard to section 648 of title 18 and
23 section 3302 of title 31; and

24 (D) proceeds from the undercover operation may be used to off-
25 set necessary and reasonable expenses incurred in the operation,
26 without regard to section 3302 of title 31.

27 (2) WRITTEN CERTIFICATION.—The authority set forth in paragraph
28 (1) may be exercised only on the written certification of the Director
29 of the Secret Service or designee that any action authorized by any
30 subparagraph of paragraph (1) is necessary for the conduct of an un-
31 dercover investigative operation. The certification shall continue in ef-
32 fect for the duration of the operation, without regard to fiscal years.

33 (3) DEPOSIT OF PROCEEDS.—As soon as practicable after the pro-
34 ceeds from an undercover investigative operation with respect to which
35 an action is authorized and carried out under subparagraphs (C) and
36 (D) of paragraph (1) are no longer necessary for the conduct of the
37 operation, the proceeds or the balance of the proceeds remaining at the
38 time shall be deposited in the Treasury as miscellaneous receipts.

39 (4) REPORTING AND DEPOSIT OF PROCEEDS ON DISPOSITION OF
40 CERTAIN BUSINESS ENTITIES.—If a corporation or business entity es-
41 tablished or acquired as part of an undercover investigative operation

1 under paragraph (1)(B) with a net value of over \$50,000 is to be liq-
2 uidated, sold, or otherwise disposed of, the Secret Service, as much in
3 advance as the Director or designee determines is practicable, shall re-
4 port the circumstance to the Secretary. The proceeds of the liquidation,
5 sale, or other disposition, after obligations are met, shall be deposited
6 in the Treasury as miscellaneous receipts.

7 (5) FINANCIAL AUDITS AND REPORTS.—

8 (A) SECRET SERVICE.—The Secret Service shall conduct de-
9 tailed financial audits of closed undercover investigative operations
10 for which a written certification was made pursuant to paragraph
11 (2) on a quarterly basis and shall report the results of the audits
12 in writing to the Secretary.

13 (B) SUBMISSION TO APPROPRIATIONS COMMITTEES.—The Sec-
14 retary annually shall submit to the Committees on Appropriations
15 of the Senate and House of Representatives, at the time that the
16 President's budget is submitted under section 1105(a) of title 31,
17 a summary of the audits.

18 **§ 10312. Coast Guard**

19 (a) IN GENERAL.—The Coast Guard is a distinct entity in the Depart-
20 ment. The Commandant reports directly to the Secretary without being re-
21 quired to report through any other official of the Department.

22 (b) TRANSFER.—

23 (1) IN GENERAL.—The authorities, functions, personnel, and assets
24 of the Coast Guard, including the authorities and functions of the Sec-
25 retary of Transportation relating to the Coast Guard, are transferred
26 to the Secretary. Notwithstanding this subtitle, the authorities, func-
27 tions, and capabilities of the Coast Guard to perform its missions shall
28 be maintained intact and without significant reduction, except as speci-
29 fied in Acts subsequent to the Homeland Security Act of 2002 (Public
30 Law 107–296, 116 Stat. 2135).

31 (2) CERTAIN TRANSFERS PROHIBITED.—No mission, function, or
32 asset (including for purposes of this paragraph a ship, aircraft, or heli-
33 copter) of the Coast Guard may be diverted to the principal and con-
34 tinuing use of another organization, unit, or entity of the Department,
35 except for details or assignments that do not reduce the Coast Guard's
36 capability to perform its missions.

37 (c) CHANGES TO MISSIONS.—

38 (1) PROHIBITION.—The Secretary may not substantially or signifi-
39 cantly reduce the missions of the Coast Guard or the Coast Guard's
40 capability to perform those missions, except as specified in Acts subse-

1 **§ 10315. Office of Counternarcotics Enforcement**

2 (a) OFFICE.—There is in the Department the Office of Counternarcotics
3 Enforcement. The Director is the head of the Office. The Director is ap-
4 pointed by the President.

5 (b) ASSIGNMENT OF PERSONNEL.—

6 (1) IN GENERAL.—The Secretary shall assign permanent staff to the
7 Office of Counternarcotics Enforcement, consistent with effective man-
8 agement of Department resources.

9 (2) LIAISONS.—The Secretary shall designate senior employees from
10 each appropriate subdivision of the Department that has significant
11 counternarcotics responsibilities to act as a liaison between that sub-
12 division and the Office of Counternarcotics Enforcement.

13 (c) LIMITATION ON CONCURRENT EMPLOYMENT.—The Director of the
14 Office of Counternarcotics Enforcement shall not be employed by, assigned
15 to, or serve as the head of, another branch of the Federal Government, a
16 State or local government, or a subdivision of the Department other than
17 the Office of Counternarcotics Enforcement.

18 (d) RESPONSIBILITIES.—The Secretary shall direct the Director of the
19 Office of Counternarcotics Enforcement—

20 (1) to coordinate policy and operations within the Department, be-
21 tween the Department and other Federal departments and agencies,
22 and between the Department and State and local agencies with respect
23 to stopping the entry of illegal drugs into the United States;

24 (2) to ensure the adequacy of resources within the Department for
25 stopping the entry of illegal drugs into the United States;

26 (3) to recommend the appropriate financial and personnel resources
27 necessary to help the Department better fulfill its responsibility to stop
28 the entry of illegal drugs into the United States;

29 (4) in the Joint Terrorism Task Force construct, to track and sever
30 connections between illegal drug trafficking and terrorism; and

31 (5) to be a representative of the Department on all task forces, com-
32 mittees, or other entities whose purpose is to coordinate the counter-
33 narcotics enforcement activities of the Department and other Federal,
34 State or local agencies.

35 (e) SAVINGS CLAUSE.—Nothing in this section shall be construed to au-
36 thorize direct control of the operations conducted by the Commissioner of
37 U.S. Customs and Border Protection, the Coast Guard, or joint terrorism
38 task forces.

39 (f) REPORTS TO CONGRESS.—

40 (1) ANNUAL BUDGET REVIEW.—The Director of the Office of Coun-
41 ternarcotics Enforcement shall, not later than 30 days after the sub-

1 mission by the President to Congress of a request for expenditures for
2 the Department, submit to the Committees on Appropriations and the
3 authorizing committees of jurisdiction of the House of Representatives
4 and the Senate a review and evaluation of the request. The review and
5 evaluation shall—

6 (A) identify a request or subpart of a request that affects or
7 may affect the counternarcotics activities of the Department or its
8 subdivisions, or that affects the ability of the Department or a
9 subdivision of the Department to meet its responsibility to stop
10 the entry of illegal drugs into the United States;

11 (B) describe with particularity how requested funds would be or
12 could be expended in furtherance of counternarcotics activities;
13 and

14 (C) compare the requests with requests for expenditures and
15 amounts appropriated by Congress in the previous fiscal year.

16 (2) EVALUATION OF COUNTERNARCOTICS ACTIVITIES.—The Director
17 of the Office of Counternarcotics Enforcement shall, not later than
18 February 1 each year, submit to the Committees on Appropriations
19 and the authorizing committees of jurisdiction of the House of Rep-
20 resentatives and the Senate a review and evaluation of the counter-
21 narcotics activities of the Department for the previous fiscal year. The
22 review and evaluation shall—

23 (A) describe the counternarcotics activities of the Department
24 and each subdivision of the Department (whether individually or
25 in cooperation with other subdivisions of the Department, or in co-
26 operation with other branches of the Federal Government or with
27 State or local agencies), including the methods, procedures, and
28 systems (including computer systems) for collecting, analyzing,
29 sharing, and disseminating information concerning narcotics activ-
30 ity within the Department and between the Department and other
31 Federal, State, and local agencies;

32 (B) describe the results of those activities, using quantifiable
33 data whenever possible;

34 (C) state whether those activities were sufficient to meet the re-
35 sponsibility of the Department to stop the entry of illegal drugs
36 into the United States, including a description of the performance
37 measures of effectiveness that were used in making that deter-
38 mination; and

39 (D) recommend, where appropriate, changes to those activities
40 to improve the performance of the Department in meeting its re-

1 sponsibility to stop the entry of illegal drugs into the United
2 States.

3 (3) CLASSIFIED OR LAW ENFORCEMENT SENSITIVE INFORMATION.—
4 Any content of a review and evaluation described in the reports re-
5 quired in this subsection that involves information classified under cri-
6 teria established by an Executive order, or whose public disclosure, as
7 determined by the Secretary, would be detrimental to the law enforce-
8 ment or national security activities of the Department or any other
9 Federal, State, or local agency, shall be presented to Congress sepa-
10 rately from the rest of the review and evaluation.

11 **§ 10316. Office of International Affairs**

12 (a) ESTABLISHMENT.—There is in the Office of the Secretary the Office
13 of International Affairs. The Director is the head of the Office. The Direc-
14 tor shall be a senior official appointed by the Secretary.

15 (b) DUTIES OF THE DIRECTOR.—The Director shall have the following
16 duties:

17 (1) To promote information and education exchange with nations
18 friendly to the United States in order to promote sharing of best prac-
19 tices and technologies relating to homeland security. The exchange
20 shall include the following:

21 (A) Exchange of information on research and development on
22 homeland security technologies.

23 (B) Joint training exercises of first responders.

24 (C) Exchange of expertise on terrorism prevention, response,
25 and crisis management.

26 (2) To identify areas for homeland security information and training
27 exchange where the United States has a demonstrated weakness and
28 another friendly nation or nations have a demonstrated expertise.

29 (3) To plan and undertake international conferences, exchange pro-
30 grams, and training activities.

31 (4) To manage international activities in the Department in coordi-
32 nation with other Federal officials responsible for counterterrorism
33 matters.

34 **§ 10317. Office for National Capital Region Coordination**

35 There is in the Office of the Secretary the Office of National Capital Re-
36 gion Coordination. The Director is the head of the Office. The Director is
37 appointed by the Secretary.

38 **§ 10318. Office of Cargo Security Policy**

39 There is in the Department the Office of Cargo Security Policy. The Di-
40 rector is the head of the Office. The Director is appointed by the Secretary.
41 The Director reports to the Assistant Secretary for Policy.

1 **§ 10319. Transportation Security Oversight Board**

2 (a) ESTABLISHMENT.—There is in the Department the Transportation
3 Security Oversight Board (in this section referred to as the “Board”).

4 (b) MEMBERSHIP.—

5 (1) NUMBER.—The Board is composed of 7 members as follows:

6 (A) The Secretary, or the Secretary’s designee.

7 (B) The Secretary of Transportation, or the Secretary of Trans-
8 portation’s designee.

9 (C) The Attorney General, or the Attorney General’s designee.

10 (D) The Secretary of Defense, or the Secretary of Defense’s
11 designee.

12 (E) The Secretary of the Treasury, or the Secretary of the
13 Treasury’s designee.

14 (F) The Director of National Intelligence, or the Director’s des-
15 ignee.

16 (G) One member appointed by the President to represent the
17 National Security Council.

18 (2) CHAIRPERSON.—The Secretary is the Chairperson of the Board.

19 (c) DUTIES.—The Board shall—

20 (1) review and ratify or disapprove a regulation or security directive
21 issued by the Administrator of the Transportation Security Administra-
22 tion under section 11507(b) of this title within 30 days after the date
23 of issuance of the regulation or directive;

24 (2) facilitate the coordination of intelligence, security, and law en-
25 forcement activities affecting transportation;

26 (3) facilitate the sharing of intelligence, security, and law enforce-
27 ment information affecting transportation among Federal agencies and
28 with carriers and other transportation providers as appropriate;

29 (4) explore the technical feasibility of developing a common database
30 of individuals who may pose a threat to transportation or national se-
31 curity;

32 (5) review plans for transportation security;

33 (6) make recommendations to the Administrator of the Transpor-
34 tation Security Administration regarding matters reviewed under para-
35 graph (5).

36 (d) QUARTERLY MEETINGS.—The Board shall meet at least quarterly.

37 (e) CONSIDERATION OF SECURITY INFORMATION.—A majority of the
38 Board may vote to close a meeting of the Board to the public, except that
39 meetings shall be closed to the public whenever classified information or
40 sensitive security information will be discussed.

1 **§ 10320. Special Assistant to the Secretary**

2 The Secretary shall appoint a Special Assistant to the Secretary. The
3 Special Assistant is responsible for—

4 (1) creating and fostering strategic communications with the private
5 sector to enhance the primary mission of the Department to protect the
6 American homeland;

7 (2) advising the Secretary on the impact of the Department’s poli-
8 cies, regulations, processes, and actions on the private sector;

9 (3) interfacing with other relevant Federal agencies with homeland
10 security missions to assess the impact of these agencies’ actions on the
11 private sector;

12 (4) creating and managing private-sector advisory councils composed
13 of representatives of industries and associations designated by the Sec-
14 retary to—

15 (A) advise the Secretary on private-sector products, applica-
16 tions, and solutions as they relate to homeland security challenges;

17 (B) advise the Secretary on homeland security policies, regula-
18 tions, processes, and actions that affect the participating indus-
19 tries and associations; and

20 (C) advise the Secretary on private-sector preparedness issues,
21 including effective methods for—

22 (i) promoting voluntary preparedness standards to the pri-
23 vate sector; and

24 (ii) assisting the private sector in adopting voluntary pre-
25 paredness standards;

26 (5) working with Federal laboratories, federally funded research and
27 development centers, other federally funded organizations, academia,
28 and the private sector to develop innovative approaches to address
29 homeland security challenges to produce and deploy the best available
30 technologies for homeland security missions;

31 (6) promoting existing public-private partnerships and developing
32 new public-private partnerships to provide for collaboration and mutual
33 support to address homeland security challenges;

34 (7) assisting in the development and promotion of private-sector best
35 practices to secure critical infrastructure;

36 (8) providing information to the private sector regarding voluntary
37 preparedness standards and the business justification for preparedness,
38 and promoting to the private sector the adoption of voluntary prepared-
39 ness standards;

40 (9) coordinating industry efforts, with respect to functions of the De-
41 partment, to identify private-sector resources and capabilities that

1 could be effective in supplementing Federal, State, and local govern-
2 ment agency efforts to prevent or respond to a terrorist attack;

3 (10) coordinating with the Commissioner of U.S. Customs and Bor-
4 der Protection and the Assistant Secretary for Trade Development of
5 the Department of Commerce on issues related to the travel and tour-
6 ism industries; and

7 (11) consulting with the Office of State and Local Government Co-
8 ordination and Preparedness on all matters of concern to the private
9 sector, including the tourism industry.

10 **§ 10321. Border Enforcement Security Task Force**

11 There is in the Department the Border Enforcement Security Task
12 Force.

13 **§ 10322. Office for Domestic Preparedness**

14 (a) ESTABLISHMENT.—There is in the Department an Office for Domes-
15 tic Preparedness. The Director is the head of the Office. The Director is
16 appointed by the President.

17 (b) RESPONSIBILITIES.—The Office for Domestic Preparedness has the
18 primary responsibility in the executive branch for the preparedness of the
19 United States for acts of terrorism, including—

20 (1) coordinating preparedness efforts at the Federal level, and work-
21 ing with all State, local, tribal, parish, and private-sector emergency re-
22 sponse providers on all matters pertaining to combating terrorism, in-
23 cluding training, exercises, and equipment support;

24 (2) coordinating or, as appropriate, consolidating communications
25 and systems of communications relating to homeland security at all lev-
26 els of government;

27 (3) directing and supervising terrorism preparedness grant programs
28 of the Federal Government (other than those programs administered by
29 the Department of Health and Human Services) for all emergency re-
30 sponse providers;

31 (4) incorporating the Strategy priorities into planning guidance on
32 an agency level for the preparedness efforts of the Office for Domestic
33 Preparedness;

34 (5) providing agency-specific training for agents and analysts within
35 the Department, other agencies, State and local agencies, and inter-
36 national entities;

37 (6) as the lead executive branch agency for preparedness of the
38 United States for acts of terrorism, cooperating closely with the Fed-
39 eral Emergency Management Agency, which shall have the primary re-
40 sponsibility within the executive branch to prepare for and mitigate the
41 effects of nonterrorist-related disasters in the United States;

1 (7) assisting and supporting the Secretary, in coordination with
2 other Directorates and entities outside the Department, in conducting
3 appropriate risk analysis and risk management activities of State, local,
4 and tribal governments consistent with the mission and functions of the
5 Department;

6 (8) administering those elements of the National Preparedness Di-
7 rectorate of the Federal Emergency Management Agency that relate to
8 terrorism, which shall be consolidated in the Department in the Office
9 for Domestic Preparedness; and

10 (9) helping to ensure the acquisition of interoperable communication
11 technology by State and local governments and emergency response
12 providers.

13 **§ 10323. Social media working group**

14 (a) ESTABLISHMENT.—The Secretary shall establish in the Department
15 a social media working group (in this section referred to as the “Group”).

16 (b) PURPOSE.—To enhance the dissemination of information through so-
17 cial media technologies between the Department and appropriate stake-
18 holders and to improve the use of social media technologies in support of
19 preparedness, response, and recovery, the Group shall identify, and provide
20 guidance and best practices to the emergency preparedness and response
21 community on, the use of social media technologies before, during, and after
22 a natural disaster or an act of terrorism or other man-made disaster.

23 (c) MEMBERSHIP.—

24 (1) IN GENERAL.—The Group shall be composed of a cross section
25 of subject matter experts from Federal, State, local, tribal, territorial,
26 and nongovernmental organization practitioners, including representa-
27 tives from the following entities:

28 (A) The Office of Public Affairs of the Department.

29 (B) The Office of the Chief Information Officer of the Depart-
30 ment.

31 (C) The Privacy Office of the Department.

32 (D) The Federal Emergency Management Agency.

33 (E) The Office of Disability Integration and Coordination of the
34 Federal Emergency Management Agency.

35 (F) The American Red Cross.

36 (G) The Forest Service.

37 (H) The Centers for Disease Control and Prevention.

38 (I) The United States Geological Survey.

39 (J) The National Oceanic and Atmospheric Administration.

1 (2) ADDITIONAL MEMBERS.—The chairperson shall appoint, on a ro-
2 tating basis, qualified individuals to the Group. The total number of
3 additional members shall—

4 (A) be equal to or greater than the total number of regular
5 members under paragraph (1); and

6 (B) include—

7 (i) not fewer than 3 representatives from the private sector;
8 and

9 (ii) representatives from—

10 (I) State, local, tribal, and territorial entities, includ-
11 ing from—

12 (aa) law enforcement;

13 (bb) fire services;

14 (cc) emergency management; and

15 (dd) public health entities;

16 (II) universities and academia; and

17 (III) nonprofit disaster relief organizations.

18 (3) TERM LIMITS.—The chairperson shall establish term limits for
19 individuals appointed to the Group under paragraph (2).

20 (d) CHAIRPERSON AND CO-CHAIRPERSON.—

21 (1) CHAIRPERSON.—The Secretary, or a designee of the Secretary,
22 shall serve as the chairperson of the Group.

23 (2) CO-CHAIRPERSON.—The chairperson shall designate, on a rotat-
24 ing basis, a representative from a State or local government who is a
25 member of the Group to serve as the co-chairperson of the Group.

26 (e) CONSULTATION WITH PUBLIC- AND PRIVATE-SECTOR ENTITIES.—To
27 the extent practicable, the Group shall work with public- and private-sector
28 entities to carry out subsection (b).

29 (f) MEETINGS.—

30 (1) IN GENERAL.—The Group shall meet—

31 (A) at the call of the chairperson; and

32 (B) not less frequently than twice each year.

33 (2) VIRTUAL MEETINGS.—Each meeting of the Group may be held
34 virtually.

35 (g) REPORTS.—During each year in which the Group meets, the Group
36 shall submit to the appropriate congressional committees a report that in-
37 cludes the following:

38 (1) A review and analysis of current and emerging social media tech-
39 nologies being used to support preparedness and response activities re-
40 lated to natural disasters and acts of terrorism and other man-made
41 disasters.

1 (2) A review of best practices and lessons learned on the use of social
2 media technologies during the response to natural disasters and acts
3 of terrorism and other man-made disasters that occurred during the
4 period covered by the report at issue.

5 (3) Recommendations to improve the Department's use of social
6 media technologies for emergency management purposes.

7 (4) Recommendations to improve public awareness of—

8 (A) the type of information disseminated through social media
9 technologies during a natural disaster or an act of terrorism or
10 other man-made disaster; and

11 (B) how to access the information.

12 (5) A review of available training for Federal, State, local, tribal, and
13 territorial officials on the use of social media technologies in response
14 to a natural disaster or an act of terrorism or other man-made dis-
15 aster.

16 (6) A review of coordination efforts with the private sector to discuss
17 and resolve legal, operational, technical, privacy, and security concerns.

18 (h) TERMINATION AND RENEWAL.—

19 (1) IN GENERAL.—The Group shall terminate on November 5, 2020,
20 unless the chairperson renews the Group for a successive 5-year period,
21 prior to November 5, 2020, by submitting to the Committee on Home-
22 land Security and Governmental Affairs of the Senate and the Com-
23 mittee on Homeland Security of the House of Representatives a certifi-
24 cation that the continued existence of the Group is necessary to fulfill
25 the purpose described in subsection (b).

26 (2) CONTINUED RENEWAL.—The chairperson may continue to renew
27 the Group for successive 5-year periods by submitting a certification in
28 accordance with paragraph (1) prior to the date on which the Group
29 would otherwise terminate.

30 **§ 10324. Office of Strategy, Policy, and Plans**

31 (a) ESTABLISHMENT.—There is in the Department an Office of Strategy,
32 Policy, and Plans. The Under Secretary for Strategy, Policy, and Plans is
33 the head of the Office. The Under Secretary is appointed by the President,
34 by and with the advice and consent of the Senate.

35 (b) DEPUTY UNDER SECRETARY.—

36 (1) DEFINITIONS.—For purposes of paragraph (2):

37 (A) CAREER EMPLOYEE.—The term “career employee” means
38 an employee (as the term is defined in section 2105 of title 5) but
39 does not include a political employee.

40 (B) POLITICAL APPOINTEE.—The term “political employee”
41 means an employee who occupies a position that has been excepted

1 from the competitive service by reason of its confidential policy-
2 determining, policy-making, or policy-advocating character.

3 (2) ESTABLISHMENT.—The Secretary may—

4 (A) establish in the Office of Strategy, Policy, and Plans a posi-
5 tion of Deputy Under Secretary to support the Under Secretary
6 for Strategy, Policy, and Plans in carrying out the Under Sec-
7 retary’s responsibilities; and

8 (B) appoint a career employee to the position.

9 (3) LIMITATION.—Except for the position provided for by paragraph
10 (2), a Deputy Under Secretary position (or a substantially similar posi-
11 tion) in the Office of Strategy, Policy, and Plans may not be estab-
12 lished unless the Secretary receives prior authorization from Congress.

13 (e) COUNTERING UNMANNED AIRCRAFT SYSTEMS COORDINATOR.—

14 (1) DEFINITIONS.—In this subsection:

15 (A) COORDINATOR.—The term “Coordinator” means the Coun-
16 tering Unmanned Aircraft Systems Coordinator.

17 (B) UAS.—The term “UAS” means unmanned aircraft systems
18 as described in section 10404 of this title.

19 (2) DESIGNATION OF COORDINATOR.—The Secretary shall designate
20 an individual in a Senior Executive Service position (as defined in sec-
21 tion 3132 of title 5) of the Department in the Office of Strategy, Pol-
22 icy, and Plans as the Countering Unmanned Aircraft Systems Coordi-
23 nator and provide appropriate staff to carry out the responsibilities of
24 the Coordinator.

25 (3) RESPONSIBILITIES.—The Coordinator shall—

26 (A) oversee and coordinate with relevant Department offices and
27 components, including the Office of Civil Rights and Civil Lib-
28 erties and the Privacy Office, on the development of guidance and
29 regulations to counter threats associated with UAS;

30 (B) promote research and development of counter UAS tech-
31 nologies in coordination within the Science and Technology Direc-
32 torate;

33 (C) coordinate with the relevant components and offices of the
34 Department, including the Office of Intelligence and Analysis, to
35 ensure the sharing of information, guidance, and intelligence relat-
36 ing to countering UAS threats, counter UAS threat assessments,
37 and counter UAS technology, including the retention of UAS and
38 counter UAS incidents within the Department;

39 (D) serve as the Department liaison, in coordination with rel-
40 evant components and offices of the Department, to the Depart-
41 ment of Defense, Federal, State, local, and Tribal law enforcement

1 entities, and the private sector regarding the activities of the De-
2 partment relating to countering UAS;

3 (E) maintain the information required under section
4 10404(h)(1)(C) of this title; and

5 (F) carry out other related counter UAS authorities and activi-
6 ties under section 10404 of this title, as directed by the Secretary.

7 (4) COORDINATION WITH APPLICABLE FEDERAL LAWS.—The Coordi-
8 nator shall, in addition to other assigned duties, coordinate with rel-
9 evant Department components and offices to ensure testing, evaluation,
10 or deployment of a system used to identify, assess, or defeat a UAS
11 is carried out in accordance with applicable Federal laws.

12 (5) COORDINATION WITH PRIVATE SECTOR.—The Coordinator shall,
13 among other assigned duties, working with the Office of Partnership
14 and Engagement and other relevant Department offices and compo-
15 nents, or other Federal agencies, as appropriate, serve as the principal
16 Department official responsible for sharing with the private sector in-
17 formation regarding counter UAS technology, particularly information
18 regarding instances in which counter UAS technology may impact law-
19 ful private-sector services or systems.

20 (B) patterns and practices of human trafficking;

21 (4) techniques to identify suspected victims of trafficking along the
22 United States border and at airport security checkpoints;

23 (5) methods to be used by the Transportation Security Administra-
24 tion and personnel from other appropriate agencies to train employees
25 of the Transportation Security Administration to—

26 (A) identify suspected victims of trafficking; and

27 (B) serve as a liaison and resource regarding human trafficking
28 prevention to appropriate State, local, and private-sector aviation
29 workers and the traveling public;

30 (6) the utilization of resources, such as indicator cards, fact sheets,
31 pamphlets, posters, brochures, and radio and television campaigns to—

32 (A) educate partners and stakeholders; and

33 (B) increase public awareness of human trafficking;

34 (7) the leveraging of partnerships with State and local governmental,
35 nongovernmental, and private-sector organizations to raise public
36 awareness of human trafficking; and

37 (8) any other activities the Secretary determines necessary to carry
38 out the Blue Campaign.

39 (d) ASSISTANT SECRETARY.—

40 (1) DEFINITIONS.—In this subsection:

1 (A) CRITICAL ECONOMIC SECURITY DOMAIN.—The term “crit-
2 ical economic security domain” means any infrastructure industry,
3 technology, or intellectual property (or combination thereof) that
4 is essential for the economic security of the United States.

5 (B) ECONOMIC SECURITY.—The term “economic security” has
6 the meaning given that term in section 10405(a) of this title.

7 (2) IN GENERAL.—There is in the Office of Strategy, Policy, and
8 Plans an Assistant Secretary, who shall assist the Secretary in carrying
9 out the duties under paragraph (3) and the responsibilities under para-
10 graph (4). Notwithstanding section 10302(b)(1) of this title, the Assist-
11 ant Secretary shall be appointed by the President without the advice
12 and consent of the Senate.

13 (3) DUTIES.—At the direction of the Secretary the Assistant Sec-
14 retary shall be responsible for policy formulation regarding matters re-
15 lating to economic security and trade, as those matters relate to the
16 mission and the operations of the Department.

17 (4) ADDITIONAL RESPONSIBILITIES.—In addition to the duties speci-
18 fied in paragraph (3) the Assistant Secretary, at the discretion of the
19 Secretary may—

20 (A) oversee—

21 (i) coordination of supply chain policy; and

22 (ii) assessments and reports to Congress related to critical
23 economic security domains;

24 (B) coordinate with stakeholders in other Federal departments
25 and agencies and nongovernmental entities with trade and eco-
26 nomic security interests authorities, and responsibilities; and

27 (C) perform such additional duties as the Secretary or the
28 Under Secretary of Strategy Policy, and Plans may prescribe.

29 **§ 10325. Immigration Detention Ombudsman**

30 (a) ESTABLISHMENT.—There is in the Department a position of Immi-
31 gration Detention Ombudsman (in this section referred to as the “Ombuds-
32 man”). The Ombudsman shall be independent of Department agencies and
33 officers and shall report directly to the Secretary. The Ombudsman shall be
34 a senior official with a background in civil rights enforcement, civil deten-
35 tion care and custody, and immigration law.

36 (b) FUNCTIONS.—The functions of the Ombudsman shall be to—

37 (1) establish and administer an independent, neutral, and confiden-
38 tial process to receive, investigate, resolve, and provide redress, includ-
39 ing referral for investigation to the Office of the Inspector General, re-
40 ferral to U.S. Citizenship and Immigration Services for immigration re-
41 lief, or other action determined appropriate, for cases in which Depart-

1 ment officers or other personnel, or contracted, subcontracted, or co-
2 operating entity personnel, are found to have engaged in misconduct
3 or violated the rights of individuals in immigration detention;

4 (2) establish an accessible and standardized process regarding com-
5 plaints against an officer or employee of U.S. Customs and Border
6 Protection or U.S. Immigration and Customs Enforcement, or con-
7 tracted, subcontracted, or cooperating entity personnel, for violations of
8 law, standards of professional conduct, contract terms, or policy related
9 to immigration detention;

10 (3) conduct unannounced inspections of detention facilities holding
11 individuals in Federal immigration custody, including those owned or
12 operated by units of State or local government and privately-owned or
13 operated facilities;

14 (4) review, examine, and make recommendations to address concerns
15 or violations of contract terms identified in reviews, audits, investiga-
16 tions, or detainee interviews regarding immigration detention facilities
17 and services;

18 (5) provide assistance to individuals affected by potential mis-
19 conduct, excessive force, or violations of law or detention standards by
20 Department officers or other personnel, or contracted, subcontracted,
21 or cooperating entity personnel; and

22 (6) ensure that the functions performed by the Ombudsman are com-
23 plementary to existing functions in the Department.

24 (e) ACCESS TO DETENTION FACILITIES.—The Ombudsman or designated
25 personnel of the Ombudsman, shall be provided unfettered access to any lo-
26 cation in each detention facility and shall be permitted confidential access
27 to any detainee at the detainee's request and any departmental records con-
28 cerning the detainee.

29 (d) COORDINATION WITH DEPARTMENT COMPONENTS.—

30 (1) RESPONSES TO RECOMMENDATIONS OF OMBUDSMAN.—The Di-
31 rector of U.S. Immigration and Customs Enforcement and the Com-
32 missioner of U.S. Customs and Border Protection shall each establish
33 procedures to provide formal responses to recommendations submitted
34 to those officials by the Ombudsman within 60 days of receiving the
35 recommendations.

36 (2) ACCESS TO INFORMATION.—The Secretary shall establish proce-
37 dures to provide the Ombudsman access to all departmental records
38 necessary to execute the responsibilities of the Ombudsman under sub-
39 section (b) or (c) not later than 60 days after a request from the Om-
40 budsman for the information.

1 (e) ANNUAL REPORT.—The Ombudsman shall prepare a report to Con-
2 gress on an annual basis on its activities, findings, and recommendations.

3 **§ 10326. Counter Threats Advisory Board**

4 (a) ESTABLISHMENT.—There is authorized in the Department, for a pe-
5 riod of 2 years beginning after December 27, 2020, a Counter Threats Ad-
6 visory Board (in this section referred to as the “Board”) that shall—

7 (1) be composed of senior representatives of departmental oper-
8 ational components and headquarters elements; and

9 (2) coordinate departmental intelligence activities and policy and in-
10 formation related to the mission and functions of the Department that
11 counter threats.

12 (b) CHARTER.—There shall be a charter to govern the structure and mis-
13 sion of the Board that shall—

14 (1) direct the Board to focus on the current threat environment and
15 the importance of aligning departmental activities to counter threats
16 under the guidance of the Secretary; and

17 (2) be reviewed and updated as appropriate.

18 (c) MEMBERS.—

19 (1) IN GENERAL.—The Board shall be composed of senior represent-
20 atives of departmental operational components and headquarters ele-
21 ments.

22 (2) CHAIR.—The Under Secretary for Intelligence and Analysis shall
23 serve as the Chair of the Board.

24 (3) ADDITIONAL MEMBERS.—The Secretary shall appoint additional
25 members of the Board from among the following:

26 (A) The Transportation Security Administration.

27 (B) U.S. Customs and Border Protection.

28 (C) U.S. Immigration and Customs Enforcement.

29 (D) The Federal Emergency Management Agency.

30 (E) The Coast Guard.

31 (F) U.S. Citizenship and Immigration Services.

32 (G) The United States Secret Service.

33 (H) The Cybersecurity and Infrastructure Security Agency.

34 (I) The Office of Operations Coordination.

35 (J) The Office of the General Counsel.

36 (K) The Office of Intelligence and Analysis.

37 (L) The Office of Strategy, Policy, and Plans.

38 (M) The Science and Technology Directorate.

39 (N) The Office for State and Local Law Enforcement.

40 (O) The Privacy Office.

41 (P) The Office for Civil Rights and Civil Liberties.

1 (Q) Other departmental offices and programs as determined ap-
2 propriate by the Secretary.

3 (d) MEETINGS.—The Board shall—

4 (1) meet on a regular basis to discuss intelligence and coordinate on-
5 going threat mitigation efforts and departmental activities, including
6 coordination with other Federal, State, local, tribal, territorial, and pri-
7 vate-sector partners; and

8 (2) make recommendations to the Secretary.

9 (e) TERRORISM ALERTS.—The Board shall advise the Secretary on the
10 issuance of terrorism alerts under section 10504 of this title.

11 (f) PROHIBITION ON ADDITIONAL FUNDS.—No additional funds are au-
12 thorized to carry out this section.

13 **§ 10327. Economic security council**

14 (a) DEFINITIONS.—In this section

15 (1) COUNCIL.—The term “Council” means the council established
16 under subsection (b).

17 (2) ECONOMIC SECURITY.—The term “economic security” has the
18 meaning given the term in section 10405 of this title.

19 (b) ESTABLISHMENT.—In accordance with the mission of the Department
20 under section 10301(b) of this title, and in particular paragraph (1)(F) of
21 that section, the Secretary shall establish a standing council of Department
22 component heads or their designees to carry out the duties described in sub-
23 section (c).

24 (c) DUTIES.—Pursuant to the scope of the mission of the Department as
25 described in in subsection (b), the Council shall provide to the Secretary ad-
26 vice and recommendations on matters of economic security, including relat-
27 ing to the following:

28 (1) Identifying concentrated risks for trade and economic security.

29 (2) Setting priorities for securing the trade and economic security of
30 the United States.

31 (3) Coordinating Department-wide activity on trade and economic se-
32 curity matters.

33 (4) With respect to the development of the continuity of the eco-
34 nomic plan of the President under section 11327 of this title.

35 (5) Proposing statutory and regulatory changes impacting trade and
36 economic security.

37 (6) Any other matters the Secretary considers appropriate.

38 (d) CHAIR AND VICE CHAIR.—The Under Secretary for Strategy, Policy,
39 and Plans—

40 (1) shall serve as Chair of the Council; and

41 (2) may designate a Council member as a Vice Chair.

1 (e) MEETINGS.—The Council shall meet not less frequently than quar-
2 terly as well as—

3 (1) at the call of the Chair; or

4 (2) at the direction of the Secretary.

5 (f) BRIEFINGS.—Not less than 180 days after December 23, 2022, and
6 every 180 days thereafter for 4 years, the Council shall brief the Committee
7 on Homeland Security and Governmental Affairs of the Senate, the Com-
8 mittee on Homeland Security of the House of Representatives, the Com-
9 mittee on Finance of the Senate, the Committee on Ways and Means of the
10 House of Representatives, the Committee on Commerce, Science, and
11 Transportation of the Senate, and the Committee on Energy and Commerce
12 of the House of Representatives on the actions and activities of the Council.

13 **Subchapter II—Functions**

14 **§ 10341. In general**

15 (a) FUNCTIONS VESTED IN SECRETARY.—All functions of all officers,
16 employees, and organizational units of the Department are vested in the
17 Secretary.

18 (b) REORGANIZATION.—

19 (1) IN GENERAL.—The Secretary may allocate or reallocate func-
20 tions among the officers of the Department, and may establish, consoli-
21 date, alter, or discontinue organizational units within the Department,
22 but only after the expiration of 60 days after providing notice of the
23 action to the appropriate congressional committees, which shall include
24 an explanation of the rationale for the action.

25 (2) LIMITATION.—Authority under paragraph (1) does not extend to
26 the abolition of an agency, entity, organizational unit, program, or
27 function established or required to be maintained by statute.

28 (c) PERFORMANCE OF FUNCTIONS.—Subject to this subtitle, every officer
29 of the Department shall perform the functions specified by law for the offi-
30 cial's office or prescribed by the Secretary.

31 (d) REDELEGATION.—Unless otherwise provided in the delegation or by
32 law, a function delegated under this subtitle may be redelegated to a subor-
33 dinate.

34 (e) GENERAL FUNCTIONS OF SECRETARY.—The Secretary—

35 (1) except as otherwise provided by this subtitle, may delegate any
36 of the Secretary's functions to an officer, employee, or organizational
37 unit of the Department;

38 (2) shall have the authority to make contracts, grants, and coopera-
39 tive agreements, and to enter into agreements with other executive
40 agencies, as may be necessary and proper to carry out the Secretary's
41 responsibilities under this subtitle or as otherwise provided by law;

1 (3) shall take reasonable steps to ensure that information systems
2 and databases of the Department are compatible with each other and
3 with appropriate databases of other Departments;

4 (4) shall ensure that there is effective and ongoing coordination of
5 Federal efforts to prevent, prepare for, and respond to acts of ter-
6 rorism and other major disasters and emergencies among the divisions
7 of the Department, including the Office for State and Local Govern-
8 ment Coordination;

9 (5) shall ensure that the Department complies with the protections
10 for human research subjects, as described in part 46 of title 45, Code
11 of Federal Regulations, or in equivalent regulations as promulgated by
12 the Secretary, with respect to research that is conducted or supported
13 by the Department; and

14 (6) has the same authorities that the Secretary of Transportation
15 has with respect to the Department of Transportation under section
16 324 of title 49.

17 (f) REGULATORY AUTHORITY.—

18 (1) VESTING AND TRANSFER OF AUTHORITY.—Except as otherwise
19 provided in sections 10622(c) and 10905(c) of this title and section
20 1315(c) of title 40, this subtitle—

21 (A) does not vest new regulatory authority in the Secretary or
22 another Federal official; and

23 (B) transfers to the Secretary or another Federal official only
24 the regulatory authority that—

25 (i) existed on November 25, 2002, in an agency, program,
26 or function transferred to the Department pursuant to the
27 Homeland Security Act of 2002 (Public Law 107–296, 116
28 Stat. 2135); or

29 (ii) on November 25, 2002, was exercised by another offi-
30 cial of the executive branch with respect to the transferred
31 agency, program, or function.

32 (2) RESTRICTION ON EXERCISE OF TRANSFERRED AUTHORITY.—
33 Transferred authority may not be exercised by an official from whom
34 it is transferred on transfer of the agency, program, or function to the
35 Secretary or another Federal official pursuant to the Homeland Secu-
36 rity Act of 2002 (Public Law 107–296, 116 Stat. 2135).

37 (3) ALTERATION OR DIMINUTION OF AUTHORITY.—The Homeland
38 Security Act of 2002 (Public Law 107–296, 116 Stat. 2135) may not
39 be construed as altering or diminishing the regulatory authority of an-
40 other executive agency, except to the extent that the Act transfers the
41 authority from the agency.

1 (g) PREEMPTION OF STATE OR LOCAL LAW.—Except as otherwise pro-
2 vided in this subtitle, this subtitle preempts no State or local law, except
3 that authority to preempt State or local law vested in a Federal agency or
4 official transferred to the Department pursuant to the Homeland Security
5 Act of 2002 (Public Law 107–296, 116 Stat. 2135) shall be transferred to
6 the Department, effective on the date of the transfer to the Department of
7 that Federal agency or official.

8 (h) COORDINATION WITH NON-FEDERAL ENTITIES.—With respect to
9 homeland security, the Secretary shall coordinate through the Office for
10 State and Local Government Coordination (including the provision of train-
11 ing and equipment) with State and local government personnel, agencies,
12 and authorities, with the private sector, and with other entities, including
13 by—

14 (1) coordinating with State and local government personnel, agen-
15 cies, and authorities, and with the private sector, to ensure adequate
16 planning, equipment, training, and exercise activities;

17 (2) coordinating and, as appropriate, consolidating, the Federal Gov-
18 ernment’s communications and systems of communications relating to
19 homeland security with State and local government personnel, agencies,
20 and authorities, the private sector, other entities, and the public; and

21 (3) distributing or, as appropriate, coordinating the distribution of
22 warnings and information to State and local government personnel,
23 agencies, and authorities, and to the public.

24 (i) MEETINGS OF NATIONAL SECURITY COUNCIL.—The Secretary may,
25 subject to the direction of the President, attend and participate in meetings
26 of the National Security Council.

27 (j) ISSUANCE OF REGULATIONS.—The issuance of regulations by the Sec-
28 retary shall be governed by chapter 5 of title 5, except as specifically pro-
29 vided in this subtitle, by laws granting regulatory authorities that are trans-
30 ferred by this subtitle, and by laws enacted after November 25, 2002.

31 (k) STANDARDS POLICY.—All standards activities of the Department
32 shall be conducted in accordance with section 12(d) of the National Tech-
33 nology Transfer and Advancement Act of 1995 (15 U.S.C. 272 note) and
34 Office of Management and Budget Circular A-119.

35 (l) PLANNING REQUIREMENTS.—The Secretary shall ensure the head of
36 each office and component of the Department takes into account the needs
37 of children, including children in under-served communities, in mission plan-
38 ning and mission execution. In furtherance of this subsection, the Secretary
39 shall require each office and component head to seek, to the extent prac-
40 ticable, advice and feedback from organizations representing the needs of

1 children. Chapter 10 of title 5 shall not apply whenever advice or feedback
2 is sought in accordance with this subsection.

3 **§ 10342. Trade and customs revenue functions**

4 (a) SUBTITLE III DEFINITIONS APPLY.—A term used in this section that
5 is defined in section 30101 of this title has the meaning given the term in
6 section 30101.

7 (b) TRADE AND CUSTOMS REVENUE FUNCTIONS.—

8 (1) DESIGNATION OF APPROPRIATE OFFICIAL.—The Secretary shall
9 designate an appropriate senior official in the Office of the Secretary
10 who shall—

11 (A) ensure that the trade and customs revenue functions of the
12 Department are coordinated within the Department and with
13 other Federal departments and agencies, and that the impact on
14 legitimate trade is taken into account in an action impacting the
15 functions; and

16 (B) monitor and report to Congress on the Department man-
17 date to ensure that the trade and customs revenue functions of the
18 Department are not diminished, including how spending, oper-
19 ations, and personnel related to these functions have kept pace
20 with the level of trade entering the United States.

21 (2) DIRECTOR OF TRADE POLICY.—There is in the Department a Di-
22 rector of Trade Policy (in this subsection referred to as the “Direc-
23 tor”), who shall be subject to the direction and control of the official
24 designated under paragraph (1). The Director shall—

25 (A) advise the official designated under paragraph (1) regarding
26 all aspects of Department policies relating to the trade and cus-
27 toms revenue functions of the Department;

28 (B) coordinate the development of Department-wide policies re-
29 garding trade and customs revenue functions and trade facilita-
30 tion; and

31 (C) coordinate the trade and customs revenue-related policies of
32 the Department with the policies of other Federal departments
33 and agencies.

34 (c) CONSULTATION ON TRADE AND CUSTOMS REVENUE FUNCTIONS.—

35 (1) BUSINESS COMMUNITY CONSULTATIONS.—The Secretary shall
36 consult with representatives of the business community involved in
37 international trade, including seeking the advice and recommendations
38 of the Commercial Customs Operations Advisory Committee, on De-
39 partment policies and actions that have a significant impact on inter-
40 national trade and customs revenue functions.

41 (2) CONGRESSIONAL NOTIFICATION.—

1 (A) IN GENERAL.—Subject to subparagraph (B), the Secretary
2 shall notify the appropriate congressional committees not later
3 than 30 days prior to the finalization of Department policies, ini-
4 tiatives, or actions that will have a major impact on trade and cus-
5 toms revenue functions. The notifications shall include a descrip-
6 tion of the proposed policies, initiatives, or actions and any com-
7 ments or recommendations provided by the Commercial Customs
8 Operations Advisory Committee and other relevant groups regard-
9 ing the proposed policies, initiatives, or actions.

10 (B) EXCEPTION.—If the Secretary determines that it is impor-
11 tant to the national security interest of the United States to final-
12 ize any Department policies, initiatives, or actions prior to the no-
13 tification described in subparagraph (A), the Secretary shall—

14 (i) notify and provide any recommendations of the Com-
15 mercial Customs Operations Advisory Committee received to
16 the appropriate congressional committees not later than 45
17 days after the date on which the policies, initiatives, or ac-
18 tions are finalized; and

19 (ii) to the extent appropriate, modify the policies, initia-
20 tives, or actions based upon the consultations with the appro-
21 priate congressional committees.

22 (d) NOTIFICATION OF REORGANIZATION OF CUSTOMS REVENUE FUNC-
23 TIONS.—

24 (1) IN GENERAL.—Not less than 45 days prior to a change in the
25 organization of any of the customs revenue functions of the Depart-
26 ment, the Secretary shall notify the Committee on Appropriations, the
27 Committee on Finance, and the Committee on Homeland Security and
28 Governmental Affairs of the Senate, and the Committee on Appropria-
29 tions, the Committee on Homeland Security, and the Committee on
30 Ways and Means of the House of Representatives of the specific assets,
31 functions, or personnel to be transferred as part of the reorganization,
32 and the reason for the transfer. The notification shall also include—

33 (A) an explanation of how trade enforcement functions will be
34 impacted by the reorganization;

35 (B) an explanation of how the reorganization meets the require-
36 ments of section 11132(b) of this title that the Department not
37 diminish the customs revenue and trade facilitation functions for-
38 merly performed by the United States Customs Service; and

39 (C) any comments or recommendations provided by the Com-
40 mercial Customs Operations Advisory Committee regarding the re-
41 organization.

1 (2) ANALYSIS.—A congressional committee referred to in paragraph
2 (1) may request that the Commercial Customs Operations Advisory
3 Committee provide a report to the committee analyzing the impact of
4 the reorganization and providing any recommendations for modifying
5 the reorganization.

6 (3) REPORT.—Not later than 1 year after a reorganization referred
7 to in paragraph (1) takes place, the Secretary, in consultation with the
8 Commercial Customs Operations Advisory Committee, shall submit a
9 report to the Committee on Finance of the Senate and the Committee
10 on Ways and Means of the House of Representatives. The report shall
11 include an assessment of the impact of, and any suggested modifica-
12 tions to, the reorganization.

13 **§ 10343. Military activities**

14 Nothing in this subtitle shall confer upon the Secretary authority to en-
15 gage in warfighting, the military defense of the United States, or other mili-
16 tary activities, nor shall anything in this subtitle limit the existing authority
17 of the Department of Defense or the armed forces to engage in warfighting,
18 the military defense of the United States, or other military activities.

19 **§ 10344. Sensitive Security Information**

20 (a) IN GENERAL.—The Secretary shall provide that each office in the De-
21 partment that handles documents marked as Sensitive Security Information
22 (in this section referred to as “SSI”) has at least 1 employee with authority
23 to coordinate and make determinations on behalf of the Department that
24 the documents meet the criteria for marking as SSI.

25 (b) REPORT.—The Secretary shall, not later than January 31 each year,
26 provide a report to the Committees on Appropriations of the Senate and the
27 House of Representatives on the titles of all Department documents that
28 are designated as SSI in their entirety during the period of January 1
29 through December 31 for the preceding year.

30 (c) GUIDANCE ON INDIVIDUAL CATEGORIES OF SSI INFORMATION.—

31 (1) IN GENERAL.—The Secretary shall promulgate guidance that in-
32 cludes common but extensive examples of SSI that further define the
33 individual categories of information cited under 49 CFR 1520(b)(1)
34 through (16) and that eliminates judgment by covered individuals in
35 the application of the SSI marking.

36 (2) PURPOSE OF GUIDANCE.—The guidance shall serve as the pri-
37 mary basis and authority for the marking of Departmental information
38 as SSI by covered individuals.

39 **§ 10345. Daily public report of covered contract awards**

40 (a) DEFINITIONS.—In this section:

1 (1) COVERED CONTRACT AWARD.—The term “covered contract
2 award”—

3 (A) means a contract action of the Department with a total con-
4 tract value of not less than \$4,000,000, including unexercised op-
5 tions; and

6 (B) includes—

7 (i) contract awards covered by the Federal
8 Acquisition Regulation;

9 (ii) modifications to a contract award that increase the
10 total value, increase the scope of work, or extend the period
11 of performance;

12 (iii) orders placed on a multiple-award or multiple-agency
13 contract that includes delivery or quantity terms that are in-
14 definite;

15 (iv) other transaction authority agreements; and

16 (v) contract awards made with other than full and open
17 competition.

18 (2) DEFINITIZED AMOUNT.—The term “definitized amount” means
19 the final amount of a covered contract award after agreement between
20 the Department and the contractor at issue.

21 (3) SMALL BUSINESS.—The term “small business” means an entity
22 that qualifies as a small business concern, as defined under section 3
23 of the Small Business Act (15 U.S.C. 632).

24 (4) TOTAL CONTRACT VALUE.—The term “total contract value”
25 means the total amount of funds expected to be provided to the con-
26 tractor at issue under the terms of the contract through the full period
27 of performance.

28 (5) UNDEFINITIZED CONTRACT ACTION.—The term “undefinitized
29 contract action” means any contract action for which the contract
30 terms, specifications, or price is not established prior to the start of
31 the performance of the covered contract award.

32 (b) DAILY CONTRACT REPORTING REQUIREMENTS.—

33 (1) REPORT.—

34 (A) IN GENERAL.—The Secretary shall post, maintain, and up-
35 date in accordance with paragraph (2) on a publicly available
36 website of the Department a daily report of all covered contract
37 awards.

38 (B) Contents.—Each report under this paragraph shall include
39 for each covered contract award information relating to the fol-
40 lowing:

- 1 (i) The contract number, modification number, or delivery
- 2 order number.
- 3 (ii) The contract type.
- 4 (iii) The amount obligated for the award.
- 5 (iv) The total contract value for the award, including all
- 6 options.
- 7 (v) The description of the purpose for the award.
- 8 (vi) The number of proposals or bids received.
- 9 (vii) The name and address of the vendor and whether the
- 10 vendor is a small business.
- 11 (viii) The period and primary place of performance for the
- 12 award.
- 13 (ix) Whether the award is multiyear.
- 14 (x) The contracting office.

15 (2) UPDATE.—The Secretary shall make updates referred to in para-

16 graph (1) not later than 5 business days after the date on which a cov-

17 ered contract is authorized or modified.

18 (3) EFFECTIVE DATE.—Paragraph (1) shall take effect on the date

19 that is 180 days after December 23, 2022.

20 (c) UNDEFINITIZED CONTRACT ACTION OR DEFINITIZED AMOUNT.—If a

21 covered contract amount reported under subsection (b) contains an

22 undefinitized contract action, the Secretary shall—

23 (1) report the estimated total contract value for the award and the

24 amount obligated on award; and

25 (2) once there is a definitized amount for the award, update the total

26 contract value and the amount obligated.

27 (d) EXEMPTION.—Each report required under subsection (a) shall not in-

28 clude covered contract awards for which synopses were exempted under sec-

29 tion 5.202(a)(1) of the Federal Acquisition Regulation, or any successor to

30 the Regulation.

31 (e) TERMINATION.—This section shall cease to have force and effect on

32 December 23, 2027.

33 **Subchapter III—Acquisitions**

34 **§ 10351. Personal services**

35 The Secretary—

36 (1) may procure the temporary or intermittent services of experts or

37 consultants (or organizations thereof) under section 3109 of title 5;

38 and

39 (2) may, whenever necessary due to an urgent homeland security

40 need, procure temporary (not to exceed 1 year) or intermittent personal

1 services, including the services of experts or consultants (or organiza-
2 tions thereof), without regard to the pay limitations of section 3109.

3 **§ 10352. Prohibition on contracts with corporate expatriates**

4 (a) DEFINITIONS AND SPECIAL RULES.—

5 (1) DEFINITIONS.—In this section:

6 (A) DOMESTIC.—The term “domestic” has the meaning given
7 the term in section 7701(a)(4) of the Internal Revenue Code of
8 1986 (26 U.S.C. 7701(a)(4)).

9 (B) EXPANDED AFFILIATED GROUP.—The term “expanded af-
10 filiated group” means an affiliated group as defined in section
11 1504(a) of the Internal Revenue Code of 1986 (26 U.S.C.
12 1504(a)) (without regard to section 1504(b) of the Code (26
13 U.S.C. 1504(b))), except that section 1504 of the Code (26 U.S.C.
14 1504) shall be applied by substituting “more than 50 percent” for
15 “at least 80 percent” each place it appears.

16 (C) FOREIGN.—The term “foreign” has the meaning given the
17 term in section 7701(a)(5) of the Internal Revenue Code of 1986
18 (26 U.S.C. 7701(a)(5)).

19 (D) FOREIGN INCORPORATED ENTITY.—The term “foreign in-
20 corporated entity” means an entity that is, or but for subsection
21 (c) would be, treated as a foreign corporation for purposes of the
22 Internal Revenue Code of 1986 (26 U.S.C. 1 et seq.).

23 (E) PERSON.—The term “person” has the meaning given the
24 term in section 7701(a)(1) of the Internal Revenue Code of 1986
25 (26 U.S.C. 7701(a)(1)).

26 (2) RULES FOR APPLICATION OF SUBSECTION (C).—In applying sub-
27 section (c) for purposes of subsection (b), the following rules apply:

28 (A) CERTAIN STOCK DISREGARDED.—There shall not be taken
29 into account in determining ownership for purposes of subsection
30 (c)(2)—

31 (i) stock held by members of the expanded affiliated group
32 which includes the foreign incorporated entity; or

33 (ii) stock of the entity which is sold in a public offering re-
34 lated to the acquisition described in subsection (c)(1).

35 (B) PLAN DEEMED IN CERTAIN CASES.—If a foreign incor-
36 porated entity acquires directly or indirectly substantially all of the
37 properties of a domestic corporation or partnership during the 4-
38 year period beginning on the date which is 2 years before the own-
39 ership requirements of subsection (c)(2) are met, these actions
40 shall be treated as pursuant to a plan.

1 (C) CERTAIN TRANSFERS DISREGARDED.—The transfer of prop-
2 erties or liabilities (including by contribution or distribution) shall
3 be disregarded if the transfers are part of a plan a principal pur-
4 pose of which is to avoid the purposes of this section.

5 (D) SPECIAL RULE FOR RELATED PARTNERSHIPS.—For pur-
6 poses of applying subsection (c) to the acquisition of a domestic
7 partnership, except as provided in regulations, all domestic part-
8 nerships that are under common control (within the meaning of
9 section 482 of the Internal Revenue Code of 1986 (26 U.S.C.
10 482)) shall be treated as one partnership.

11 (E) TREATMENT OF CERTAIN RIGHTS.—The Secretary shall
12 prescribe regulations necessary to—

13 (i) treat warrants, options, contracts to acquire stock, con-
14 vertible debt instruments, and other similar interests as stock;
15 and

16 (ii) treat stock as not stock.

17 (b) IN GENERAL.—The Secretary may not enter into a contract with a
18 foreign incorporated entity that is treated as an inverted domestic corpora-
19 tion under subsection (c), or with a subsidiary of the entity.

20 (c) INVERTED DOMESTIC CORPORATION.—For purposes of this section,
21 a foreign incorporated entity shall be treated as an inverted domestic cor-
22 poration if, pursuant to a plan (or a series of related transactions)—

23 (1) the entity completes before, on, or after November 25, 2002, the
24 direct or indirect acquisition of substantially all of the properties held
25 directly or indirectly by a domestic corporation or substantially all of
26 the properties constituting a trade or business of a domestic partner-
27 ship;

28 (2) after the acquisition at least 80 percent of the stock (by vote or
29 value) of the entity is held—

30 (A) in the case of an acquisition with respect to a domestic cor-
31 poration, by former shareholders of the domestic corporation by
32 reason of holding stock in the domestic corporation; or

33 (B) in the case of an acquisition with respect to a domestic
34 partnership, by former partners of the domestic partnership by
35 reason of holding a capital or profits interest in the domestic part-
36 nership; and

37 (3) the expanded affiliated group which after the acquisition includes
38 the entity does not have substantial business activities in the foreign
39 country in which or under the law of which the entity is created or or-
40 ganized when compared to the total business activities of the expanded
41 affiliated group.

1 (d) WAIVERS.—The Secretary shall waive subsection (b) with respect to
2 a specific contract if the Secretary determines that the waiver is required
3 in the interest of national security.

4 **§ 10353. Lead system integrator; financial interests**

5 (a) IN GENERAL.—With respect to contracts entered into after July 1,
6 2007, and except as provided in subsection (b), no entity performing lead
7 system integrator functions in the acquisition of a major system by the De-
8 partment may have a direct financial interest in the development or con-
9 struction of an individual system or element of a system of systems.

10 (b) EXCEPTION.—An entity described in subsection (a) may have a direct
11 financial interest in the development or construction of an individual system
12 or element of a system of systems if—

13 (1) the Secretary certifies to the Committees on Appropriations of
14 the Senate and the House of Representatives, the Committee on Home-
15 land Security of the House of Representatives, the Committee on
16 Transportation and Infrastructure of the House of Representatives, the
17 Committee on Homeland Security and Governmental Affairs of the
18 Senate, and the Committee on Commerce, Science and Transportation
19 of the Senate that—

20 (A) the entity was selected by the Department as a contractor
21 to develop or construct the system or element concerned through
22 the use of competitive procedures; and

23 (B) the Department took appropriate steps to prevent an orga-
24 nizational conflict of interest in the selection process; or

25 (2) the entity was selected by a subcontractor to serve as a lower-
26 tier subcontractor, through a process over which the entity exercised
27 no control.

28 (c) CONSTRUCTION.—Nothing in this section shall be construed to pre-
29 clude an entity described in subsection (a) from performing work necessary
30 to integrate two or more individual systems or elements of a system of sys-
31 tems with each other.

32 (d) REGULATIONS UPDATE.—The Secretary shall update the acquisition
33 regulations of the Department to specify fully in the regulations the matters
34 with respect to lead system integrators set forth in this section. The regula-
35 tions shall include—

36 (1) a precise and comprehensive definition of the term “lead system
37 integrator”, modeled after that used by the Department of Defense;
38 and

39 (2) a specification of various types of contracts and fee structures
40 that are appropriate for use by lead system integrators in the produc-
41 tion, fielding, and sustainment of complex systems.

1 **§ 10354. Requirements to buy certain items related to na-**
2 **tional security interests**

3 (a) DEFINITIONS.—In this section:

4 (1) COVERED ITEM.—The term “covered item” means any of the fol-
5 lowing:

6 (A) Footwear provided as part of a uniform.

7 (B) Uniforms.

8 (C) Holsters and tactical pouches.

9 (D) Patches, insignia, and embellishments.

10 (E) Chemical, biological, radiological, and nuclear protective
11 gear.

12 (F) Body armor components intended to provide ballistic protec-
13 tion for an individual, consisting of 1 or more of the following:

14 (i) Soft ballistic panels.

15 (ii) Hard ballistic plates.

16 (iii) Concealed armor carriers worn under a uniform.

17 (iv) External armor carriers worn over a uniform.

18 (G) Any other item of clothing or protective equipment as deter-
19 mined appropriate by the Secretary.

20 (2) FRONTLINE OPERATIONAL COMPONENT.—The term “frontline
21 operational component” means any of the following entities of the De-
22 partment:

23 (A) U.S. Customs and Border Protection.

24 (B) U.S. Immigration and Customs Enforcement.

25 (C) The United States Secret Service.

26 (D) The Transportation Security Administration.

27 (E) The Federal Protective Service.

28 (F) The Federal Emergency Management Agency.

29 (G) The Federal Law Enforcement Training Centers.

30 (H) The Cybersecurity and Infrastructure Security Agency.

31 (b) REQUIREMENTS.—

32 (1) IN GENERAL.—The Secretary shall ensure that any procurement
33 of a covered item for a frontline operational component meets the fol-
34 lowing criteria:

35 (A)(i) To the maximum extent possible, not less than 1/3 of
36 funds obligated in a specific fiscal year for the procurement of the
37 covered items shall be covered items that are manufactured or
38 supplied in the United States by entities that qualify as small
39 business concerns, as that term is described under section 3 of the
40 Small Business Act (15 U.S.C. 632).

1 (ii) Covered items may only be supplied pursuant to clause (i)
2 to the extent that United States entities that qualify as small busi-
3 ness concerns—

4 (I) are unable to manufacture covered items in the United
5 States; and

6 (II) meet the criteria identified in subparagraph (B).

7 (B) Each contractor with respect to the procurement of a cov-
8 ered item, including the end-item manufacturer of a covered
9 item—

10 (i) is an entity registered with the System for Award Man-
11 agement (or successor system) administered by the General
12 Services Administration; and

13 (ii) is in compliance with ISO 9001:2015 of the Inter-
14 national Organization for Standardization (or successor
15 standard) or a standard determined appropriate by the Sec-
16 retary to ensure the quality of products and adherence to ap-
17 plicable statutory and regulatory requirements.

18 (C) Each supplier of a covered item with an insignia (such as
19 any patch, badge, or emblem) and each supplier of the insignia,
20 if the covered item with the insignia or the insignia, as the case
21 may be, is not produced, applied, or assembled in the United
22 States, shall—

23 (i) store the covered item with the insignia or the insignia
24 in a locked area;

25 (ii) report any pilferage or theft of the covered item with
26 the insignia or the insignia occurring at any stage before de-
27 livery of the covered item with the insignia or the insignia;
28 and

29 (iii) destroy any defective or unusable covered item with in-
30 signia or insignia in a manner established by the Secretary,
31 and maintain records, for 3 years after the creation of the
32 records, of the destruction that include the date of the de-
33 struction, a description of the covered item with insignia or
34 insignia destroyed, the quantity of the covered item with in-
35 signia or insignia destroyed, and the method of destruction.

36 (2) WAIVER.—

37 (A) IN GENERAL.—In the case of a national emergency declared
38 by the President under the National Emergencies Act (50 U.S.C.
39 1601 et seq.) or a major disaster declared by the President under
40 section 401 of the Robert T. Stafford Disaster Relief and Emer-
41 gency Assistance Act (42 U.S.C. 5170), the Secretary may waive

1 a requirement in subparagraph (A), (B) or (C) of paragraph (1)
2 if the Secretary determines there is an insufficient supply of a cov-
3 ered item that meets the requirement.

4 (B) NOTICE.— Not later than 60 days after the date on which
5 the Secretary determines a waiver under subparagraph (A) is nec-
6 essary, the Secretary shall provide to the Committee on Homeland
7 Security and Governmental Affairs and the Committee on Appro-
8 priations of the Senate and the Committee on Homeland Security,
9 the Committee on Oversight and Reform, and the Committee on
10 Appropriations of the House of Representatives notice of the de-
11 termination, which shall include the following:

12 (i) Identification of the national emergency or major dis-
13 aster declared by the President.

14 (ii) Identification of the covered item for which the Sec-
15 retary intends to issue the waiver.

16 (iii) A description of the demand for the covered item and
17 corresponding lack of supply from contractors able to meet
18 the criteria described in subparagraph (B) or (C) of para-
19 graph (1).

20 (c) PRICING.— The Secretary shall ensure that covered items are pur-
21 chased at a fair and reasonable price, consistent with the procedures and
22 guidelines specified in the Federal Acquisition Regulation.

23 (d) REPORT.—Not later than December 23, 2023, and annually there-
24 after, the Secretary shall provide to the Committee on Homeland Security,
25 the Committee on Oversight and Reform, the Committee on Small Business,
26 and the Committee on Appropriations of the House of Representatives, and
27 the Committee on Homeland Security and Governmental Affairs, the Com-
28 mittee on Small Business and Entrepreneurship, and the Committee on Ap-
29 propriations of the Senate a briefing on instances in which vendors have
30 failed to meet deadlines for delivery of covered items and corrective actions
31 taken by the Department in response to those instances.

32 (e) EFFECTIVE DATE.—This section applies with respect to a contract
33 entered into by the Department or any frontline operational component on
34 or after the date that is 180 days after December 23, 2022.

35 **Subchapter IV—Human Resources** 36 **Management**

37 **§ 10361. Establishment of human resources management** 38 **system**

39 (a) POSITIONS COMPENSATED IN ACCORDANCE WITH EXECUTIVE
40 SCHEDULE.—An individual who, on the day preceding the individual's date
41 of transfer pursuant to the Homeland Security Act of 2002 (Public Law

1 107–296, 116 Stat. 2135), held a position compensated in accordance with
2 the Executive Schedule prescribed in chapter 53 of title 5, and who, without
3 a break in service, is appointed in the Department to a position having du-
4 ties comparable to the duties performed immediately preceding the appoint-
5 ment shall continue to be compensated in the new position at not less than
6 the rate provided for the former position, for the duration of the service of
7 the individual in the new position.

8 (b) COORDINATION RULE.—An exercise of authority under chapter 97 of
9 title 5, including under a system established under that chapter, shall be
10 in conformance with the requirements of this section.

11 **§ 10362. Labor-management relations**

12 (a) LIMITATION ON EXCLUSIONARY AUTHORITY.—

13 (1) IN GENERAL.—An agency or subdivision of an agency transferred
14 to the Department pursuant to the Homeland Security Act of 2002
15 (Public Law 107–296, 116 Stat. 2135) shall not be excluded from the
16 coverage of chapter 71 of title 5, as a result of an order issued under
17 section 7103(b)(1) of title 5 after June 18, 2002, unless—

18 (A) the mission and responsibilities of the agency (or subdivi-
19 sion) materially change; and

20 (B) a majority of the employees in the agency (or subdivision)
21 have as their primary duty intelligence, counterintelligence, or in-
22 vestigative work directly related to terrorism investigation.

23 (2) EXCLUSIONS ALLOWABLE.—Nothing in paragraph (1) shall af-
24 fect the effectiveness of an order to the extent that the order excludes
25 a portion of an agency or subdivision of an agency as to which—

26 (A) recognition as an appropriate unit has never been conferred
27 for purposes of chapter 71 of title 5; or

28 (B) recognition has been revoked or otherwise terminated as a
29 result of a determination under subsection (b)(1).

30 (b) PROVISIONS RELATING TO BARGAINING UNITS.—

31 (1) LIMITATION RELATING TO APPROPRIATE UNITS.—Each unit rec-
32 ognized as an appropriate unit for purposes of chapter 71 of title 5,
33 as of January 23, 2003 (and a subdivision of a unit), shall, if the unit
34 (or subdivision) is transferred to the Department pursuant to the
35 Homeland Security Act of 2002 (Public Law 107–296, 116 Stat.
36 2135), continue to be so recognized for those purposes, unless—

37 (A) the mission and responsibilities of the unit (or subdivision)
38 materially change; and

39 (B) a majority of the employees within the unit (or subdivision)
40 have as their primary duty intelligence, counterintelligence, or in-
41 vestigative work directly related to terrorism investigation.

1 (2) LIMITATION RELATING TO POSITIONS OR EMPLOYEES.—A posi-
2 tion or employee within a unit (or subdivision of a unit) as to which
3 continued recognition is given under paragraph (1) shall not be ex-
4 cluded from the unit (or subdivision), for purposes of chapter 71 of
5 title 5, unless the primary job duty of the position or employee—

6 (A) consists of intelligence, counterintelligence, or investigative
7 work directly related to terrorism investigation; and

8 (B) materially changes (in the case of a position within a unit
9 (or subdivision) that is first established before January 24, 2003,
10 or to which the employee is first appointed before that date).

11 (c) WAIVER.—If the President determines that the application of sub-
12 sections (a), (b), and (d) would have a substantial adverse impact on the
13 ability of the Department to protect homeland security, the President may
14 waive the application of the subsections 10 days after the President has sub-
15 mitted to Congress a written explanation of the reasons for the determina-
16 tion.

17 (d) COORDINATION RULE.—No other provision of this subtitle or the
18 Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2135), or
19 of an amendment made by the Act, may be construed or applied in a man-
20 ner so as to limit, supersede, or otherwise affect this section, except to the
21 extent that it does so by specific reference to this section.

22 (e) RULE OF CONSTRUCTION.—Nothing in section 9701(e) of title 5 shall
23 be considered to apply with respect to an agency or subdivision of an agency
24 that is excluded from the coverage of chapter 71 of title 5 by virtue of an
25 order issued under section 7103(b) of the title and the preceding provisions
26 of this section (as applicable), or to an employee of the agency or subdivi-
27 sion or to an individual or entity representing the employees or representa-
28 tives thereof.

29 **§ 10363. Use of counternarcotics enforcement activities in**
30 **certain employee performance appraisals**

31 (a) DEFINITIONS.—In this section:

32 (1) NATIONAL DRUG CONTROL PROGRAM AGENCY.—The term “Na-
33 tional Drug Control Program Agency” means—

34 (A) a National Drug Control Program Agency, as defined in
35 section 702 of the Office of National Drug Control Policy Reau-
36 thorization Act of 1998 (21 U.S.C. 1701); and

37 (B) a subdivision of the Department that has a significant coun-
38 ternarcotics responsibility, as determined by—

39 (i) the Director of the Office of Counternarcotics Enforce-
40 ment; or

1 (ii) if applicable, the counternarcotics officer's successor in
2 function (as determined by the Secretary).

3 (2) PERFORMANCE APPRAISAL SYSTEM.—The term “performance
4 appraisal system” means a system under which periodic appraisals of
5 job performance of employees are made, whether under chapter 43 of
6 title 5, or otherwise.

7 (b) IN GENERAL.—Each subdivision of the Department that is a National
8 Drug Control Program Agency shall include as one of the criteria in its per-
9 formance appraisal system, for each employee directly or indirectly involved
10 in the enforcement of Federal, State, or local narcotics laws, the perform-
11 ance of that employee with respect to the enforcement of Federal, State, or
12 local narcotics laws, relying to the greatest extent practicable on objective
13 performance measures, including—

14 (1) the contribution of that employee to seizures of narcotics and ar-
15 rests of violators of Federal, State, or local narcotics laws; and

16 (2) the degree to which that employee cooperated with or contributed
17 to the efforts of other employees, either in the Department or other
18 Federal, State, or local agencies, in counternarcotics enforcement.

19 **§ 10364. Compliance with laws protecting equal employment**
20 **opportunity and providing whistleblower protec-**
21 **tions**

22 Nothing in this subtitle shall be construed as exempting the Department
23 from requirements applicable with respect to executive agencies—

24 (1) to provide equal employment protection for employees of the De-
25 partment (including under section 2302(b)(1) of title 5 and the Notifi-
26 cation and Federal Employee Antidiscrimination and Retaliation Act of
27 2002 (Public Law 107–174, 5 U.S.C. 2301 note)); or

28 (2) to provide whistleblower protections for employees of the Depart-
29 ment (including under paragraphs (8) and (9) of section 2302(b) of
30 title 5 and the Notification and Federal Employee Antidiscrimination
31 and Retaliation Act of 2002 (Public Law 107–174, 5 U.S.C. 2301
32 note)).

33 **§ 10365. Use of protective equipment or measures by em-**
34 **ployees**

35 No funds may be used to propose or effect a disciplinary or adverse ac-
36 tion, with respect to any Department employee who engages regularly with
37 the public in the performance of his or her official duties, solely because
38 that employee elects to utilize protective equipment or measures, including
39 surgical masks, N95 respirators, gloves, or hand-sanitizers, where use of the
40 equipment or measures is in accord with Department policy, and Centers

1 for Disease Control and Prevention and Office of Personnel Management
2 guidance.

3 **§ 10366. Homeland Security Rotation Program**

4 (a) ESTABLISHMENT.—The Secretary shall establish the Homeland Security
5 Rotation Program (in this section referred to as the “Rotation Program”) for employees of the Department. The Rotation Program shall use
6 applicable best practices, including those from the Chief Human Capital Officers Council.
7
8

9 (b) GOALS.—The Rotation Program established by the Secretary shall—

10 (1) be established in accordance with the Human Capital Strategic
11 Plan of the Department;

12 (2) provide middle and senior level employees in the Department the
13 opportunity to broaden their knowledge through exposure to other components of the Department;
14

15 (3) expand the knowledge base of the Department by providing for
16 rotational assignments of employees to other components;

17 (4) build professional relationships and contacts among the employees in the Department;
18

19 (5) invigorate the workforce with exciting and professionally rewarding opportunities;
20

21 (6) incorporate Department human capital strategic plans and activities, and address critical human capital deficiencies, recruitment and retention efforts, and succession planning in the Federal workforce of the Department; and
22
23
24

25 (7) complement and incorporate (but not replace) rotational programs in the Department in effect on October 4, 2006.
26

27 (c) ADMINISTRATION.—

28 (1) IN GENERAL.—The Chief Human Capital Officer shall administer the Rotation Program.
29

30 (2) RESPONSIBILITIES.—The Chief Human Capital Officer shall—

31 (A) provide oversight of the establishment and implementation of the Rotation Program;
32

33 (B) establish a framework that supports the goals of the Rotation Program and promotes cross-disciplinary rotational opportunities;
34
35

36 (C) establish eligibility for employees to participate in the Rotation Program and select participants from employees who apply;
37

38 (D) establish incentives for employees to participate in the Rotation Program, including promotions and employment preferences;
39
40

1 (E) ensure that the Rotation Program provides professional
2 education and training;

3 (F) ensure that the Rotation Program develops qualified em-
4 ployees and future leaders with broad-based experience throughout
5 the Department;

6 (G) provide for greater interaction among employees in compo-
7 nents of the Department; and

8 (H) coordinate with rotational programs in the Department in
9 effect on October 4, 2006.

10 (d) ALLOWANCES, PRIVILEGES, AND BENEFITS.—All allowances, privi-
11 leges, rights, seniority, and other benefits of employees participating in the
12 Rotation Program shall be preserved.

13 **§ 10367. Rotational cybersecurity research program**

14 To enhance the Department's cybersecurity capacity, the Secretary may
15 establish a rotational research, development, and training program for—

16 (1) detail to the Cybersecurity and Infrastructure Security Agency
17 (including the National Cybersecurity and Communications Integration
18 Center authorized by section 10706 of this title) of Coast Guard Acad-
19 emy graduates and faculty; and

20 (2) detail to the Coast Guard Academy, as faculty, of individuals
21 with expertise and experience in cybersecurity who are employed by—

22 (A) the Cybersecurity and Infrastructure Security Agency (in-
23 cluding the National Cybersecurity and Communications Integra-
24 tion Center);

25 (B) the Directorate of Science and Technology; or

26 (C) institutions that have been designated by the Department
27 as a Center of Excellence for Cyber Defense, or the equivalent.

28 **§ 10368. Homeland Security Education Program**

29 (a) ESTABLISHMENT.—The Secretary, acting through the Administrator
30 of the Federal Emergency Management Agency, shall establish a graduate-
31 level Homeland Security Education Program in the National Capital Region
32 to provide educational opportunities to senior Federal officials and selected
33 State and local officials with homeland security and emergency management
34 responsibilities. The Administrator shall appoint an individual to administer
35 the activities under this section.

36 (b) LEVERAGING OF EXISTING RESOURCES.—To maximize efficiency and
37 effectiveness in carrying out the Homeland Security Education Program,
38 the Administrator shall use existing Department-reviewed master's degree
39 curricula in homeland security, including curricula pending accreditation, to-
40 gether with associated learning materials, quality assessment tools, digital
41 libraries, exercise systems, and other educational facilities, including the Na-

1 tional Domestic Preparedness Consortium, the National Fire Academy, and
2 the Emergency Management Institute. The Administrator may develop addi-
3 tional educational programs, as appropriate.

4 (c) STUDENT ENROLLMENT.—

5 (1) SOURCES.—The student body of the Homeland Security Edu-
6 cation Program shall include officials from Federal, State, local, and
7 tribal governments, and from other sources designated by the Adminis-
8 trator.

9 (2) ENROLLMENT PRIORITIES AND SELECTION CRITERIA.—The Ad-
10 ministrator shall establish policies governing student enrollment prior-
11 ities and selection criteria that are consistent with the mission of the
12 Homeland Security Education Program.

13 (3) DIVERSITY.—The Administrator shall take reasonable steps to
14 ensure that the student body represents racial, gender, and ethnic di-
15 versity.

16 (d) SERVICE COMMITMENT.—

17 (1) IN GENERAL.—Before an employee selected for the Homeland
18 Security Education Program may be assigned to participate in the pro-
19 gram, the employee shall agree in writing—

20 (A) to continue in the service of the agency sponsoring the em-
21 ployee during the 2-year period beginning on the date on which
22 the employee completes the program, unless the employee is invol-
23 untarily separated from the service of that agency for reasons
24 other than a reduction in force; and

25 (B) to pay to the Government the amount of the additional ex-
26 penses incurred by the Government in connection with the employ-
27 ee's education if the employee is voluntarily separated from the
28 service of the agency before the end of the period described in sub-
29 paragraph (A).

30 (2) PAYMENT OF EXPENSES.—

31 (A) EXEMPTION.—An employee who leaves the service of the
32 sponsoring agency to enter into the service of another agency in
33 any branch of the Government shall not be required to make a
34 payment under paragraph (1)(B), unless the head of the agency
35 that sponsored the education of the employee notifies that em-
36 ployee before the date on which the employee enters the service
37 of the other agency that payment is required under that para-
38 graph.

39 (B) AMOUNT OF PAYMENT.—If an employee is required to make
40 a payment under paragraph (1)(B), the agency that sponsored the
41 education of the employee shall determine the amount of the pay-

1 ment, except that the amount may not exceed the pro rata share
2 of the expenses incurred for the time remaining in the 2-year pe-
3 riod.

4 (3) RECOVERY OF PAYMENT.—If an employee who is required to
5 make a payment under this subsection does not make the payment, a
6 sum equal to the amount of the expenses incurred by the Government
7 for the education of that employee is recoverable by the Government
8 from the employee or his estate by—

9 (A) setoff against accrued pay, compensation, amount of retire-
10 ment credit, or other amount due the employee from the Govern-
11 ment; or

12 (B) another method provided by law for the recovery of amounts
13 owing to the Government.

14 **§ 10369. Annual employee award program**

15 (a) IN GENERAL.—The Secretary may establish an annual employee
16 award program to recognize Department employees or groups of employees
17 for significant contributions to the achievement of the Department’s goals
18 and missions. If such a program is established, the Secretary shall—

19 (1) establish within the program categories of awards, each with spe-
20 cific criteria, that emphasize honoring employees who are at the non-
21 supervisory level;

22 (2) publicize within the Department how any employee or group of
23 employees may be nominated for an award;

24 (3) establish an internal review board comprised of representatives
25 from Department components, headquarters, and field personnel to
26 submit to the Secretary award recommendations regarding specific em-
27 ployees or groups of employees;

28 (4) select recipients from the pool of nominees submitted by the in-
29 ternal review board under paragraph (3) and convene a ceremony at
30 which employees or groups of employees receive the awards from the
31 Secretary; and

32 (5) publicize the program within the Department.

33 (b) CONSULTATION.—The internal review board described in subsection
34 (a)(3) shall, when carrying out its function under subsection (a)(3), consult
35 with representatives from operational components and headquarters, includ-
36 ing supervisory and nonsupervisory personnel, and employee labor organiza-
37 tions that represent Department employees.

38 (c) RULE OF CONSTRUCTION.—Nothing in this section may be construed
39 to authorize additional funds to carry out the requirements of this section
40 or to require the Secretary to provide monetary bonuses to recipients of an
41 award under this section.

Subchapter V—Cybersecurity

§ 10381. Workforce assessment and strategy

(a) DEFINITIONS.—In this section:

(1) CYBERSECURITY CATEGORY.—The term “Cybersecurity Category” means a position’s or incumbent’s primary work function involving cybersecurity, which is further defined by Specialty Area.

(2) SPECIALTY AREA.—The term “Specialty Area” means any of the common types of cybersecurity work as recognized by the National Initiative for Cybersecurity Education’s National Cybersecurity Workforce Framework report.

(b) WORKFORCE ASSESSMENT.—The Secretary shall assess the cybersecurity workforce of the Department. The assessment shall include, at a minimum—

(1) an assessment of the readiness and capacity of the workforce of the Department to meet its cybersecurity mission;

(2) information on where cybersecurity workforce positions are located in the Department;

(3) information on which cybersecurity workforce positions are—

(A) performed by—

(i) permanent full-time equivalent employees of the Department, including, to the greatest extent practicable, demographic information about the employees;

(ii) independent contractors; and

(iii) individuals employed by other Federal agencies, including the National Security Agency; or

(B) vacant; and

(4) information on—

(A) the percentage of individuals in each Cybersecurity Category and Specialty Area who received essential training to perform their jobs; and

(B) in cases in which that essential training was not received, what challenges, if any, were encountered with respect to the provision of the essential training.

(c) WORKFORCE STRATEGY.—

(1) ESTABLISHMENT, MAINTENANCE, AND UPDATES.—The Secretary shall—

(A) develop a comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department; and

1 (B) maintain and, as necessary, update the comprehensive
2 workforce strategy developed under subparagraph (A).

3 (2) CONTENTS.—The comprehensive workforce strategy developed
4 under paragraph (1) shall include a description of—

5 (A) a multi-phased recruitment plan, including with respect to
6 experienced professionals, members of disadvantaged or under-
7 served communities, the unemployed, and veterans;

8 (B) a 5-year implementation plan;

9 (C) a 10-year projection of the cybersecurity workforce needs of
10 the Department;

11 (D) any obstacle impeding the hiring and development of a cy-
12 bersecurity workforce in the Department; and

13 (E) any gap in the existing cybersecurity workforce of the De-
14 partment and a plan to fill the gap.

15 (d) UPDATES.—The Secretary shall submit to the appropriate congres-
16 sional committees annual updates on—

17 (1) the cybersecurity workforce assessment required under subsection
18 (b); and

19 (2) the progress of the Secretary in carrying out the comprehensive
20 workforce strategy required to be developed under subsection (c).

21 **§ 10382. Homeland Workforce Measurement Initiative**

22 (a) DEFINITIONS.—In this section:

23 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
24 priate congressional committees” means—

25 (A) the Committee on Homeland Security and Governmental
26 Affairs of the Senate;

27 (B) the Committee on Homeland Security of the House of Rep-
28 resentatives; and

29 (C) the Committee on House Administration of the House of
30 Representatives.

31 (2) CYBERSECURITY WORK CATEGORY; DATA ELEMENT CODE; SPE-
32 CIALTY AREA.—The terms “Cybersecurity Work Category”, “Data Ele-
33 ment Code”, and “Specialty Area” have the same meanings given those
34 terms in the Office of Personnel Management’s Guide to Data Stand-
35 ards.

36 (3) DIRECTOR.—The term “Director” means the Director of the Of-
37 fice of Personnel Management.

38 (b) NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIA-
39 TIVE.—

40 (1) IN GENERAL.—The Secretary shall—

1 (A) identify all cybersecurity workforce positions in the Depart-
2 ment;

3 (B) determine the primary Cybersecurity Work Category and
4 Specialty Area of those positions; and

5 (C) assign the corresponding Data Element Code, as set forth
6 in the Office of Personnel Management’s Guide to Data Standards
7 that is aligned with the National Initiative for Cybersecurity Edu-
8 cation’s National Cybersecurity Workforce Framework report, in
9 accordance with paragraph (2).

10 (2) EMPLOYMENT CODES.—

11 (A) PROCEDURES.—The Secretary shall establish procedures
12 to—

13 (i) identify open positions that include cybersecurity func-
14 tions (as defined in the Office of Personnel Management’s
15 Guide to Data Standards); and

16 (ii) assign the appropriate employment code to each posi-
17 tion, using agreed-on standards and definitions.

18 (B) CODE ASSIGNMENTS.—The Secretary shall assign the ap-
19 propriate employment code to—

20 (i) each employee in the Department who carries out cyber-
21 security functions; and

22 (ii) each open position in the Department that has been
23 identified as having cybersecurity functions.

24 (3) PROGRESS REPORT.—The Director shall submit a progress re-
25 port on the implementation of this subsection to the appropriate con-
26 gressional committees.

27 (c) IDENTIFICATION OF CYBERSECURITY SPECIALTY AREAS OF CRITICAL
28 NEED.—

29 (1) IN GENERAL.—Annually through 2021, the Secretary, in con-
30 sultation with the Director, shall—

31 (A) identify Cybersecurity Work Categories and Specialty Areas
32 of critical need in the Department’s cybersecurity workforce; and

33 (B) submit a report to the Director that—

34 (i) describes the Cybersecurity Work Categories and Spe-
35 cialty Areas identified under subparagraph (A); and

36 (ii) substantiates the critical need designations.

37 (2) GUIDANCE.—The Director shall provide the Secretary with time-
38 ly guidance for identifying Cybersecurity Work Categories and Spe-
39 cialty Areas of critical need, including—

40 (A) current Cybersecurity Work Categories and Specialty Areas
41 with acute skill shortages; and

1 (B) Cybersecurity Work Categories and Specialty Areas with
2 emerging skill shortages.

3 (3) CYBERSECURITY CRITICAL NEEDS REPORT.—Not later than 18
4 months after December 18, 2014, the Secretary, in consultation with
5 the Director, shall—

6 (A) identify Specialty Areas of critical need for cybersecurity
7 workforce across the Department; and

8 (B) submit a progress report on the implementation of this sub-
9 section to the appropriate congressional committees.

10 (d) COMPTROLLER GENERAL STATUS REPORTS.—The Comptroller Gen-
11 eral shall—

12 (1) analyze and monitor the implementation of subsections (b) and
13 (c); and

14 (2) not later than 3 years after December 18, 2014, submit a report
15 to the appropriate congressional committees that describes the status
16 of the implementation.

17 **Subchapter VI—Miscellaneous Provisions**

18 **§ 10391. Advisory committees**

19 (a) IN GENERAL.—The Secretary may establish, appoint members of, and
20 use the services of, advisory committees, that the Secretary considers nec-
21 essary. An advisory committee established under this section may be ex-
22 empted by the Secretary from chapter 10 of title 5, but the Secretary shall
23 publish notice in the Federal Register announcing the establishment of the
24 committee and identifying its purpose and membership. Notwithstanding the
25 preceding sentence, members of an advisory committee that is exempted by
26 the Secretary under the preceding sentence who are special Government em-
27 ployees (as that term is defined in section 202 of title 18) shall be eligible
28 for certifications under section 208(b)(3) of title 18, for official actions
29 taken as a member of the advisory committee.

30 (b) TERMINATION.—An advisory committee established by the Secretary
31 shall terminate 2 years after the date of its establishment, unless the Sec-
32 retary makes a written determination to extend the advisory committee to
33 a specified date, which shall not be more than 2 years after the date on
34 which the determination is made. The Secretary may make any number of
35 subsequent extensions consistent with this subsection.

36 **§ 10392. Use of appropriated funds**

37 (a) IN GENERAL.—Unless otherwise provided, funds may be used for the
38 following:

39 (1) Purchase of uniforms without regard to the general purchase
40 price limitation for the current fiscal year;

1 (2) Purchase of insurance for official motor vehicles operated in for-
2 eign countries;

3 (3) Entering into contracts with the Department of State to furnish
4 health and medical services to employees and their dependents serving
5 in foreign countries;

6 (4) Services authorized by section 3109 of title 5; and

7 (5) The hire and purchase of motor vehicles, as authorized by section
8 1343 of title 31.

9 (b) POLICE-LIKE USE OF VEHICLES.—The purchase for police-type use
10 of passenger vehicles may be made without regard to the general purchase
11 price limitation for the current fiscal year.

12 (c) DISPOSAL OF PROPERTY.—

13 (1) STRICT COMPLIANCE.—If specifically authorized to dispose of
14 real property in this subtitle or any law, the Secretary shall exercise
15 this authority in strict compliance with subchapter IV of chapter 5 of
16 title 40.

17 (2) DEPOSIT OF PROCEEDS.—The Secretary shall deposit the pro-
18 ceeds of an exercise of property disposal authority into the miscella-
19 neous receipts of the Treasury under section 3302(b) of title 31.

20 (d) GIFTS.—Except as authorized by section 10397 or 11321 of this title,
21 section 2601 of title 10, or section 504 of title 14, gifts or donations of
22 services or property of or for the Department may not be accepted, used,
23 or disposed of unless specifically permitted in advance in an appropriations
24 Act and only under the conditions and for the purposes specified in the ap-
25 propriations Act.

26 (e) BUDGET REQUEST.—Under section 1105 of title 31, the President
27 shall submit to Congress a detailed budget request for the Department for
28 each fiscal year.

29 **§ 10393. Reports and consultation addressing use of appro-**
30 **riated funds**

31 (a) IN GENERAL.—Notwithstanding this subtitle, a report, notification, or
32 consultation addressing directly or indirectly the use of appropriated funds
33 and stipulated by this subtitle to be submitted to, or held with, Congress
34 or a Congressional committee shall also be submitted to, or held with, the
35 Committees on Appropriations of the Senate and the House of Representa-
36 tives under the same conditions and with the same restrictions as stipulated
37 by this subtitle.

38 (b) REPROGRAMMING AND TRANSFER OF FUNDS.—Notifications by the
39 Department under an authority for reprogramming or transfer of funds
40 shall be made solely to the Committees on Appropriations of the Senate and
41 the House of Representatives.

1 **§ 10394. Buy America requirements**

2 (a) DEFINITION OF UNITED STATES.—In this section, the term “United
3 States” includes the possessions of the United States.

4 (b) REQUIREMENT.—Except as provided in subsections (d) and (e), funds
5 appropriated or otherwise available to the Department may not be used for
6 the procurement of an item described in subsection (c) under a contract en-
7 tered into by the Department on and after August 16, 2009, if the item
8 is not grown, reprocessed, reused, or produced in the United States.

9 (c) COVERED ITEMS.—An item referred to in subsection (b) is an article
10 or item of any of the following, if the item is directly related to the national
11 security interests of the United States:

12 (1) Clothing and the materials and components of clothing, other
13 than sensors, electronics, or other items added to, and not normally as-
14 sociated with, clothing (and the materials and components of clothing).

15 (2) Tents, tarpaulins, covers, textile belts, bags, protective equipment
16 (including body armor), sleep systems, load carrying equipment (includ-
17 ing fieldpacks), textile marine equipment, parachutes, or bandages.

18 (3) Cotton and other natural fiber products, woven silk or woven silk
19 blends, spun silk yarn for cartridge cloth, synthetic fabric or coated
20 synthetic fabric (including all textile fibers and yarns that are for use
21 in the fabrics), canvas products, or wool (whether in the form of fiber
22 or yarn or contained in fabrics, materials, or manufactured articles).

23 (4) An item of individual equipment manufactured from or con-
24 taining the fibers, yarns, fabrics, or materials.

25 (d) APPLICABILITY TO CONTRACTS AND SUBCONTRACTS FOR PROCURE-
26 MENT OF COMMERCIAL PRODUCTS.—

27 (1) DEFINITION OF COMMERCIAL PRODUCT.—In this section, the
28 word “commercial product” has the meaning given the term in section
29 103 of title 41.

30 (2) IN GENERAL.—This section is applicable to contracts and sub-
31 contracts for the procurement of commercial products notwithstanding
32 section 1906 of title 41, with the exception of commercial products list-
33 ed under paragraphs (3) and (4) of subsection (c).

34 (e) EXCEPTIONS.—

35 (1) AVAILABILITY.—

36 (A) MATERIALS.—Subsection (b) does not apply to covered
37 items that are, or include, materials determined to be non-avail-
38 able in accordance with Federal Acquisition Regulation 25.104
39 Nonavailable Articles.

40 (B) UNSATISFACTORY QUALITY AND INSUFFICIENT QUAN-
41 TITY.—Subsection (b) does not apply to the extent that the Sec-

1 retary determines that satisfactory quality and sufficient quantity
2 of an article or item described in subsection (c) grown, reproc-
3 essed, reused, or produced in the United States cannot be pro-
4 cured as and when needed at United States market prices.

5 (2) DE MINIMIS NONCOMPLIANCE.—Notwithstanding subsection (b),
6 the Secretary may accept delivery of an item covered by subsection (c)
7 that contains non-compliant fibers if the total value of non-compliant
8 fibers contained in the end item does not exceed 10 percent of the total
9 purchase price of the end item.

10 (3) CERTAIN PROCUREMENTS OUTSIDE THE UNITED STATES.—Sub-
11 section (b) does not apply to the following:

12 (A) Procurements by vessels in foreign waters.

13 (B) Emergency procurements.

14 (4) SMALL PURCHASES.—Subsection (b) does not apply to purchases
15 for amounts not greater than the simplified acquisition threshold re-
16 ferred to in section 3205 of title 10.

17 (f) NOTIFICATION REQUIRED WITHIN 7 DAYS AFTER CONTRACT AWARD
18 IF CERTAIN EXCEPTIONS APPLIED.—In the case of a contract for the pro-
19 curement of an item described in subsection (c), if the Secretary applies an
20 exception set forth in subsection (e)(1) with respect to that contract, the
21 Secretary shall, not later than 7 days after the award of the contract, post
22 a notification that the exception has been applied on the Internet site main-
23 tained by the General Services Administration known as FedBizOpps.gov
24 (or a successor site).

25 (g) INCLUSION OF INFORMATION IN NEW TRAINING PROGRAMS.—The
26 Secretary shall ensure that a training program for the acquisition workforce
27 includes comprehensive information on the requirements of this section and
28 the regulations implementing this section.

29 (h) CONSISTENCY WITH INTERNATIONAL AGREEMENTS.—This section
30 shall be applied in a manner consistent with United States obligations under
31 international agreements.

32 **§ 10395. Horse adoption program**

33 With respect to a horse or other equine belonging to a component or
34 agency of the Department, no funds made available in any Act may be used
35 to destroy or put out to pasture any horse or other equine that has become
36 unfit for service, unless the trainer or handler is first given the option to
37 take possession of the equine through an adoption program that has safe-
38 guards against slaughter and inhumane treatment.

1 **§ 10396. Future Years Homeland Security Program**

2 (a) IN GENERAL.—Each budget request submitted to Congress for the
3 Department under section 1105 of title 31, shall, at or about the same time,
4 be accompanied by a Future Years Homeland Security Program.

5 (b) CONTENTS.—The Future Years Homeland Security Program shall—

6 (1) include the same type of information, organizational structure,
7 and level of detail as the future years defense program submitted to
8 Congress by the Secretary of Defense under section 221 of title 10;

9 (2) set forth the homeland security strategy of the Department,
10 which shall be developed and updated as appropriate annually by the
11 Secretary, that was used to develop program planning guidance for the
12 Future Years Homeland Security Program; and

13 (3) include an explanation of how the resource allocations included
14 in the Future Years Homeland Security Program correlate to the
15 homeland security strategy set forth under paragraph (2).

16 **§ 10397. Federal Law Enforcement Training Centers**

17 (a) DEFINITIONS.—In this section:

18 (1) BASIC TRAINING.—The term “basic training” means the entry-
19 level training required to instill in new Federal law enforcement per-
20 sonnel fundamental knowledge of criminal laws, law enforcement and
21 investigative techniques, laws and rules of evidence, rules of criminal
22 procedure, constitutional rights, search and seizure, and related issues.

23 (2) DETAILED INSTRUCTORS.—The term “detailed instructors”
24 means personnel who are assigned to the Federal Law Enforcement
25 Training Centers (in this section referred to as “FLETC”) for a period
26 of time to serve as instructors for the purpose of conducting basic and
27 advanced training.

28 (3) DIRECTOR.—The term “Director” means the Director of
29 FLETC.

30 (4) DISTRIBUTED LEARNING.—The term “distributed learning”
31 means education in which students take academic courses by accessing
32 information and communicating with the instructor, from various loca-
33 tions, on an individual basis, over a computer network or via other
34 technologies.

35 (5) EMPLOYEE.—The term “employee” has the meaning given the
36 term in section 2105 of title 5.

37 (6) FEDERAL AGENCY.—The term “Federal agency” means—

38 (A) an executive department as defined in section 101 of title
39 5;

40 (B) an independent establishment as defined in section 104 of
41 title 5;

1 (C) a Government corporation as defined in section 9101 of title
2 31;

3 (D) the Government Printing Office;

4 (E) the United States Capitol Police;

5 (F) the United States Supreme Court Police; and

6 (G) Government agencies with law enforcement related duties.

7 (7) LAW ENFORCEMENT PERSONNEL.—The term “law enforcement
8 personnel” means an individual, including a criminal investigator (com-
9 monly known as “agent”) and uniformed police (commonly known as
10 “officer”), who has statutory authority to search, seize, make arrests,
11 or carry firearms.

12 (8) LOCAL.—The term “local” means—

13 (A) of or pertaining to any county, parish, municipality, city,
14 town, township, rural community, unincorporated town or village,
15 local public authority, educational institution, special district,
16 intrastate district, council of governments (regardless of whether
17 the council of governments is incorporated as a nonprofit corpora-
18 tion under State law), regional or interstate government entity,
19 agency or instrumentality of a local government, or other political
20 subdivision of a State; and

21 (B) an Indian tribe or authorized tribal organization, or in Alas-
22 ka a Native village or Alaska Regional Native Corporation.

23 (9) PARTNER ORGANIZATION.—The term “partner organization”
24 means a Federal agency participating in FLETC’s training programs
25 under a formal memorandum of understanding.

26 (10) STATE.—The term “State” means a State, the District of Co-
27 lumbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the
28 Northern Mariana Islands, and any possession of the United States.

29 (11) STUDENT INTERN.—The term “student intern” means any eli-
30 gible baccalaureate or graduate degree student participating in
31 FLETC’s College Intern Program.

32 (b) ESTABLISHMENT.—The Secretary shall maintain in the Department
33 the Federal Law Enforcement Training Centers. The Director—

34 (1) is the head of FLETC;

35 (2) shall occupy a career-reserved position in the Senior Executive
36 Service; and

37 (3) shall report to the Secretary.

38 (c) FUNCTIONS OF THE DIRECTOR.—The Director shall—

39 (1) develop training goals and establish strategic and tactical organi-
40 zational program plans and priorities;

1 (2) provide direction and management for FLETC's training facilities,
2 ties, programs, and support activities while ensuring that organiza-
3 tional program goals and priorities are executed in an effective and ef-
4 ficient manner;

5 (3) develop homeland security and law enforcement training cur-
6 ricula, including curricula relating to domestic preparedness and re-
7 sponse to threats or acts of terrorism, for Federal, State, local, tribal,
8 territorial, and international law enforcement and security agencies and
9 private-sector security agencies;

10 (4) monitor progress toward strategic and tactical FLETC plans re-
11 garding training curricula, including curricula relating to domestic pre-
12 paredness and response to threats or acts of terrorism, and facilities;

13 (5) ensure the timely dissemination of homeland security information
14 as necessary to Federal, State, local, tribal, territorial, and inter-
15 national law enforcement and security agencies and the private sector
16 to achieve the training goals for those entities, in accordance with para-
17 graph (1);

18 (6) carry out delegated acquisition responsibilities in a manner
19 that—

20 (A) fully complies with—

21 (i) Federal law;

22 (ii) the Federal Acquisition Regulation, including require-
23 ments regarding agency obligations to contract only with re-
24 sponsible prospective contractors; and

25 (iii) Department acquisition management directives; and

26 (B) maximizes opportunities for small business participation;

27 (7) coordinate and share information with the heads of relevant com-
28 ponents and offices on digital learning and training resources, as ap-
29 propriate;

30 (8) advise the Secretary on matters relating to executive level policy
31 and program administration of Federal, State, local, tribal, territorial,
32 and international law enforcement and security training activities and
33 private-sector security agency training activities, including training ac-
34 tivities relating to domestic preparedness and response to threats or
35 acts of terrorism;

36 (9) collaborate with the Secretary and relevant officials at other Fed-
37 eral departments and agencies, as appropriate, to improve international
38 instructional development, training, and technical assistance provided
39 by the Federal Government to foreign law enforcement; and

40 (10) carry out such other functions as the Secretary determines are
41 appropriate.

1 (d) TRAINING RESPONSIBILITIES.—

2 (1) IN GENERAL.—The Director may provide training to employees
3 of Federal agencies who are engaged, directly or indirectly, in home-
4 land security operations or Federal law enforcement activities, includ-
5 ing operations or activities relating to domestic preparedness and re-
6 sponse to threats or acts of terrorism. In carrying out the training, the
7 Director shall—

8 (A) evaluate best practices of law enforcement training methods
9 and curriculum content to maintain state-of-the-art expertise in
10 adult learning methodology;

11 (B) provide expertise and technical assistance, including on do-
12 mestic preparedness and response to threats or acts of terrorism,
13 to Federal, State, local, tribal, territorial, and international law
14 enforcement and security agencies and private-sector security
15 agencies; and

16 (C) maintain a performance evaluation process for students.

17 (2) RELATIONSHIP WITH LAW ENFORCEMENT AGENCIES.—The Di-
18 rector shall consult with relevant law enforcement and security agencies
19 in the development and delivery of FLETC's training programs.

20 (3) TRAINING DELIVERY LOCATIONS.—The training required under
21 paragraph (1) may be conducted at FLETC facilities, at appropriate
22 off-site locations, or by distributed learning.

23 (4) STRATEGIC PARTNERSHIPS.—

24 (A) IN GENERAL.—The Director may—

25 (i) execute strategic partnerships with State and local law
26 enforcement to provide them with specific training, including
27 maritime law enforcement training; and

28 (ii) coordinate with the Director of the Cybersecurity and
29 Infrastructure Security Agency and with private-sector stake-
30 holders, including critical infrastructure owners and opera-
31 tors, to provide training pertinent to improving coordination,
32 security, and resiliency of critical infrastructure.

33 (B) PROVISION OF INFORMATION.—The Director shall provide
34 to the Committee on Homeland Security of the House of Rep-
35 resentatives and the Committee on Homeland Security and Gov-
36 ernmental Affairs of the Senate, on request, information on activi-
37 ties undertaken in the previous year pursuant to subparagraph
38 (A).

39 (5) FLETC DETAILS TO DEPARTMENT.—The Director may detail em-
40 ployees of FLETC to positions throughout the Department in further-
41 ance of improving the effectiveness and quality of training provided by

1 the Department and, as appropriate, the development of critical depart-
2 mental programs and initiatives.

3 (6) DETAIL OF INSTRUCTORS TO FLETC.—Partner organizations
4 that wish to participate in FLETC training programs shall assign non-
5 reimbursable detailed instructors to FLETC for designated time peri-
6 ods to support all training programs at FLETC, as appropriate. The
7 Director shall determine the number of detailed instructors that is pro-
8 portional to the number of training hours requested by each partner
9 organization scheduled by FLETC for each fiscal year. If a partner or-
10 ganization is unable to provide a proportional number of detailed in-
11 structors, the partner organization shall reimburse FLETC for the sal-
12 ary equivalent for the detailed instructors, as appropriate.

13 (7) PARTNER ORGANIZATION EXPENSES REQUIREMENTS.—

14 (A) IN GENERAL.—Partner organizations shall be responsible
15 for the following expenses:

16 (i) Salaries, travel expenses, lodging expenses, and miscella-
17 neous per diem allowances of their personnel attending train-
18 ing courses at FLETC.

19 (ii) Salaries and travel expenses of instructors and support
20 personnel involved in conducting advanced training at
21 FLETC for partner organization personnel and the cost of
22 expendable supplies and special equipment for the training,
23 unless the supplies and equipment are common to FLETC-
24 conducted training and have been included in FLETC's budg-
25 et for the applicable fiscal year.

26 (B) EXCESS BASIC AND ADVANCED FEDERAL TRAINING.—All
27 hours of advanced training and hours of basic training provided
28 in excess of the training for which appropriations were made avail-
29 able shall be paid by the partner organizations and provided to
30 FLETC on a reimbursable basis in accordance with section 4104
31 of title 5.

32 (8) PROVISION OF NON-FEDERAL TRAINING.—

33 (A) IN GENERAL.—The Director may charge and retain fees
34 that would pay for FLETC's actual costs of the training for the
35 following:

36 (i) State, local, tribal, and territorial law enforcement per-
37 sonnel.

38 (ii) Foreign law enforcement officials, including provision of
39 the training at the International Law Enforcement Academies
40 wherever established.

1 (iii) Private-sector security officers, participants in the
2 Federal Flight Deck Officer program under section 40932 of
3 this title, and other appropriate private-sector individuals.

4 (B) WAIVER.—The Director may waive the requirement for re-
5 imbursement of any cost under this section and shall maintain
6 records regarding the reasons for any requirements waived.

7 (9) REIMBURSEMENT.—The Director may reimburse travel or other
8 expenses for non-Federal personnel who attend activities relating to
9 training sponsored by FLETC, at travel and per diem rates established
10 by the General Services Administration.

11 (10) STUDENT SUPPORT.—In furtherance of FLETC's training mis-
12 sion, the Director may provide the following support to students:

13 (A) Athletic and related activities.

14 (B) Short-term medical services.

15 (C) Chaplain services.

16 (11) AUTHORITY TO HIRE FEDERAL ANNUITANTS.—

17 (A) IN GENERAL.—Notwithstanding another law, the Director
18 may appoint and maintain, as necessary, Federal annuitants who
19 have expert knowledge and experience to meet the training respon-
20 sibilities under this subsection.

21 (B) NO REDUCTION IN RETIREMENT PAY.—A Federal annuitant
22 employed pursuant to this paragraph shall not be subject to any
23 reduction in pay for annuity allocable to the period of actual em-
24 ployment under section 8344 or 8468 of title 5 or a similar provi-
25 sion of any other retirement system for employees.

26 (C) RE-EMPLOYED ANNUITANTS.—A Federal annuitant em-
27 ployed pursuant to this paragraph shall not be considered an em-
28 ployee for purposes of subchapter III of chapter 83 or chapter 84
29 of title 5 or such other retirement system (referred to in subpara-
30 graph (B)) as may apply.

31 (D) COUNTING.—Federal annuitants shall be counted on a full-
32 time equivalent basis.

33 (E) LIMITATION.—No appointment under this paragraph may
34 be made that would result in the displacement of any employee.

35 (12) TRAVEL FOR INTERMITTENT EMPLOYEES.—The Director may
36 reimburse intermittent Federal employees traveling from outside a com-
37 muting distance (to be predetermined by the Director) for travel ex-
38 penses.

39 (e) HOUSING.—Individuals attending training at any FLETC facility
40 shall, to the extent practicable and in accordance with FLETC policy, reside
41 in on-FLETC or FLETC-provided housing.

1 (f) ADDITIONAL FISCAL AUTHORITIES.—To further the goals and objec-
2 tives of FLETC, the Director may—

3 (1) expend funds for public awareness and to enhance community
4 support of law enforcement training, including the advertisement of
5 available law enforcement training programs;

6 (2) accept and use gifts of property, both real and personal, and ac-
7 cept gifts of services, for purposes that promote the functions of the
8 Director pursuant to subsection (c) and the training responsibilities of
9 the Director under subsection (d);

10 (3) accept reimbursement from other Federal agencies for the con-
11 struction or renovation of training and support facilities and the use
12 of equipment and technology on government owned-property;

13 (4) obligate funds in anticipation of reimbursements from agencies
14 receiving training at FLETC, except that total obligations at the end
15 of a fiscal year may not exceed total budgetary resources available at
16 the end of the fiscal year;

17 (5) in accordance with the purchasing authority provided under sec-
18 tion 10392(a) and (b) of this title—

19 (A) purchase employee and student uniforms; and

20 (B) purchase and lease passenger motor vehicles, including vehi-
21 cles for police-type use;

22 (6) provide room and board for student interns; and

23 (7) expend funds each fiscal year to honor and memorialize FLECT
24 graduates who have died in the line of duty.

25 (g) PROHIBITION ON NEW FUNDING.—No funds are authorized to carry
26 out this section. This section shall be carried out using amounts otherwise
27 appropriated or made available for that purpose.

28 **§ 10398. Fees**

29 (a) FEES FOR CREDENTIALING AND BACKGROUND INVESTIGATIONS IN
30 TRANSPORTATION.—The Secretary shall charge reasonable fees for pro-
31 viding credentialing and background investigations in the field of transpor-
32 tation. The establishment and collection of fees shall be subject to the fol-
33 lowing requirements:

34 (1) Fees, in the aggregate, shall not exceed the costs incurred by the
35 Department associated with providing the credential or performing the
36 background record checks.

37 (2) The Secretary shall charge fees in amounts that are reasonably
38 related to the costs of providing services in connection with the activity
39 or item for which the fee is charged.

40 (3) A fee may not be collected except to the extent the fee will be
41 expended to pay for—

1 (A) the costs of conducting or obtaining a criminal history
2 record check and a review of available law enforcement databases
3 and commercial databases and records of other governmental and
4 international agencies;

5 (B) reviewing and adjudicating requests for waiver and appeals
6 of agency decisions with respect to providing the credential, per-
7 forming the background record check, and denying requests for
8 waiver and appeals; and

9 (C) other costs related to providing the credential or performing
10 the background record check.

11 (4) A fee collected shall be available for expenditure only to pay the
12 costs incurred in providing services in connection with the activity or
13 item for which the fee is charged and shall remain available until ex-
14 pended.

15 (b) RECURRENT TRAINING OF ALIENS IN OPERATION OF AIRCRAFT.—

16 (1) PROCESS FOR REVIEWING THREAT ASSESSMENTS.—Notwith-
17 standing section 40959(a)(1) of this title, the Secretary shall establish
18 a process to ensure that an alien (as defined in section 101(a) of the
19 Immigration and Nationality Act (8 U.S.C. 1101(a)) applying for re-
20 current training in the operation of an aircraft is properly identified
21 and has not, since the time of a prior threat assessment conducted
22 under section 40959(a)(2) of this title, become a risk to aviation or na-
23 tional security.

24 (2) INTERRUPTION OF TRAINING.—If the Secretary determines, in
25 carrying out the process established under paragraph (1), that an alien
26 is a present risk to aviation or national security, the Secretary shall
27 immediately notify the person providing the training of the determina-
28 tion and that person shall not provide the training or, if training has
29 commenced, that person shall immediately terminate the training.

30 (3) FEES.—The Secretary may charge reasonable fees under sub-
31 section (a) for providing credentialing and background investigations
32 for aliens in connection with the process for recurrent training estab-
33 lished under paragraph (1). The fees shall be promulgated by notice
34 in the Federal Register.

35 (c) COLLECTION OF FEES FROM NON-FEDERAL PARTICIPANTS IN MEET-
36 INGS.—

37 (1) IN GENERAL.—The Secretary may collect fees from a non-Fed-
38 eral participant in a conference, seminar, exhibition, symposium, or
39 similar meeting conducted by the Department in advance of the con-
40 ference, either directly or by contract, and those fees shall be credited
41 to the appropriation or account from which the costs of the conference,

1 seminar, exhibition, symposium, or similar meeting are paid and shall
2 be available to pay the costs of the Department with respect to the con-
3 ference or to reimburse the Department for costs incurred with respect
4 to the conference.

5 (2) DEPOSIT OF EXCESS FEES.—If the total amount of fees collected
6 with respect to a conference exceeds the actual costs of the Department
7 with respect to the conference, the excess amount shall be deposited
8 into the Treasury as miscellaneous receipts.

9 **§ 10399. Reports to Committee on Commerce, Science, and**
10 **Transportation**

11 The Committee on Commerce, Science, and Transportation of the Senate
12 shall receive the reports required by the following provisions of law in the
13 same manner and to the same extent that the reports are to be received
14 by the Committee on Homeland Security and Governmental Affairs of the
15 Senate:

16 (1) Section 7209(b)(1)(C) of the Intelligence Reform and Terrorism
17 Prevention Act of 2004 (Public Law 108–458, 8 U.S.C. 1185 note).

18 (2) Title III of the Implementing Recommendations of the 9/11
19 Commission Act of 2007 (Public Law 110–53, 121 Stat. 296).

20 (3) Section 511(d) of the Implementing Recommendations of the 9/
21 11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 323).

22 (4) Section 804(c) of the Implementing Recommendations of the 9/
23 11 Commission Act of 2007 (42 U.S.C. 2000ee–3(c)).

24 (5) Section 901(b) of the Implementing Recommendations of the 9/
25 11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 370).

26 **§ 10400. Annual ammunition and weaponry reports**

27 (a) IN GENERAL.—The Secretary annually shall submit to Congress
28 along with the submission of the President’s budget proposal pursuant to
29 section 1105(a) of title 31 the following:

30 (1) A comprehensive report on the purchase and usage of ammuni-
31 tion, subdivided by ammunition type.

32 (2) A comprehensive report on the purchase and usage of weapons,
33 subdivided by weapon type.

34 (b) CONTENTS.—

35 (1) AMMUNITION REPORT.—The ammunition report shall include—

36 (A) the quantity of ammunition in inventory at the end of the
37 preceding calendar year, and the amount of ammunition expended
38 and purchased, subdivided by ammunition type, during the year
39 for each relevant component or agency in the Department;

1 (B) a description of how the quantity, usage, and purchase
2 aligns to each component or agency's mission requirements for
3 certification, qualification, training, and operations; and

4 (C) details on all contracting practices applied by the Depart-
5 ment, including comparative details regarding other contracting
6 options with respect to cost and availability.

7 (2) WEAPONRY REPORT.—The weaponry report shall include—

8 (A) the quantity of weapons in inventory at the end of the pre-
9 ceeding calendar year, and the amount of weapons, subdivided by
10 weapon type, included in the budget request for each relevant com-
11 ponent or agency in the Department;

12 (B) a description of how the quantity and purchase aligns to
13 each component or agency's mission requirements for certification,
14 qualification, training, and operations; and

15 (C) details on all contracting practices applied by the Depart-
16 ment, including comparative details regarding other contracting
17 options with respect to cost and availability.

18 (e) REPORT SUBMITTED IN APPROPRIATE FORMAT.—Each report shall
19 be submitted in an appropriate format to ensure the safety of law enforce-
20 ment personnel.

21 **§ 10401. National identification system not authorized**

22 Nothing in this subtitle or the Homeland Security Act of 2002 (Public
23 Law 107–296, 116 Stat. 2135) shall be construed to authorize the develop-
24 ment of a national identification system or card.

25 **§ 10402. Functions and authorities of Administrator of Gen-
26 eral Services not affected**

27 (a) OPERATION, MAINTENANCE, AND PROTECTION OF FEDERAL BUILD-
28 INGS AND GROUNDS.—Nothing in this subtitle may be construed to affect
29 the functions or authorities of the Administrator of General Services with
30 respect to the operation, maintenance, and protection of buildings and
31 grounds owned or occupied by the Federal Government and under the juris-
32 diction, custody, or control of the Administrator. Except for the law enforce-
33 ment and related security functions transferred under section
34 11101(b)(1)(C) of this title, the Administrator shall retain all powers, func-
35 tions, and authorities vested in the Administrator under chapters 1 (except
36 section 121(e)(2)(A)) and 5 through 11 of title 40, and other provisions of
37 law that are necessary for the operation, maintenance, and protection of the
38 buildings and grounds.

39 (b) LIMITATION ON COLLECTION AND USE OF RENTS AND FEES AND
40 FEDERAL BUILDINGS FUND.—

1 (1) STATUTORY CONSTRUCTION.—Nothing in this subtitle may be
2 construed—

3 (A) to direct the transfer of, or affect, the authority of the Ad-
4 ministrator of General Services to collect rents and fees, including
5 fees collected for protective services; or

6 (B) to authorize the Secretary or another official in the Depart-
7 ment to obligate amounts in the Federal Buildings Fund estab-
8 lished by section 592 of title 40.

9 (2) USE OF TRANSFERRED AMOUNTS.—Amounts transferred by the
10 Administrator of General Services to the Secretary out of rents and
11 fees collected by the Administrator shall be used by the Secretary solely
12 for the protection of buildings or grounds owned or occupied by the
13 Federal Government.

14 **§ 10403. Research and development pilot program**

15 (a) AUTHORITY.—Until September 30, 2024, and subject to subsection
16 (c), the Secretary may carry out a pilot program under which the Secretary
17 may exercise the following authorities:

18 (1) RESEARCH AND DEVELOPMENT PROJECTS.—When the Secretary
19 carries out basic, applied, and advanced research and development
20 projects, including the expenditure of funds for the projects, the Sec-
21 retary may exercise the same authority (subject to the same limitations
22 and conditions) with respect to the research and projects as the Sec-
23 retary of Defense may exercise under section 4021 of title 10 (except
24 for subsections (b) and (f)), after making a determination that the use
25 of a contract, grant, or cooperative agreement for the project is not
26 feasible or appropriate.

27 (2) PROTOTYPE PROJECTS.—The Secretary—

28 (A) may, under the authority of paragraph (1), carry out proto-
29 type projects under section 4022 of title 10; and

30 (A) in applying the authorities of section 4022 of title 10, shall
31 perform the functions of the Secretary of Defense as prescribed
32 in section 4022.

33 (b) PROCUREMENT OF TEMPORARY AND INTERMITTENT SERVICES.—The
34 Secretary may—

35 (1) procure the temporary or intermittent services of experts or con-
36 sultants (or organizations of experts or consultants) in accordance with
37 section 3109(b) of title 5; and

38 (2) whenever necessary due to an urgent homeland security need,
39 procure temporary (not to exceed 1 year) or intermittent personal serv-
40 ices, including the services of experts or consultants (or organizations

1 of experts or consultants), without regard to the pay limitations of sec-
2 tion 3109 of title 5.

3 (c) ADDITIONAL REQUIREMENTS.—

4 (1) IN GENERAL.—The authority of the Secretary under this section
5 shall terminate September 30, 2024, unless before that date the Sec-
6 retary—

7 (A) issues policy guidance detailing the appropriate use of that
8 authority; and

9 (B) provides training to each employee who may exercise that
10 authority.

11 (2) REPORT.—The Secretary shall provide an annual report to the
12 Committees on Appropriations of the Senate and the House of Rep-
13 resentatives, the Committee on Homeland Security and Governmental
14 Affairs of the Senate, and the Committee on Homeland Security of the
15 House of Representatives detailing the projects for which the authority
16 granted by subsection (a) was used, the rationale for its use, the funds
17 spent using that authority, the outcome of each project for which that
18 authority was used, and the results of any audits of the projects.

19 **§ 10404. Protection of certain facilities and assets from un-**
20 **manned aircraft**

21 (a) DEFINITIONS.—In this section:

22 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
23 priate congressional committees” means—

24 (A) the Committee on Homeland Security and Governmental
25 Affairs, the Committee on Commerce, Science, and Transporta-
26 tion, and the Committee on the Judiciary of the Senate; and

27 (B) the Committee on Homeland Security, the Committee on
28 Transportation and Infrastructure, the Committee on Energy and
29 Commerce, and the Committee on the Judiciary of the House of
30 Representatives.

31 (2) BUDGET.—The term “budget”, with respect to a fiscal year,
32 means the budget for that fiscal year that is submitted to Congress by
33 the President under section 1105(a) of title 31.

34 (3) COVERED FACILITY OR ASSET.—The term “covered facility or
35 asset” means a facility or asset that—

36 (A) is identified as high-risk and a potential target for unlawful
37 unmanned aircraft activity by the Secretary or the Attorney Gen-
38 eral, in coordination with the Secretary of Transportation with re-
39 spect to potentially impacted airspace, through a risk-based as-
40 sessment for purposes of this section (except that in the case of
41 the missions described in clauses (i)(II) and (iii)(I) of subpara-

1 graph (C), the missions shall be presumed to be for the protection
2 of a facility or asset that is assessed to be high-risk and a poten-
3 tial target for unlawful unmanned aircraft activity);

4 (B) is located in the United States (including the territories and
5 possessions, territorial seas, or navigable waters of the United
6 States); and

7 (C) directly relates to 1 or more—

8 (i) missions authorized to be performed by the Department,
9 consistent with governing statutes, regulations, and orders
10 issued by the Secretary, pertaining to—

11 (I) security or protection functions of U.S. Customs
12 and Border Protection, including securing or protecting
13 facilities, aircraft, and vessels, whether moored or under-
14 way;

15 (II) United States Secret Service protection operations
16 pursuant to sections 3056(a) and 3056A(a) of title 18
17 and the Presidential Protection Assistance Act of 1976
18 (18 U.S.C. 3056 note); or

19 (III) protection of facilities pursuant to section
20 1315(a) of title 40;

21 (ii) missions authorized to be performed by the Department
22 of Justice, consistent with governing statutes, regulations,
23 and orders issued by the Attorney General, pertaining to—

24 (I) personal protection operations by—

25 (aa) the Federal Bureau of Investigation as speci-
26 fied in section 533 of title 28; and

27 (bb) the United States Marshals Service of Fed-
28 eral jurists, court officers, witnesses, and other
29 threatened individuals in the interests of justice, as
30 specified in section 566(e)(1)(A) of title 28;

31 (II) protection of penal, detention, and correctional fa-
32 cilities and operations conducted by the Federal Bureau
33 of Prisons; or

34 (III) protection of the buildings and grounds leased,
35 owned, or operated by or for the Department of Justice,
36 and the provision of security for Federal courts, as speci-
37 fied in section 566(a) of title 28;

38 (iii) missions authorized to be performed by the Depart-
39 ment or the Department of Justice, acting together or sepa-
40 rately, consistent with governing statutes, regulations, and or-

1 ders issued by the Secretary or the Attorney General, respec-
2 tively, pertaining to—

3 (I) protection of a National Special Security Event
4 and Special Event Assessment Rating event;

5 (II) the provision of support to State, local, territorial,
6 or tribal law enforcement, on request of the chief execu-
7 tive officer of the State or territory, to ensure protection
8 of people and property at mass gatherings, that is lim-
9 ited to a specified time frame and location, within avail-
10 able resources, and without delegating any authority
11 under this section to State, local, territorial, or tribal law
12 enforcement; or

13 (III) protection of an active Federal law enforcement
14 investigation, emergency response, or security function,
15 that is limited to a specified time frame and location; or

16 (iv) missions authorized to be performed by the Coast
17 Guard, including those described in clause (iii) as directed by
18 the Secretary, and as further set forth in section 528 of title
19 14, and consistent with governing statutes, regulations, and
20 orders issued by the Secretary of the Department in which
21 the Coast Guard is operating.

22 (4) ELECTRONIC COMMUNICATION; INTERCEPT; ORAL COMMUNICA-
23 TION; WIRE COMMUNICATION.—The terms “electronic communication”,
24 “intercept”, “oral communication”, and “wire communication” have
25 the meanings given those terms in section 2510 of title 18.

26 (5) HOMELAND SECURITY OR JUSTICE BUDGET MATERIALS.—The
27 term “homeland security or justice budget materials”, with respect to
28 a fiscal year, means the materials submitted to Congress by the Sec-
29 retary and the Attorney General in support of the budget for that fiscal
30 year.

31 (6) RISK-BASED ASSESSMENT.—The term “risk-based assessment”
32 includes an evaluation of threat information specific to a covered facil-
33 ity or asset and, with respect to potential impacts on the safety and
34 efficiency of the national airspace system and the needs of law enforce-
35 ment and national security at each covered facility or asset identified
36 by the Secretary or the Attorney General, respectively, an evaluation
37 of each of the following factors:

38 (A) Potential impacts to safety, efficiency, and use of the na-
39 tional airspace system, including potential effects on manned air-
40 craft and unmanned aircraft systems, aviation safety, airport oper-
41 ations, infrastructure, and air navigation services related to the

1 use of any system or technology for carrying out the actions de-
2 scribed in subsection (e)(1).

3 (B) Options for mitigating identified impacts to the national
4 airspace system related to the use of any system or technology, in-
5 cluding minimizing when possible the use of any technology that
6 disrupts the transmission of radio or electronic signals, for car-
7 rying out the actions described in subsection (e)(1).

8 (C) Potential consequences of the impacts of actions taken
9 under subsection (e)(1) to the national airspace system and infra-
10 structure if not mitigated.

11 (D) The ability to provide reasonable advance notice to aircraft
12 operators consistent with the safety of the national airspace sys-
13 tem and the needs of law enforcement and national security.

14 (E) The setting and character of a covered facility or asset, in-
15 cluding whether it is located in a populated area or near other
16 structures, whether the facility is open to the public, whether the
17 facility is also used for nongovernmental functions, and any poten-
18 tial for interference with wireless communications or for injury or
19 damage to individuals or property.

20 (F) The setting, character, time frame, and national airspace
21 system impacts of National Special Security Events and Special
22 Event Assessment Rating events.

23 (G) Potential consequences to national security, public safety, or
24 law enforcement if threats posed by unmanned aircraft systems
25 are not mitigated or defeated.

26 (7) UNMANNED AIRCRAFT; UNMANNED AIRCRAFT SYSTEM.—The
27 terms “unmanned aircraft” and “unmanned aircraft system” have the
28 meanings given those terms in section 44801 of title 49.

29 (b) AUTHORITY.—Notwithstanding section 41062 of this title or sections
30 32, 1030, and 1367 and chapters 119 and 206 of title 18, the Secretary
31 and the Attorney General may, for their respective Departments, take, and
32 may authorize officers and employees of the Department or the Department
33 of Justice with assigned duties that include the security or protection of
34 people, facilities, or assets, to take such actions as are described in sub-
35 section (e)(1) that are necessary to mitigate a credible threat (as defined
36 by the Secretary or the Attorney General, in consultation with the Secretary
37 of Transportation) that an unmanned aircraft system or unmanned aircraft
38 poses to the safety or security of a covered facility or asset.

39 (c) ACTIONS DESCRIBED.—

40 (1) IN GENERAL.—The actions authorized in subsection (b) are the
41 following:

1 (A) During the operation of the unmanned aircraft system, de-
2 tect, identify, monitor, and track the unmanned aircraft system or
3 unmanned aircraft, without prior consent, including by means of
4 intercept or other access of a wire communication, an oral commu-
5 nication, or an electronic communication used to control the un-
6 manned aircraft system or unmanned aircraft.

7 (B) Warn the operator of the unmanned aircraft system or un-
8 manned aircraft, including by passive or active, and direct or indi-
9 rect physical, electronic, radio, and electromagnetic means.

10 (C) Disrupt control of the unmanned aircraft system or un-
11 manned aircraft, without prior consent, including by disabling the
12 unmanned aircraft system or unmanned aircraft by intercepting,
13 interfering, or causing interference with wire, oral, electronic, or
14 radio communications used to control the unmanned aircraft sys-
15 tem or unmanned aircraft.

16 (D) Seize or exercise control of the unmanned aircraft system
17 or unmanned aircraft.

18 (E) Seize or otherwise confiscate the unmanned aircraft system
19 or unmanned aircraft.

20 (F) Use reasonable force, if necessary, to disable, damage, or
21 destroy the unmanned aircraft system or unmanned aircraft.

22 (2) COORDINATION WITH SECRETARY OF TRANSPORTATION.—The
23 Secretary and the Attorney General shall develop for their respective
24 Departments the actions described in paragraph (1) in coordination
25 with the Secretary of Transportation.

26 (3) RESEARCH, TESTING, TRAINING, AND EVALUATION.—The Sec-
27 retary and the Attorney General shall conduct research, testing, and
28 training on, and evaluation of equipment, including electronic equip-
29 ment, to determine its capability and utility prior to the use of that
30 technology for an action described in paragraph (1).

31 (4) COORDINATION WITH ADMINISTRATOR OF FEDERAL AVIATION
32 ADMINISTRATION.—The Secretary and the Attorney General shall co-
33 ordinate with the Administrator of the Federal Aviation Administration
34 when an action authorized by this section might affect aviation safety,
35 civilian aviation and aerospace operations, aircraft airworthiness, or the
36 use of airspace.

37 (d) FORFEITURE.—An unmanned aircraft system or unmanned aircraft
38 described in subsection (b) that is seized by the Secretary or the Attorney
39 General is subject to forfeiture to the United States.

40 (e) REGULATIONS AND GUIDANCE.—

1 (1) IN GENERAL.—The Secretary, the Attorney General, and the
2 Secretary of Transportation may prescribe regulations and shall issue
3 guidance in their respective areas to carry out this section.

4 (2) COORDINATION.—

5 (A) COORDINATION WITH SECRETARY OF TRANSPORTATION.—

6 The Secretary and the Attorney General shall coordinate the de-
7 velopment of their respective guidance under paragraph (1) with
8 the Secretary of Transportation.

9 (B) COORDINATION WITH SECRETARY OF TRANSPORTATION
10 AND ADMINISTRATOR OF FEDERAL AVIATION ADMINISTRATION.—

11 The Secretary and the Attorney General shall respectively coordi-
12 nate with the Secretary of Transportation and the Administrator
13 of the Federal Aviation Administration before issuing any guid-
14 ance, or otherwise implementing this section, if the guidance or
15 implementation might affect aviation safety, civilian aviation and
16 aerospace operations, aircraft airworthiness, or the use of airspace.

17 (f) PRIVACY PROTECTION.—The regulations or guidance issued to carry
18 out actions authorized under subsection (c) by the Secretary, the Secretary
19 of Transportation, or the Attorney General, as the case may be, shall ensure
20 that—

21 (1) the interception or acquisition of, or access to, or maintenance
22 or use of, communications to or from an unmanned aircraft system
23 under this section is conducted in a manner consistent with the 1st and
24 4th Amendments to the Constitution and applicable provisions of Fed-
25 eral law;

26 (2) communications to or from an unmanned aircraft system are
27 intercepted or acquired only to the extent necessary to support an ac-
28 tion described in subsection (c)(1);

29 (3) records of the communications are maintained only for as long
30 as necessary, and in no event for more than 180 days, unless the Sec-
31 retary or the Attorney General determines that maintenance of the
32 records is necessary to investigate or prosecute a violation of law or
33 to directly support an ongoing security operation, is required under
34 Federal law, or is necessary for the purpose of any litigation;

35 (4) the communications are not disclosed outside the Department or
36 the Department of Justice unless the disclosure—

37 (A) is necessary to investigate or prosecute a violation of law;

38 (B) would support the Department of Defense, a Federal law
39 enforcement agency, or the enforcement activities of a regulatory
40 agency of the Federal Government in connection with a criminal
41 or civil investigation of, or a regulatory, statutory, or other en-

1 enforcement action relating to, an action described in subsection
2 (c)(1);

3 (C) is between the Department and the Department of Justice
4 in the course of a security or protection operation of either agency
5 or a joint operation of the agencies; or

6 (D) is otherwise required by law; and

7 (5) to the extent necessary, the Department and the Department of
8 Justice may share threat information, which shall not include commu-
9 nications referred to in subsection (c), with State, local, territorial, or
10 tribal law enforcement agencies in the course of a security or protection
11 operation.

12 (g) BUDGET.—The Secretary and the Attorney General shall submit to
13 Congress, as a part of the homeland security or justice budget materials for
14 each fiscal year a consolidated funding display that identifies the funding
15 source for the actions described in subsection (c)(1) in the Department or
16 the Department of Justice. The funding display shall be in unclassified form
17 but may contain a classified annex.

18 (h) SEMIANNUAL BRIEFINGS AND NOTIFICATIONS.—

19 (1) BRIEFINGS.—

20 (A) IN GENERAL.—On a semiannual basis during the period be-
21 ginning 6 months after October 5, 2018, and ending on the date
22 specified in subsection (l), the Secretary and the Attorney General
23 shall, respectively, provide a briefing to the appropriate congres-
24 sional committees on the activities carried out pursuant to this
25 section.

26 (B) JOINT BRIEFING REQUIRED.—Each briefing shall be con-
27 ducted jointly with the Secretary of Transportation.

28 (C) CONTENT.—Each briefing shall include—

29 (i) policies, programs, and procedures to mitigate or elimi-
30 nate impacts of the activities on the national airspace system;

31 (ii) a description of instances in which actions described in
32 subsection (c)(1) have been taken, including all instances that
33 may have resulted in harm, damage, or loss to a person or
34 to private property;

35 (iii) a description of the guidance, policies, or procedures
36 established to address privacy, civil rights, and civil liberties
37 issues implicated by the actions allowed under this section, as
38 well as any changes or subsequent efforts that would signifi-
39 cantly affect privacy, civil rights or civil liberties;

40 (iv) a description of options considered and steps taken to
41 mitigate identified impacts to the national airspace system re-

1 lated to the use of any system or technology, including the
2 minimization of the use of technology that disrupts the trans-
3 mission of radio or electronic signals, for carrying out the ac-
4 tions described in subsection (c)(1);

5 (v) a description of instances in which communications
6 intercepted or acquired during the course of operations of an
7 unmanned aircraft system were held for more than 180 days
8 or shared outside of the Department or the Department of
9 Justice;

10 (vi) how the Secretary, the Attorney General, and the Sec-
11 retary of Transportation have informed the public as to the
12 possible use of authorities under this section; and

13 (vii) how the Secretary, the Attorney General, and the Sec-
14 retary of Transportation have engaged with Federal, State,
15 and local law enforcement agencies to implement and use the
16 authorities under this section.

17 (D) BRIEFING TO BE IN UNCLASSIFIED FORM.—Each briefing
18 shall be in unclassified form but may be accompanied by an addi-
19 tional classified briefing.

20 (2) NOTIFICATION.—Within 30 days of deploying new technology to
21 carry out the actions described in subsection (c)(1), the Secretary and
22 the Attorney General shall, respectively, submit a notification to the ap-
23 propriate congressional committees. The notification shall include a de-
24 scription of options considered to mitigate identified impacts on the na-
25 tional airspace system related to the use of any system or technology,
26 including the minimization of the use of technology that disrupts the
27 transmission of radio or electronic signals, for carrying out the actions
28 described in subsection (c)(1).

29 (i) RULE OF CONSTRUCTION.—Nothing in this section may be construed
30 to—

31 (1) vest in the Secretary or the Attorney General any authority of
32 the Secretary of Transportation or the Administrator of the Federal
33 Aviation Administration;

34 (2) vest in the Secretary of Transportation or the Administrator of
35 the Federal Aviation Administration any authority of the Secretary or
36 the Attorney General;

37 (3) vest in the Secretary any authority of the Attorney General;

38 (4) vest in the Attorney General any authority of the Secretary; or

39 (5) provide a new basis of liability for State, local, territorial, or trib-
40 al law enforcement officers who participate in the protection of a mass
41 gathering identified by the Secretary or Attorney General under sub-

1 section (a)(3)(C)(iii)(II), act within the scope of their authority, and
2 do not exercise the authority granted to the Secretary and Attorney
3 General by this section.

4 (j) SCOPE OF AUTHORITY.—Nothing in this section shall be construed to
5 provide the Secretary or the Attorney General with additional authorities
6 beyond those described in subsections (a)(3)(C)(iii) and (b).

7 (k) DEPARTMENT ASSESSMENT.—

8 (1) REPORT.—Not later than 1 year after October 5, 2018, the Sec-
9 retary shall conduct, in coordination with the Attorney General and the
10 Secretary of Transportation, an assessment to the appropriate congres-
11 sional committees, including—

12 (A) an evaluation of the threat from unmanned aircraft systems
13 to United States critical infrastructure (as defined in section
14 10101 of this title) and to domestic large hub airports (as defined
15 in section 40102 of title 49);

16 (B) an evaluation of current Federal, State, local, territorial, or
17 tribal law enforcement authorities to counter the threat identified
18 in subparagraph (A), and recommendations, if any, for potential
19 changes to existing authorities to allow State, local, territorial, and
20 tribal law enforcement to assist Federal law enforcement to
21 counter the threat where appropriate;

22 (C) an evaluation of the knowledge of, efficiency of, and effec-
23 tiveness of current procedures and resources available to owners
24 of critical infrastructure and domestic large hub airports when
25 they believe a threat from unmanned aircraft systems is present
26 and what additional actions, if any, the Department or the De-
27 partment of Transportation could implement under existing au-
28 thorities to assist these entities to counter the threat identified in
29 subparagraph (A);

30 (D) an assessment of what, if any, additional authorities are
31 needed by each Department and by law enforcement to counter
32 the threat identified in subparagraph (A); and

33 (E) an assessment of what, if any, additional research and de-
34 velopment the Department needs to counter the threat identified
35 in subparagraph (A).

36 (2) REPORT TO BE IN UNCLASSIFIED FORM.—The report shall be
37 submitted in unclassified form but may contain a classified annex.

38 (l) TERMINATION.—The authority to carry out this section with respect
39 to a covered facility or asset specified in subsection (a)(3) shall terminate
40 on November 18, 2023.

1 **§ 10405. Homeland security critical domain research and de-**
2 **velopment**

3 (a) DEFINITIONS.—In this section

4 (1) ECONOMIC SECURITY.— The term “economic security” means
5 the condition of having secure and resilient domestic production capac-
6 ity, combined with reliable access to the global resources necessary to
7 maintain an acceptable standard of living and to protect core national
8 values.

9 (2) UNITED STATES CRITICAL DOMAINS FOR ECONOMIC SECURITY.—
10 The term “United States critical domains for economic security” means
11 the critical infrastructure and other associated industries, technologies,
12 and intellectual property, or any combination thereof, that are essential
13 to the economic security of the United States.

14 (b) IN GENERAL.—

15 (1) RESEARCH AND DEVELOPMENT.—The Secretary may conduct re-
16 search and development to—

17 (A) identify United States critical domains for economic security
18 and homeland security; and

19 (B) evaluate the extent to which disruption, corruption, exploi-
20 tation, or dysfunction of any critical domain poses a substantial
21 threat to homeland security.

22 (2) REQUIREMENTS.—

23 (A) RISK ANALYSIS OF CRITICAL DOMAINS.—The research
24 under paragraph (1) shall include a risk analysis of each identified
25 United States critical domain for economic security to determine
26 the degree to which there exists a present or future threat to
27 homeland security in the event of disruption, corruption, exploi-
28 tation, or dysfunction to the domain. The research shall consider,
29 to the extent possible, the following:

30 (i) The vulnerability and resilience of relevant supply
31 chains.

32 (ii) Foreign production, processing, and manufacturing
33 methods.

34 (iii) Influence of malign economic actors.

35 (iv) Asset ownership.

36 (v) Relationships in the supply chains of the domains.

37 (vi) The degree to which the conditions referred to in
38 clauses (i) through (v) would place a domain at risk of dis-
39 ruption, corruption, exploitation, or dysfunction.

40 (B) ADDITIONAL RESEARCH INTO HIGH-RISK CRITICAL DO-
41 MAINS.—Based on the identification and risk analysis of United

1 States critical domains for economic security pursuant to para-
2 graph (1) and subparagraph (A), respectively, the Secretary may
3 conduct additional research into those critical domains, or specific
4 elements of those domains, with respect to which there exists the
5 highest degree of a present or future threat to homeland security
6 in the event of disruption, corruption, exploitation, or dysfunction
7 to a domain. For each high-risk domain, or element of a domain,
8 the research shall—

- 9 (i) describe the underlying infrastructure and processes;
10 (ii) analyze present and projected performance of industries
11 that comprise or support the domain;
12 (iii) examine the extent to which the supply chain of a
13 product or service necessary to the domain is concentrated,
14 either through a small number of sources, or if multiple
15 sources are concentrated in one geographic area;
16 (iv) examine the extent to which the demand for supplies
17 of goods and services of those industries can be fulfilled by
18 present and projected performance of other industries, iden-
19 tify strategies, plans, and potential barriers to expand the
20 supplier industrial base, and identify the barriers to the par-
21 ticipation of those other industries;
22 (v) consider each domain's performance capacities in stable
23 economic environments, under adversarial supply conditions,
24 and under crisis economic constraints;
25 (vi) identify and define needs and requirements to establish
26 supply resiliency within each domain; and
27 (vii) consider the effects of sector consolidation, including
28 foreign consolidation, either through mergers or acquisitions,
29 or due to recent geographic realignment, on those industries'
30 performances.

31 (3) CONSULTATION.—In conducting the research under paragraphs
32 (1) and (2)(B), the Secretary may consult with appropriate Federal
33 agencies, State agencies, and private sector stakeholders.

34 (4) PUBLICATION.— Beginning December 27, 2022, the Secretary
35 shall publish a report containing information relating to the research
36 under paragraphs (1) and (2)(B), including findings, evidence, analysis,
37 and recommendations. The report shall be updated annually through
38 2026.

39 (e) SUBMISSION OF REPORT TO CONGRESS.—Not later than 90 days after
40 the publication of each report required under subsection (b)(4), the Sec-
41 retary shall transmit to the Committee on Homeland Security of the House

1 of Representatives and the Committee on Homeland Security and Govern-
2 mental Affairs of the Senate the report, together with a description of ac-
3 tions the Secretary, in consultation with appropriate Federal agencies, will
4 undertake or has undertaken in response to the report.

5 (d) AUTHORIZATOIN OF APPROPRIATIONS.—There is authorized to be ap-
6 propriated \$1,000,000 for each of fiscal years 2023 through 2026 to carry
7 out this section.

8 **§ 10406. Department of Homeland Security Nonrecurring**
9 **Expenses Fund**

10 (a) ESTABLISHMENT.—There is in the Treasury the Department of
11 Homeland Security Nonrecurring Expenses Fund (in this section referred
12 to as “the Fund”).

13 (b) TRANSFER OF UNOBLIGATED BALANCES OF EXPIRED DISCRE-
14 TIONARY AMOUNTS.—Unobligated balances of expired discretionary
15 amounts appropriated for a fiscal year from the General Fund of the Treas-
16 ury to the Department by any Act may be transferred (not later than the
17 end of the 5th fiscal year after the last fiscal year for which the amounts
18 are available for the purposes for which appropriated) into the Fund.

19 (c) AVAILABILITY OF AMOUNTS.—Amounts deposited in the Fund shall
20 be available until expended, in addition to such other funds as may be avail-
21 able for those purposes, for information technology system modernization
22 and facilities infrastructure improvements necessary for the operation of the
23 Department, subject to approval by the Office of Management and Budget.

24 NOTIFICATION OF PLANNED USE OF AMOUNTS.—Amounts in the Fund
25 may be obligated only after the Committees on Appropriations of the House
26 of Representatives and the Senate are notified at least 15 days in advance
27 of the planned use of amounts.

28 **§ 10407. Mentor firm-protege firm program**

29 (a) DEFINITIONS.—In this section:

30 (1) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term
31 “historically Black college or university” has the meaning given the
32 term “part B institution” insection 322 of the Higher Education Act
33 of 1965 (20 U.S.C. 1061).

34 (2) MENTOR FIRM.—The term “mentor firm” means a for-profit
35 business concern that is not a small business concern that—

36 (A) has the ability to assist and commits to assisting a protege
37 to compete for Federal prime contracts and subcontracts; and

38 (B) satisfies any other requirements imposed by the Secretary.

39 (3) MINORITY-SERVING INSTITUTION.—The term “minority-serving
40 institution” means an institution of higher education described

1 insection 371(a) of the Higher Education Act of 1965 (20 U.S.C.
2 1067q(a)).

3 (4) PROTEGE FIRM.—The term “protege firm” means a small busi-
4 ness concern, a historically Black college or university, or a minority-
5 serving institution that—

6 (A) is eligible to enter into a prime contract or subcontract with
7 the Department; and

8 (B) satisfies any other requirements imposed by the Secretary.

9 (5) SMALL BUSINESS ACT DEFINITIONS.—The terms “small business
10 concern”, “small business concern owned and controlled by veterans”,
11 “small business concern owned and controlled by service-disabled vet-
12 erans”, “qualified HUBZone small business concern”, and
13 “smallbusiness concern owned and controlled by women” have the
14 meanings giventhe terms, respectively, undersection 3 of the Small
15 Business Act (15 U.S.C. 632). The term “small business concern
16 owned and controlled by socially and economically disadvantaged indi-
17 viduals” has the meaning given the term insection 8(d)(3)(C) of the
18 Small business Act (15 U.S.C. 637(d)(3)(C)).

19 (b) ESTABLISHMENT.—There is in the Department a mentor-protege pro-
20 gram (in this section referred to as the “Program”) under which a mentor
21 firm enters into an agreement with a protege firm for the purpose of assist-
22 ing the protege firm to compete for prime contracts and subcontracts of the
23 Department.

24 (c) ELIGIBILITY.—The Secretary shall establish criteria for mentor firms
25 and protege firms to be eligible to participate in the Program, including a
26 requirement that a firm is not included on any list maintained by the Fed-
27 eral Government of contractors that have been suspended or debarred.

28 (d) PROGRAM APPLICATION AND APPROVAL.—

29 (1) APPLICATION.— The Secretary, acting through the Office of
30 Small and Disadvantaged Business Utilization of the Department, shall
31 establish a process for submission of an application jointly by a mentor
32 firm and the protege firm selected by the mentor firm. The application
33 shall include each of the following:

34 (A) A description of the assistance to be provided by the mentor
35 firm, including, to the extent available, the number and a brief de-
36 scription of each anticipated subcontract to be awarded to the pro-
37 tege firm.

38 (B) A schedule with milestones for achieving the assistance to
39 be provided over the period of participation in the Program.

40 (C) An estimate of the costs to be incurred by the mentor firm
41 for providing assistance under the Program.

1 (D) Attestations that Program participants will submit to the
2 Secretary reports at times specified by the Secretary to assist the
3 Secretary in evaluating the protege firm's developmental progress.

4 (E) Attestations that Program participants will inform the Sec-
5 retary in the event of a change in eligibility or voluntary with-
6 drawal from the Program.

7 (2) APPROVAL.—Not later than 60 days after receipt of an applica-
8 tion pursuant to paragraph (1), the head of the Office of Small and
9 Disadvantaged Business Utilization shall notify applicants of approval
10 or, in the case of disapproval, the process for resubmitting an applica-
11 tion for reconsideration.

12 (3) RESCISSION.—The head of the Office of Small and Disadvan-
13 taged Business Utilization may rescind the approval of an application
14 under this subsection if it determines that the action is in the best in-
15 terest of the Department.

16 (e) PROGRAM DURATION.—A mentor firm and protege firm approved
17 under subsection (d) shall enter into an agreement to participate in the Pro-
18 gram for a period of not less than 36 months.

19 (f) PROGRAM BENEFITS.—A mentor firm and protege firm that enter
20 into an agreement under subsection (e) may receive the following Program
21 benefits:

22 (1) With respect to an award of a contract that requires a subcon-
23 tracting plan, a mentor firm may receive evaluation credit for partici-
24 pating in the Program.

25 (2) With respect to an award of a contract that requires a subcon-
26 tracting plan, a mentor firm may receive credit for a protege firm per-
27 forming as a first tier subcontractor or a subcontractor at any tier in
28 an amount equal to the total dollar value of any subcontracts awarded
29 to the protege firm.

30 (3) A protege firm may receive technical, managerial, financial, or
31 any other mutually agreed upon benefit from a mentor firm, including
32 a subcontract award.

33 (g) REPORTING.—Not later than December 23, 2023, and annually there-
34 after, the head of the Office of Small and Disadvantaged Business Utiliza-
35 tion shall submit to the Committee on Homeland Security and Govern-
36 mental Affairs and the Committee on Small Business and Entrepreneurship
37 of the Senate and the Committee on Homeland Security and the Committee
38 on Small Business of the House of Representatives a report that—

39 (1) identifies each agreement between a mentor firm and a protege
40 firm entered into under this section, including the number of protege
41 firm participants that are—

- 1 (A) small business concerns;
- 2 (B) small business concerns owned and controlled by veterans;
- 3 (C) small business concerns owned and controlled by service-dis-
- 4 abled veterans;
- 5 (D) qualified HUBZone small business concerns;
- 6 (E) small business concerns owned and controlled by socially
- 7 and economically disadvantaged individuals;
- 8 (F) small business concerns owned and controlled by women;
- 9 (G) historically Black colleges and universities; and
- 10 (H) minority-serving institutions;
- 11 (2) describes the type of assistance provided by mentor firms to pro-
- 12 tege firms;
- 13 (3) identifies contracts in the Department in which a mentor firm
- 14 serving as the prime contractor provided subcontracts to a protege firm
- 15 under the Program; and
- 16 (4) assesses the degree to which there has been—
- 17 (A) an increase in the technical capabilities of protege firms;
- 18 and
- 19 (B) an increase in the quantity and estimated value of prime
- 20 contract and subcontract awards to protege firms for the period
- 21 covered by the report.
- 22 (h) RULE OF CONSTRUCTION.—Nothing in this section may be construed
- 23 to limit, diminish, impair, or otherwise affect the authority of the Depart-
- 24 ment to participate in any program carried out by or requiring approval of
- 25 the Small Business Administration or adopt or follow any regulation or pol-
- 26 icy that the Administrator of the Small Business Administration may pro-
- 27 mulgate, except that, to the extent that any provision of this section (includ-
- 28 ing subsection (a)) conflicts with any other provision of law, regulation, or
- 29 policy, this section shall control. Bottom of Form Top of Form

30 **Chapter 105—Information Analysis**

Sec.

10501. Discharging responsibilities.
10502. Access to information.
10503. Terrorist travel program.
10504. Homeland Security Advisory System.
10505. Homeland security information sharing.
10506. Comprehensive information technology network architecture.
10507. Coordination with information sharing environment.
10508. Intelligence components.
10509. Training for employees of intelligence components.
10510. Intelligence training development for State and local government officials.
10511. Information sharing incentives.
10512. Department of Homeland Security State, Local, and Regional Fusion Center Initiative.
10513. Homeland Security Information Sharing Fellows Program.
10514. Rural Policing Institute.
10515. Interagency Threat Assessment and Coordination Group.

- 10516. Classified Information Advisory Officer.
- 10517. Annual report and briefing on intelligence activities of the Department.
- 10518. Data framework.
- 10519. Procedures for sharing information.
- 10520. Privacy Officer.

1 **§ 10501. Discharging responsibilities**

2 (a) IN GENERAL.—The Secretary shall ensure that the responsibilities of
3 the Department relating to information analysis, including those described
4 in subsection (b), are carried out through the Under Secretary for Intel-
5 ligence and Analysis.

6 (b) RESPONSIBILITIES OF SECRETARY.—The responsibilities of the Sec-
7 retary relating to intelligence and analysis shall be as follows:

8 (1) To access, receive, and analyze law enforcement information, in-
9 telligence information, and other information from agencies of the Fed-
10 eral Government, State and local government agencies (including law
11 enforcement agencies), and private-sector entities, and to integrate the
12 information, in support of the mission responsibilities of the Depart-
13 ment and the functions of the National Counterterrorism Center estab-
14 lished under section 119 of the National Security Act of 1947 (50
15 U.S.C. 3056), to—

16 (A) identify and assess the nature and scope of terrorist threats
17 to the homeland;

18 (B) detect and identify threats of terrorism against the United
19 States; and

20 (C) understand the threats in light of actual and potential
21 vulnerabilities of the homeland.

22 (2) To carry out comprehensive assessments of the vulnerabilities of
23 the key resources and critical infrastructure of the United States, in-
24 cluding the performance of risk assessments to determine the risks
25 posed by particular types of terrorist attacks within the United States
26 (including an assessment of the probability of success of attacks and
27 the feasibility and potential efficacy of various countermeasures to the
28 attacks).

29 (3) To integrate relevant information, analysis, and vulnerability as-
30 sessments (regardless of whether the information, analysis, or assess-
31 ments are provided by or produced by the Department) in order to—

32 (A) identify priorities for protective and support measures re-
33 garding terrorist and other threats to homeland security by the
34 Department, other agencies of the Federal Government, State and
35 local government agencies and authorities, the private sector, and
36 other entities; and

1 (B) prepare finished intelligence and information products in
2 both classified and unclassified formats, as appropriate, whenever
3 reasonably expected to be of benefit to a State, local, or tribal gov-
4 ernment (including a State, local, or tribal law enforcement agen-
5 cy) or a private-sector entity.

6 (4) To ensure, under section 10502 of this title, the timely and effi-
7 cient access by the Department to all information necessary to dis-
8 charge the responsibilities under this section, including obtaining the
9 information from other agencies of the Federal Government.

10 (5) To review, analyze, and make recommendations for improve-
11 ments to the policies and procedures governing the sharing of informa-
12 tion within the scope of the information sharing environment estab-
13 lished under section 11908 of this title, including homeland security in-
14 formation, terrorism information, and weapons of mass destruction in-
15 formation, and policies, guidelines, procedures, instructions, or stand-
16 ards established under that section.

17 (6) To disseminate, as appropriate, information analyzed by the De-
18 partment within the Department, to other agencies of the Federal Gov-
19 ernment with responsibilities relating to homeland security, and to
20 agencies of State and local governments and private-sector entities with
21 equivalent responsibilities in order to assist in the deterrence, preven-
22 tion, preemption of, or response to, terrorist attacks against the United
23 States.

24 (7) To consult with the Director of National Intelligence and other
25 appropriate intelligence, law enforcement, or other elements of the Fed-
26 eral Government to establish collection priorities and strategies for in-
27 formation, including law enforcement-related information, relating to
28 threats of terrorism against the United States through such means as
29 the representation of the Department in discussions regarding require-
30 ments and priorities in the collection of the information.

31 (8) To consult with State and local governments and private-sector
32 entities to ensure appropriate exchanges of information, including law
33 enforcement-related information, relating to threats of terrorism
34 against the United States.

35 (9) To ensure that—

36 (A) material received pursuant to this subtitle is protected from
37 unauthorized disclosure and handled and used only for the per-
38 formance of official duties; and

39 (B) intelligence information under this subtitle is shared, re-
40 tained, and disseminated consistent with the authority of the Di-
41 rector of National Intelligence to protect intelligence sources and

1 methods under the National Security Act of 1947 (50 U.S.C. 3001
2 et seq.) and related procedures and, as appropriate, similar au-
3 thorities of the Attorney General concerning sensitive law enforce-
4 ment information.

5 (10) To request additional information from other agencies of the
6 Federal Government, State and local government agencies, and the pri-
7 vate sector relating to threats of terrorism in the United States, or re-
8 lating to other areas of responsibility assigned by the Secretary, includ-
9 ing the entry into cooperative agreements through the Secretary to ob-
10 tain the information.

11 (11) To establish and utilize, in conjunction with the chief informa-
12 tion officer of the Department, a secure communications and informa-
13 tion technology infrastructure, including data-mining and other ad-
14 vanced analytical tools, in order to access, receive, and analyze data
15 and information in furtherance of the responsibilities under this sec-
16 tion, and to disseminate information acquired and analyzed by the De-
17 partment, as appropriate.

18 (12) To ensure, in conjunction with the chief information officer of
19 the Department, that information databases and analytical tools devel-
20 oped or utilized by the Department—

21 (A) are compatible with one another and with relevant informa-
22 tion databases of other agencies of the Federal Government; and

23 (B) treat information in the databases in a manner that com-
24 plies with applicable Federal law on privacy.

25 (13) To coordinate training and other support to the elements and
26 personnel of the Department, other agencies of the Federal Govern-
27 ment, and State and local governments that provide information to the
28 Department, or are consumers of information provided by the Depart-
29 ment, in order to facilitate the identification and sharing of information
30 revealed in their ordinary duties and the optimal utilization of informa-
31 tion received from the Department.

32 (14) To coordinate with elements of the intelligence community and
33 with Federal, State, and local law enforcement agencies, and the pri-
34 vate sector, as appropriate.

35 (15) To provide intelligence and information analysis and support to
36 other elements of the Department.

37 (16) To coordinate and enhance integration among the intelligence
38 components of the Department, including through strategic oversight of
39 the intelligence activities of the components.

40 (17) To establish the intelligence collection, processing, analysis, and
41 dissemination priorities, policies, processes, standards, guidelines, and

1 procedures for the intelligence components of the Department, con-
2 sistent with directions from the President and, as applicable, the Direc-
3 tor of National Intelligence.

4 (18) To establish a structure and process to support the missions
5 and goals of the intelligence components of the Department.

6 (19) To ensure that, whenever possible, the Department—

7 (A) produces and disseminates unclassified reports and analytic
8 products based on open-source information; and

9 (B) produces and disseminates the reports and analytic prod-
10 ucts contemporaneously with reports or analytic products con-
11 cerning the same or similar information that the Department pro-
12 duced and disseminated in a classified format.

13 (20) To establish within the Office of Intelligence and Analysis an
14 internal continuity of operations plan.

15 (21) Based on intelligence priorities set by the President, and guid-
16 ance from the Secretary and, as appropriate, the Director of National
17 Intelligence—

18 (A) to provide to the heads of each intelligence component of
19 the Department guidance for developing the budget pertaining to
20 the activities of the component; and

21 (B) to present to the Secretary a recommendation for a consoli-
22 dated budget for the intelligence components of the Department,
23 together with comments from the heads of the components.

24 (22) To perform such other duties relating to the responsibilities as
25 the Secretary may provide.

26 (23)(A) Not later than 6 months after December 23, 2016, to con-
27 duct an intelligence-based review and comparison of the risks and con-
28 sequences of EMP and GMD facing critical infrastructure and submit
29 to the Committee on Homeland Security and the Permanent Select
30 Committee on Intelligence of the House of Representatives and the
31 Committee on Homeland Security and Governmental Affairs and the
32 Select Committee on Intelligence of the Senate a recommended strategy
33 to protect and prepare the critical infrastructure of the homeland
34 against threats of EMP and GMD. The recommended strategy shall—

35 (i) be based on findings of the research and development con-
36 ducted under section 10918 of this title;

37 (ii) be developed in consultation with the relevant Federal Sec-
38 tor Risk Management Agencies (as defined under Presidential Pol-
39 icy Directive–21) for critical infrastructure;

40 (iii) be developed in consultation with the relevant sector coordi-
41 nating councils for critical infrastructure;

1 (iv) be informed, to the extent practicable, by the findings of the
2 intelligence-based review and comparison of the risks and con-
3 sequences of EMP and GMD facing critical infrastructure; and

4 (v) be submitted in unclassified form, but may include a classi-
5 fied annex.

6 (B) Not less frequently than every 2 years after the strategy is sub-
7 mitted, for the next 6 years, to submit updates of the recommended
8 strategy.

9 (C) The Secretary, if appropriate, may incorporate the recommended
10 strategy into a broader recommendation developed by the Department
11 to help protect and prepare critical infrastructure from terrorism,
12 cyberattacks, and other threats if, as incorporated, the recommended
13 strategy complies with subparagraph (A).

14 (c) STAFF.—

15 (1) IN GENERAL.—The Secretary shall provide the Office of Intel-
16 ligence and Analysis with a staff of analysts having appropriate exper-
17 tise and experience to assist the offices in discharging responsibilities
18 under this section.

19 (2) PRIVATE-SECTOR ANALYSTS.—Analysts under this subsection
20 may include analysts from the private sector.

21 (3) SECURITY CLEARANCES.—Analysts under this subsection shall
22 possess security clearances appropriate for their work under this sec-
23 tion.

24 (d) DETAIL OF PERSONNEL.—

25 (1) IN GENERAL.—To assist the Office of Intelligence and Analysis
26 in discharging responsibilities under this section, personnel of the agen-
27 cies listed in paragraph (2) may be detailed to the Department for the
28 performance of analytic functions and related duties.

29 (2) COVERED AGENCIES.—The agencies referred to in paragraph (1)
30 are as follows:

31 (A) The Department of State.

32 (B) The Central Intelligence Agency.

33 (C) The Federal Bureau of Investigation.

34 (D) The National Security Agency.

35 (E) The National Geospatial-Intelligence Agency.

36 (F) The Defense Intelligence Agency.

37 (G) Any other agency of the Federal Government that the
38 President considers appropriate.

39 (3) COOPERATIVE AGREEMENTS.—The Secretary and the head of the
40 agency concerned may enter into cooperative agreements for the pur-
41 pose of detailing personnel under this subsection.

1 (4) BASIS.—The detail of personnel under this subsection may be on
2 a reimbursable or non-reimbursable basis.

3 (e) FUNCTIONS TRANSFERRED.—The Secretary succeeds to, and there is
4 assigned to the Office of Intelligence and Analysis and the Office of Infra-
5 structure Protection, the functions, personnel, assets, and liabilities of the
6 following entities:

7 (1) The National Infrastructure Protection Center of the Federal
8 Bureau of Investigation (other than the Computer Investigations and
9 Operations Section), including the functions of the Attorney General
10 relating thereto.

11 (2) The National Communications System of the Department of De-
12 fense, including the functions of the Secretary of Defense relating
13 thereto.

14 (3) The Critical Infrastructure Assurance Office of the Department
15 of Commerce, including the functions of the Secretary of Commerce re-
16 lating thereto.

17 (4) The National Infrastructure Simulation and Analysis Center of
18 the Department of Energy and the energy security and assurance pro-
19 gram and activities of the Department of Energy, including the func-
20 tions of the Secretary of Energy relating thereto.

21 (5) The Federal Computer Incident Response Center of the General
22 Services Administration, including the functions of the Administrator
23 of General Services relating thereto.

24 **§ 10502. Access to information**

25 (a) IN GENERAL.—

26 (1) THREAT AND VULNERABILITY INFORMATION.—Except as other-
27 wise directed by the President, the Secretary shall have access the Sec-
28 retary considers necessary to all information, including reports, assess-
29 ments, analyses, and unevaluated intelligence relating to threats of ter-
30 rorism against the United States and to other areas of responsibility
31 assigned by the Secretary, and to all information concerning infrastruc-
32 ture or other vulnerabilities of the United States to terrorism, whether
33 or not the information has been analyzed, that may be collected, pos-
34 sessed, or prepared by an agency of the Federal Government.

35 (2) OTHER INFORMATION.—The Secretary also shall have access to
36 other information relating to matters under the responsibility of the
37 Secretary that may be collected, possessed, or prepared by an agency
38 of the Federal Government as the President may further provide.

39 (b) MANNER OF ACCESS.—Except as otherwise directed by the President,
40 with respect to information to which the Secretary has access under this
41 section—

1 (1) the Secretary may obtain the material upon request, and may
2 enter into cooperative arrangements with other executive agencies to
3 provide the material or provide Department officials with access to it
4 on a regular or routine basis, including requests or arrangements in-
5 volving broad categories of material, access to electronic databases, or
6 both; and

7 (2) regardless of whether the Secretary has made a request or en-
8 tered into a cooperative arrangement under paragraph (1), all agencies
9 of the Federal Government shall promptly provide to the Secretary—

10 (A) all reports (including information reports containing intel-
11 ligence which has not been fully evaluated), assessments, and ana-
12 lytical information relating to threats of terrorism against the
13 United States and to other areas of responsibility assigned by the
14 Secretary;

15 (B) all information concerning the vulnerability of the infra-
16 structure of the United States, or other vulnerabilities of the
17 United States, to terrorism, whether or not the information has
18 been analyzed;

19 (C) all other information relating to significant and credible
20 threats of terrorism against the United States, whether or not the
21 information has been analyzed; and

22 (D) other information or material as the President may direct.

23 (e) TREATMENT UNDER CERTAIN LAWS.—The Secretary shall be deemed
24 to be a Federal law enforcement, intelligence, protective, national defense,
25 immigration, or national security official, and shall be provided with all in-
26 formation from law enforcement agencies that is required to be given to the
27 Director of National Intelligence, under any provision of the following:

28 (1) The USA PATRIOT Act (Public Law 107–56, 115 Stat. 272).

29 (2) Section 2517(6) of title 18.

30 (3) Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure (18
31 U.S.C. App.).

32 (d) ACCESS TO INTELLIGENCE AND OTHER INFORMATION.—

33 (1) ACCESS BY ELEMENTS OF FEDERAL GOVERNMENT.—Nothing
34 in this chapter shall preclude an element of the intelligence community
35 (as that term is defined in section 3 of the National Security Act of
36 1947 (50 U.S.C. 3003)), or any other element of the Federal Govern-
37 ment with responsibility for analyzing terrorist threat information,
38 from receiving intelligence or other information relating to terrorism.

39 (2) SHARING OF INFORMATION.—The Secretary, in consultation
40 with the Director of National Intelligence, shall work to ensure that in-
41 telligence or other information relating to terrorism to which the De-

1 partment has access is appropriately shared with the elements of the
2 Federal Government referred to in paragraph (1), as well as with State
3 and local governments, as appropriate.

4 **§ 10503. Terrorist travel program**

5 (a) REQUIREMENT TO ESTABLISH.—The Secretary, in consultation with
6 the Director of the National Counterterrorism Center and consistent with
7 the strategy developed under section 7201 of the Intelligence Reform and
8 Terrorism Prevention Act of 2004 (Public Law 108–458, 50 U.S.C. 3056
9 note), shall establish a program to oversee the implementation of the Sec-
10 retary’s responsibilities with respect to terrorist travel.

11 (b) HEAD OF THE PROGRAM.—The Secretary shall designate an official
12 of the Department to be responsible for carrying out the program. The offi-
13 cial shall be—

- 14 (1) the Assistant Secretary for Policy; or
15 (2) an official appointed by the Secretary who reports directly to the
16 Secretary.

17 (c) DUTIES.—The official designated under subsection (b) shall assist the
18 Secretary in improving the Department’s ability to prevent terrorists from
19 entering the United States or remaining in the United States undetected
20 by—

- 21 (1) developing relevant strategies and policies;
22 (2) reviewing the effectiveness of existing programs and recom-
23 mending improvements, if necessary;
24 (3) making recommendations on budget requests and on the alloca-
25 tion of funding and personnel;
26 (4) ensuring effective coordination, with respect to policies, pro-
27 grams, planning, operations, and dissemination of intelligence and in-
28 formation relating to terrorist travel—

29 (A) among appropriate subdivisions of the Department, as de-
30 termined by the Secretary and including—

- 31 (i) U.S. Customs and Border Protection;
32 (ii) U.S. Immigration and Customs Enforcement;
33 (iii) U.S. Citizenship and Immigration Services;
34 (iv) the Transportation Security Administration; and
35 (v) the Coast Guard; and

36 (B) between the Department and other appropriate Federal
37 agencies; and

38 (5) serving as the Secretary’s primary point of contact with the Na-
39 tional Counterterrorism Center for implementing initiatives related to
40 terrorist travel and ensuring that the recommendations of the Center
41 related to terrorist travel are carried out by the Department.

1 **§ 10504. Homeland Security Advisory System**

2 (a) IN GENERAL.—The Secretary shall administer the Homeland Security
3 Advisory System under this section to provide advisories or warnings re-
4 garding the threat or risk that acts of terrorism will be committed on the
5 homeland to Federal, State, local, and tribal government authorities and to
6 the people of the United States, as appropriate. The Secretary shall exercise
7 primary responsibility for providing the advisories or warnings.

8 (b) REQUIRED ELEMENTS.—In administering the Homeland Security Ad-
9 visory System, the Secretary shall—

10 (1) establish criteria for the issuance and revocation of the advisories
11 or warnings;

12 (2) develop a methodology, relying on the criteria established under
13 paragraph (1), for the issuance and revocation of the advisories or
14 warnings;

15 (3) provide, in each advisory or warning, specific information and ad-
16 vice regarding appropriate protective measures and countermeasures
17 that may be taken in response to the threat or risk, at the maximum
18 level of detail practicable, to enable individuals, government entities,
19 emergency response providers, and the private sector to act appro-
20 priately;

21 (4) whenever possible, limit the scope of each advisory or warning
22 to a specific region, locality, or economic sector believed to be under
23 threat or at risk; and

24 (5) not, in issuing an advisory or warning, use color designations as
25 the exclusive means of specifying homeland security threat conditions
26 that are the subject of the advisory or warning.

27 **§ 10505. Homeland security information sharing**

28 (a) INFORMATION SHARING.—Consistent with section 11908 of this title,
29 the Secretary, acting through the Under Secretary for Intelligence and
30 Analysis, shall integrate the information and standardize the format of the
31 products of the intelligence components of the Department containing home-
32 land security information, terrorism information, weapons of mass destruc-
33 tion information, or national intelligence (as defined in section 3 of the Na-
34 tional Security Act of 1947 (50 U.S.C. 3003)) except for internal security
35 protocols or personnel information of the intelligence components, or other
36 administrative processes that are administered by any chief security officer
37 of the Department.

38 (b) INFORMATION SHARING AND KNOWLEDGE MANAGEMENT OFFI-
39 CERS.—For each intelligence component of the Department, the Secretary
40 shall designate an information sharing and knowledge management officer
41 who shall report to the Under Secretary for Intelligence and Analysis re-

1 garding coordinating the different systems used in the Department to gath-
2 er and disseminate homeland security information or national intelligence
3 (as defined in section 3 of the National Security Act of 1947 (50 U.S.C.
4 3003)).

5 (c) STATE, LOCAL, AND PRIVATE-SECTOR SOURCES OF INFORMATION.—

6 (1) ESTABLISHMENT OF BUSINESS PROCESSES.—The Secretary, act-
7 ing through the Director of the Cybersecurity and Infrastructure Secu-
8 rity Agency, as appropriate, shall—

9 (A) establish Department-wide procedures for the review and
10 analysis of information provided by State, local, and tribal govern-
11 ments and the private sector;

12 (B) as appropriate, integrate the information into the informa-
13 tion gathered by the Department and other departments and agen-
14 cies of the Federal Government; and

15 (C) make available the information, as appropriate, within the
16 Department and to other departments and agencies of the Federal
17 Government.

18 (2) FEEDBACK.—The Secretary shall develop mechanisms to provide
19 feedback regarding the analysis and utility of information provided by
20 an entity of State, local, or tribal government or the private sector that
21 provides the information to the Department.

22 (d) TRAINING AND EVALUATION OF EMPLOYEES.—

23 (1) TRAINING.—The Secretary, acting through the Under Secretary
24 for Intelligence and Analysis or the Director of the Cybersecurity and
25 Infrastructure Security Agency, as appropriate, shall provide to em-
26 ployees of the Department opportunities for training and education to
27 develop an understanding of—

28 (A) the definitions of homeland security information and na-
29 tional intelligence (as defined in section 3 of the National Security
30 Act of 1947 (50 U.S.C. 3003)); and

31 (B) how information available to the employees as part of their
32 duties—

33 (i) might qualify as homeland security information or na-
34 tional intelligence; and

35 (ii) might be relevant to the Office of Intelligence and
36 Analysis and the intelligence components of the Department.

37 (2) EVALUATIONS.—The Under Secretary for Intelligence and Anal-
38 ysis shall—

39 (A) on an ongoing basis, evaluate how employees of the Office
40 of Intelligence and Analysis and the intelligence components of the
41 Department are utilizing homeland security information or na-

1 tional intelligence, sharing information within the Department, as
2 described in this title, and participating in the information sharing
3 environment established under section 11908 of this title; and

4 (B) provide to the appropriate component heads regular reports
5 regarding the evaluations under subparagraph (A).

6 (e) RECEIPT OF INFORMATION FROM UNITED STATES SECRET SERV-
7 ICE.—

8 (1) IN GENERAL.—The Under Secretary for Intelligence and Anal-
9 ysis shall receive from the United States Secret Service homeland secu-
10 rity information, terrorism information, weapons of mass destruction
11 information (as these terms are defined in section 11908 of this title),
12 or national intelligence (as defined in section 3 of the National Security
13 Act of 1947 (50 U.S.C. 3003)), as well as suspect information obtained
14 in criminal investigations. The United States Secret Service shall co-
15 operate with the Under Secretary for Intelligence and Analysis with re-
16 spect to activities under this section and section 10506 of this title.

17 (2) SAVINGS CLAUSE.—Nothing in the Implementing Recommenda-
18 tions of the 9/11 Commission Act of 2007 (Public Law 110–53, 121
19 Stat. 266) shall interfere with the operation of section 3056(g) of title
20 18, or with the authority of the Secretary or the Director of the United
21 States Secret Service regarding the budget of the United States Secret
22 Service.

23 **§ 10506. Comprehensive information technology network ar-**
24 **chitecture**

25 (a) DEFINITION OF COMPREHENSIVE INFORMATION TECHNOLOGY NET-
26 WORK ARCHITECTURE.—The term “comprehensive information technology
27 network architecture” means an integrated framework for evolving or main-
28 taining existing information technology and acquiring new information tech-
29 nology to achieve the strategic management and information resources man-
30 agement goals of the Office of Intelligence and Analysis.

31 (b) ESTABLISHMENT.—The Secretary, acting through the Under Sec-
32 retary for Intelligence and Analysis, shall establish, consistent with the poli-
33 cies and procedures developed under section 11908 of this title, and con-
34 sistent with the enterprise architecture of the Department, a comprehensive
35 information technology network architecture for the Office of Intelligence
36 and Analysis that connects the various databases and related information
37 technology assets of the Office of Intelligence and Analysis and the intel-
38 ligence components of the Department in order to promote internal informa-
39 tion sharing among the intelligence and other personnel of the Department.

1 **§ 10507. Coordination with information sharing environ-**
2 **ment**

3 (a) GUIDANCE.—All activities to comply with sections 10504, 10505, and
4 10506 of this title shall be—

5 (1) consistent with policies, guidelines, procedures, instructions, or
6 standards established under section 11908 of this title;

7 (2) implemented in coordination with, as appropriate, the program
8 manager for the information sharing environment established under
9 that section;

10 (3) consistent with applicable guidance issued by the Director of Na-
11 tional Intelligence; and

12 (4) consistent with applicable guidance issued by the Secretary relat-
13 ing to the protection of law enforcement information or proprietary in-
14 formation.

15 (b) CONSULTATION.—In carrying out the duties and responsibilities
16 under this chapter, the Under Secretary for Intelligence and Analysis shall
17 take into account the views of the heads of the intelligence components of
18 the Department.

19 **§ 10508. Intelligence components**

20 Subject to the direction and control of the Secretary, and consistent with
21 applicable guidance issued by the Director of National Intelligence, the re-
22 sponsibilities of the head of each intelligence component of the Department
23 are as follows:

24 (1) To ensure that the collection, processing, analysis, and dissemi-
25 nation of information within the scope of the information sharing envi-
26 ronment, including homeland security information, terrorism informa-
27 tion, weapons of mass destruction information, and national intelligence
28 (as defined in section 3 of the National Security Act of 1947 (50
29 U.S.C. 3003)), are carried out effectively and efficiently in support of
30 the intelligence mission of the Department, as led by the Under Sec-
31 retary for Intelligence and Analysis.

32 (2) To otherwise support and implement the intelligence mission of
33 the Department, as led by the Under Secretary for Intelligence and
34 Analysis.

35 (3) To incorporate the input of the Under Secretary for Intelligence
36 and Analysis with respect to performance appraisals, bonus or award
37 recommendations, pay adjustments, and other forms of commendation.

38 (4) To coordinate with the Under Secretary for Intelligence and
39 Analysis in developing policies and requirements for the recruitment
40 and selection of intelligence officials of the intelligence component.

1 (5) To advise and coordinate with the Under Secretary for Intel-
2 ligence and Analysis on any plan to reorganize or restructure the intel-
3 ligence component that would, if implemented, result in realignments
4 of intelligence functions.

5 (6) To ensure that employees of the intelligence component have
6 knowledge of, and comply with, the programs and policies established
7 by the Under Secretary for Intelligence and Analysis and other appro-
8 priate officials of the Department and that the employees comply with
9 all applicable laws and regulations.

10 (7) To perform other activities relating to the responsibilities the
11 Secretary may provide.

12 **§ 10509. Training for employees of intelligence components**

13 The Secretary shall provide training and guidance for employees, officials,
14 and senior executives of the intelligence components of the Department to
15 develop knowledge of laws, regulations, operations, policies, procedures, and
16 programs that are related to the functions of the Department relating to
17 the collection, processing, analysis, and dissemination of information within
18 the scope of the information sharing environment, including homeland secu-
19 rity information, terrorism information, and weapons of mass destruction
20 information, or national intelligence (as the term is defined in section 3 of
21 the National Security Act of 1947 (50 U.S.C. 3003)).

22 **§ 10510. Intelligence training development for State and**
23 **local government officials**

24 (a) CURRICULUM.—The Secretary, acting through the Under Secretary
25 for Intelligence and Analysis, shall—

26 (1) develop a curriculum for training State, local, and tribal govern-
27 ment officials, including law enforcement officers, intelligence analysts,
28 and other emergency response providers, in the intelligence cycle and
29 Federal laws, practices, and regulations regarding the development,
30 handling, and review of intelligence and other information; and

31 (2) ensure that the curriculum includes executive level training for
32 senior level State, local, and tribal law enforcement officers, intelligence
33 analysts, and other emergency response providers.

34 (b) TRAINING.—To the extent possible, the Federal Law Enforcement
35 Training Center and other existing Federal entities with the capacity and
36 expertise to train State, local, and tribal government officials based on the
37 curriculum developed under subsection (a) shall be used to carry out the
38 training programs created under this section. If the entities do not have the
39 capacity, resources, or capabilities to conduct the training, the Secretary
40 may approve another entity to conduct the training.

1 (c) CONSULTATION.—In carrying out the duties described in subsection
2 (a), the Under Secretary for Intelligence and Analysis shall consult with the
3 Director of the Federal Law Enforcement Training Center, the Attorney
4 General, the Director of National Intelligence, the Administrator of the Fed-
5 eral Emergency Management Agency, and other appropriate parties, such
6 as private industry, institutions of higher education, nonprofit institutions,
7 and other intelligence agencies of the Federal Government.

8 **§ 10511. Information sharing incentives**

9 (a) AWARDS.—In making cash awards under chapter 45 of title 5, the
10 President or the head of an agency, in consultation with the program man-
11 ager designated under section 11908 of this title, may consider the success
12 of an employee in appropriately sharing information within the scope of the
13 information sharing environment established under that section, including
14 homeland security information, terrorism information, and weapons of mass
15 destruction information, or national intelligence (as defined in section 3 of
16 the National Security Act of 1947 (50 U.S.C. 3003)), in a manner con-
17 sistent with policies, guidelines, procedures, instructions, or standards estab-
18 lished by the President or, as appropriate, the program manager of that en-
19 vironment for the implementation and management of that environment.

20 (b) OTHER INCENTIVES.—The head of each department or agency de-
21 scribed in section 11908(f), in consultation with the program manager des-
22 ignated under section 11908, shall adopt best practices regarding effective
23 ways to educate and motivate officers and employees of the Federal Govern-
24 ment to participate fully in the information sharing environment, includ-
25 ing—

26 (1) promotions and other nonmonetary awards; and

27 (2) the publicizing of information sharing accomplishments by indi-
28 vidual employees and, where appropriate, the tangible end benefits that
29 resulted.

30 **§ 10512. Department of Homeland Security State, Local, and** 31 **Regional Fusion Center Initiative**

32 (a) DEFINITIONS.—In this section:

33 (1) FUSION CENTER.—The term “fusion center” means a collabo-
34 rative effort of two or more Federal, State, local, or tribal government
35 agencies that combines resources, expertise, or information with the
36 goal of maximizing the ability of the agencies to detect, prevent, inves-
37 tigate, apprehend, and respond to criminal or terrorist activity.

38 (2) INFORMATION SHARING ENVIRONMENT.—The term “information
39 sharing environment” means the information sharing environment es-
40 tablished under section 11908 of this title.

1 (3) INTELLIGENCE ANALYST.—The term “intelligence analyst”
2 means an individual who regularly advises, administers, supervises, or
3 performs work in the collection, gathering, analysis, evaluation, report-
4 ing, production, or dissemination of information on political, economic,
5 social, cultural, physical, geographical, scientific, or military conditions,
6 trends, or forces in foreign or domestic areas that directly or indirectly
7 affect national security.

8 (4) INTELLIGENCE-LED POLICING.—The term “intelligence-led polic-
9 ing” means the collection and analysis of information to produce an in-
10 telligence end product designed to inform law enforcement decision-
11 making at the tactical and strategic levels.

12 (5) TERRORISM INFORMATION.—The term “terrorism information”
13 has the meaning given the term in section 11908 of this title.

14 (b) ESTABLISHMENT.—The Secretary, in consultation with the program
15 manager of the information sharing environment established under section
16 11908 of this title, the Attorney General, the Privacy Officer of the Depart-
17 ment, the Officer for Civil Rights and Civil Liberties of the Department,
18 and the Privacy and Civil Liberties Oversight Board established under sec-
19 tion 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004
20 (42 U.S.C. 2000ee), shall establish a Department of Homeland Security
21 State, Local, and Regional Fusion Center Initiative to establish partnerships
22 with State, local, and regional fusion centers.

23 (c) DEPARTMENT SUPPORT AND COORDINATION.—Through the Depart-
24 ment of Homeland Security State, Local, and Regional Fusion Center Ini-
25 tiative, and in coordination with the principal officials of participating State,
26 local, or regional fusion centers and the officers designated as the Homeland
27 Security Advisors of the States, the Secretary shall—

28 (1) provide operational and intelligence advice and assistance to
29 State, local, and regional fusion centers;

30 (2) support efforts to include State, local, and regional fusion centers
31 in efforts to establish an information sharing environment;

32 (3) conduct tabletop and live training exercises to regularly assess
33 the capability of individual and regional networks of State, local, and
34 regional fusion centers to integrate the efforts of the networks with the
35 efforts of the Department;

36 (4) coordinate with other relevant Federal entities engaged in home-
37 land security-related activities;

38 (5) provide analytic and reporting advice and assistance to State,
39 local, and regional fusion centers;

40 (6) review information within the scope of the information sharing
41 environment, including homeland security information, terrorism infor-

1 mation, and weapons of mass destruction information, that is gathered
2 by State, local, and regional fusion centers, and to incorporate the in-
3 formation, as appropriate, into the Department's own information;

4 (7) provide management assistance to State, local, and regional fu-
5 sion centers;

6 (8) serve as a point of contact to ensure the dissemination of infor-
7 mation within the scope of the information sharing environment, in-
8 cluding homeland security information, terrorism information, and
9 weapons of mass destruction information;

10 (9) facilitate close communication and coordination between State,
11 local, and regional fusion centers and the Department;

12 (10) provide State, local, and regional fusion centers with expertise
13 on Department resources and operations;

14 (11) provide training to State, local, and regional fusion centers and
15 encourage the fusion centers to participate in terrorism threat-related
16 exercises conducted by the Department; and

17 (12) carry out other duties the Secretary determines are appropriate.

18 (d) PERSONNEL ASSIGNMENT.—

19 (1) IN GENERAL.—The Under Secretary for Intelligence and Anal-
20 ysis shall, to the maximum extent practicable, assign officers and intel-
21 ligence analysts from components of the Department to participating
22 State, local, and regional fusion centers.

23 (2) PERSONNEL SOURCES.—Officers and intelligence analysts as-
24 signed to participating fusion centers under this subsection may be as-
25 signed from the following Department components, in coordination with
26 the respective component head and in consultation with the principal
27 officials of participating fusion centers:

28 (A) Office of Intelligence and Analysis.

29 (B) Cybersecurity and Infrastructure Security Agency.

30 (C) Transportation Security Administration.

31 (D) U.S. Customs and Border Protection.

32 (E) U.S. Immigration and Customs Enforcement.

33 (F) Coast Guard.

34 (G) Other components of the Department, as determined by the
35 Secretary.

36 (3) QUALIFYING CRITERIA.—

37 (A) IN GENERAL.—The Secretary shall develop qualifying cri-
38 teria for a fusion center to participate in the assigning of Depart-
39 ment officers or intelligence analysts under this section.

40 (B) CRITERIA.—Criteria developed under subparagraph (A)
41 may include—

1 (i) whether the fusion center, through its mission and gov-
2 ernance structure, focuses on a broad counterterrorism ap-
3 proach, and whether that broad approach is pervasive
4 through all levels of the organization;

5 (ii) whether the fusion center has sufficient numbers of
6 adequately trained personnel to support a broad counterter-
7 rorism mission;

8 (iii) whether the fusion center has—

9 (I) access to relevant law-enforcement, emergency-re-
10 sponse, private-sector, open-source, and national-security
11 data; and

12 (II) the ability to share and analytically utilize that
13 data for lawful purposes;

14 (iv) whether the fusion center is adequately funded by the
15 State, local, or regional government to support its counterter-
16 rorism mission; and

17 (v) the relevancy of the mission of the fusion center to the
18 particular source component of Department officers or intel-
19 ligence analysts.

20 (4) PREREQUISITE.—

21 (A) INTELLIGENCE ANALYSIS, PRIVACY, AND CIVIL LIBERTIES
22 TRAINING.—Before being assigned to a fusion center under this
23 section, an officer or intelligence analyst shall undergo—

24 (i) appropriate intelligence analysis or information sharing
25 training using an intelligence-led policing curriculum that is
26 consistent with—

27 (I) standard training and education programs offered
28 to Department law enforcement and intelligence per-
29 sonnel; and

30 (II) the Criminal Intelligence Systems Operating Poli-
31 cies under part 23 of title 28, Code of Federal Regula-
32 tions (or any corresponding similar rule or regulation);

33 (ii) appropriate privacy and civil liberties training that is
34 developed, supported, or sponsored by the Privacy Officer ap-
35 pointed under section 10520 of this title and the Officer for
36 Civil Rights and Civil Liberties of the Department, in con-
37 sultation with the Privacy and Civil Liberties Oversight
38 Board established under section 1061 of the Intelligence Re-
39 form and Terrorism Prevention Act of 2004 (42 U.S.C.
40 2000ee); and

1 (iii) other training prescribed by the Under Secretary for
2 Intelligence and Analysis.

3 (B) PRIOR WORK EXPERIENCE IN AREA.—In determining the
4 eligibility of an officer or intelligence analyst to be assigned to a
5 fusion center under this section, the Under Secretary for Intel-
6 ligence and Analysis shall consider the familiarity of the officer or
7 intelligence analyst with the State, locality, or region, as deter-
8 mined by such factors as whether the officer or intelligence ana-
9 lyst—

10 (i) has been previously assigned in the geographic area; or

11 (ii) has previously worked with intelligence officials or law
12 enforcement or other emergency response providers from that
13 State, locality, or region.

14 (5) EXPEDITED SECURITY CLEARANCE PROCESSING.—The Under
15 Secretary for Intelligence and Analysis—

16 (A) shall ensure that each officer or intelligence analyst as-
17 signed to a fusion center under this section has the appropriate
18 security clearance to contribute effectively to the mission of the fu-
19 sion center; and

20 (B) may request that security clearance processing be expedited
21 for each officer or intelligence analyst and may use available funds
22 for this purpose.

23 (6) ADDITIONAL QUALIFICATIONS.—Each officer or intelligence ana-
24 lyst assigned to a fusion center under this section shall satisfy any
25 other qualifications the Under Secretary for Intelligence and Analysis
26 may prescribe.

27 (e) RESPONSIBILITIES.—An officer or intelligence analyst assigned to a
28 fusion center under this section shall—

29 (1) assist law enforcement agencies and other emergency response
30 providers of State, local, and tribal governments and fusion center per-
31 sonnel in using information within the scope of the information sharing
32 environment, including homeland security information, terrorism infor-
33 mation, and weapons of mass destruction information, to develop a
34 comprehensive and accurate threat picture;

35 (2) review homeland security-relevant information from law enforce-
36 ment agencies and other emergency response providers of State, local,
37 and tribal government;

38 (3) create intelligence and other information products derived from
39 the information and other homeland security-relevant information pro-
40 vided by the Department; and

1 (4) assist in the dissemination of the products, as coordinated by the
2 Under Secretary for Intelligence and Analysis, to law enforcement
3 agencies and other emergency response providers of State, local, and
4 tribal government, other fusion centers, and appropriate Federal agen-
5 cies.

6 (f) BORDER INTELLIGENCE PRIORITY.—

7 (1) IN GENERAL.—The Secretary shall make it a priority to assign
8 officers and intelligence analysts under this section from U.S. Customs
9 and Border Protection, U.S. Immigration and Customs Enforcement,
10 and the Coast Guard to participating State, local, and regional fusion
11 centers located in jurisdictions along land or maritime borders of the
12 United States in order to enhance the integrity of and security at the
13 borders by helping Federal, State, local, and tribal law enforcement au-
14 thorities to identify, investigate, and otherwise interdict persons, weap-
15 ons, and related contraband that pose a threat to homeland security.

16 (2) BORDER INTELLIGENCE PRODUCTS.—When performing the re-
17 sponsibilities described in subsection (e), officers and intelligence ana-
18 lysts assigned to participating State, local, and regional fusion centers
19 under this section shall have, as a primary responsibility, the creation
20 of border intelligence products that—

21 (A) assist State, local, and tribal law enforcement agencies in
22 deploying their resources most efficiently to help detect and inter-
23 dict terrorists, weapons of mass destruction, and related contra-
24 band at land or maritime borders of the United States;

25 (B) promote more consistent and timely sharing of border secu-
26 rity-relevant information among jurisdictions along land or mari-
27 time borders of the United States; and

28 (C) enhance the Department's situational awareness of the
29 threat of acts of terrorism at or involving the land or maritime
30 borders of the United States.

31 (g) DATABASE ACCESS.—To fulfill the objectives described under sub-
32 section (e), each officer or intelligence analyst assigned to a fusion center
33 under this section shall have appropriate access to all relevant Federal data-
34 bases and information systems, consistent with policies, guidelines, proce-
35 dures, instructions, or standards established by the President or, as appro-
36 priate, the program manager of the information sharing environment for the
37 implementation and management of that environment.

38 (h) CONSUMER FEEDBACK.—

39 (1) IN GENERAL.—The Secretary shall create a voluntary mechanism
40 for a State, local, or tribal law enforcement officer or other emergency
41 response provider who is a consumer of the intelligence or other infor-

1 information products referred to in subsection (e) to provide feedback to the
2 Department on the quality and utility of the intelligence products.

3 (2) REPORT.—The Secretary shall submit annually to the Committee
4 on Homeland Security and Governmental Affairs of the Senate and the
5 Committee on Homeland Security of the House of Representatives a
6 report that includes a description of the consumer feedback obtained
7 under paragraph (1) and, if applicable, how the Department has ad-
8 justed its production of intelligence products in response to that con-
9 sumer feedback.

10 (i) RULE OF CONSTRUCTION.—

11 (1) IN GENERAL.—The authorities granted under this section shall
12 supplement the authorities granted under section 10501(b) of this title,
13 and nothing in this section shall be construed to abrogate the authori-
14 ties granted under section 10501(b).

15 (2) PARTICIPATION.—Nothing in this section shall be construed to
16 require a State, local, or regional government or entity to accept the
17 assignment of officers or intelligence analysts of the Department into
18 the fusion center of that State, locality, or region.

19 (j) GUIDELINES.—The Secretary, in consultation with the Attorney Gen-
20 eral, shall establish guidelines for fusion centers created and operated by
21 State and local governments, to include standards that a fusion center
22 shall—

23 (1) collaboratively develop a mission statement, identify expectations
24 and goals, measure performance, and determine effectiveness for that
25 fusion center;

26 (2) create a representative governance structure that includes law
27 enforcement officers and other emergency response providers and, as
28 appropriate, the private sector;

29 (3) create a collaborative environment for the sharing of intelligence
30 and information among Federal, State, local, and tribal government
31 agencies (including law enforcement officers and other emergency re-
32 sponse providers), the private sector, and the public, consistent with
33 policies, guidelines, procedures, instructions, or standards established
34 by the President or, as appropriate, the program manager of the infor-
35 mation sharing environment;

36 (4) leverage the databases, systems, and networks available from
37 public- and private-sector entities, in accordance with all applicable
38 laws, to maximize information sharing;

39 (5) develop, publish, and adhere to a privacy and civil liberties policy
40 consistent with Federal, State, and local law;

1 (6) provide, in coordination with the Privacy Officer of the Depart-
2 ment and the Officer for Civil Rights and Civil Liberties of the Depart-
3 ment, appropriate privacy and civil liberties training for all State, local,
4 tribal, and private-sector representatives at the fusion center;

5 (7) ensure appropriate security measures are in place for the facility,
6 data, and personnel;

7 (8) select and train personnel based on the needs, mission, goals, and
8 functions of that fusion center;

9 (9) offer a variety of intelligence and information services and prod-
10 ucts to recipients of fusion center intelligence and information; and

11 (10) incorporate law enforcement officers, other emergency response
12 providers, and, as appropriate, the private sector, into all relevant
13 phases of the intelligence and fusion process, consistent with the mis-
14 sion statement developed under paragraph (1), either through full-time
15 representatives or liaison relationships with the fusion center to enable
16 the receipt and sharing of information and intelligence.

17 (k) Fusion Center Information Sharing Strategy.—Not later than 1 year
18 after March 2, 2020, and not less frequently than once every 5 years there-
19 after, the Secretary shall develop or update a strategy for Department en-
20 gagement with fusion centers. The strategy shall be developed and updated
21 in consultation with the heads of intelligence components of the Depart-
22 ment, the Chief Privacy Officer, the Officer for Civil Rights and Civil Lib-
23 erties, officials of fusion centers, officers designated as Homeland Security
24 Advisors, and the heads of other relevant agencies, as appropriate. The
25 strategy shall include the following:

26 (1) Specific goals and objectives for sharing information and engag-
27 ing with fusion centers through—

28 (A) the direct deployment of personnel from intelligence compo-
29 nents of the Department;

30 (B) the use of Department unclassified and classified informa-
31 tion sharing systems, including the Homeland Security Informa-
32 tion Network and the Homeland Secure Data Network, or any
33 successor systems; and

34 (C) any additional means.

35 (2) The performance metrics to be used to measure success in
36 achieving the goals and objectives referred to in paragraph (1).

37 (3) A 5-year plan for continued engagement with fusion centers.

38 (l) THREAT INFORMATION SHARING

39 (1) DEFINITIONS.—In this subsection:

1 (A) SURFACE TRANSPORTATION ASSET.—The term “surface
2 transportation asset” includes facilities, equipment, or systems
3 used to provide transportation services by—

4 (i) a public transportation agency (as that term is defined
5 insection 40501 of this title);

6 (ii) a railroad carrier (as that term is defined insection
7 20102(3) of title 49);

8 (iii) an owner or operator of—

9 (I) an entity offering scheduled, fixed-route transpor-
10 tation services by over-the-road bus (as that term is de-
11 fined insection 40701 of this title); or

12 (II) a bus terminal; or

13 (iv) other transportation facilities, equipment, or systems,
14 as determined by the Secretary.

15 (B) TARGETED VIOLENCE.—The term “targeted violence”
16 means an incident of violence in which an attacker selected a par-
17 ticular target to inflict mass injury or death with no discernable
18 political or ideological motivation beyond mass injury or death.

19 (C) TERRORISM.—The term “terrorism” means—

20 (i) domestic terrorism (as that term is defined insection
21 2331(5) of title 18); and

22 (ii) international terrorism (as that term is defined
23 insection 2331(1) of title 18).

24 (2) PRIORIZATION OF ASSIGNMENT OF OFFICERS AND INTEL-
25 LIGENCE OFFICERS.—The Secretary shall prioritize the assignment of
26 officers and intelligence analysts underthis section from the Transpor-
27 tation Security Administration and, as appropriate, from the Office of
28 Intelligence and Analysis of the Department, to locations with partici-
29 pating State, local, and regional fusion centers in jurisdictions with a
30 high-risk surface transportation asset to enhance the security of those
31 assets, including by improving timely sharing, in a manner consistent
32 with the protection of privacy rights, civil rights, and civil liberties, of
33 information regarding threats of terrorism and other threats, including
34 targeted violence.

35 (3) INTELLIGENCE PRODUCTS.—Officers and intelligence analysts
36 assigned to locations with participating State, local, and regional fusion
37 centers under this subsection shall participate in the generation and
38 dissemination, to surface transportation assets, of transportation secu-
39 rity intelligence products, with an emphasis on those products that re-
40 late to threats of terrorism and other threats, including targeted vio-
41 lence, that—

1 (A) assist State, local, and Tribal law enforcement agencies in
2 deploying their resources, including personnel, most efficiently to
3 help detect, prevent, investigate, apprehend, and respond to the
4 threats;

5 (B) promote more consistent and timely sharing with and
6 among jurisdictions of threat information; and

7 (C) enhance the Department's situational awareness of the
8 threats.

9 (4) CLEARANCES.—The Secretary shall make available to appro-
10 priate owners and operators of surface transportation assets, and to
11 any other person that the Secretary determines appropriate to foster
12 greater sharing of classified information relating to threats of terrorism
13 and other threats, including targeted violence, to surface transportation
14 assets, the process of application for security clearances under Execu-
15 tive Order No. 13549 (Aug. 18, 2010, 75 Fed. Reg. 51609) or any suc-
16 cessor Executive order.

17 (5) REPORTS TO CONGRESS.—

18 (A) SECRETARY.—Not later than December 27, 2022, the Sec-
19 retary shall submit to the Committee on Homeland Security of the
20 House of Representatives and the Committee on Homeland Secu-
21 rity and Governmental Affairs of the Senate a report that includes
22 a detailed description of the measures used to ensure privacy
23 rights, civil rights, and civil liberties protections in carrying out
24 this subsection.

25 (B) COMPTROLLER GENERAL.—Not later than December 27,
26 2023, the Comptroller General shall submit to the Committee on
27 Homeland Security of the House of Representatives and the Com-
28 mittee on Homeland Security and Governmental Affairs of the
29 Senate a review of the implementation of this subsection, including
30 an assessment of the measures used to ensure privacy rights, civil
31 rights, and civil liberties protections, and any recommendations to
32 improve this implementation, together with any recommendations
33 to improve information sharing with State, local, Tribal, terri-
34 torial, and private sector entities to prevent, identify, and respond
35 to threats of terrorism and other threats, including targeted vio-
36 lence, to surface transportation assets.

37 **§ 10513. Homeland Security Information Sharing Fellows**
38 **Program**

39 (a) ESTABLISHMENT.—The Secretary, acting through the Under Sec-
40 retary for Intelligence and Analysis, and in consultation with the Chief

1 Human Capital Officer, shall establish the Homeland Security Information
2 Sharing Fellows Program for the purpose of—

3 (1) detailing State, local, and tribal law enforcement officers and in-
4 telligence analysts to the Department in accordance with subchapter VI
5 of chapter 33 of title 5, to participate in the work of the Office of Intel-
6 ligence and Analysis in order to become familiar with—

7 (A) the relevant missions and capabilities of the Department
8 and other Federal agencies; and

9 (B) the role, programs, products, and personnel of the Office of
10 Intelligence and Analysis; and

11 (2) promoting information sharing between the Department and
12 State, local, and tribal law enforcement officers and intelligence ana-
13 lysts by assigning the officers and analysts to—

14 (A) serve as a point of contact in the Department to assist in
15 the representation of State, local, and tribal information require-
16 ments;

17 (B) identify information within the scope of the information
18 sharing environment, including homeland security information, ter-
19 rorism information, and weapons of mass destruction information,
20 that is of interest to State, local, and tribal law enforcement offi-
21 cers, intelligence analysts, and other emergency response pro-
22 viders;

23 (C) assist Department analysts in preparing and disseminating
24 products derived from information within the scope of the informa-
25 tion sharing environment, including homeland security informa-
26 tion, terrorism information, and weapons of mass destruction in-
27 formation, that are tailored to State, local, and tribal law enforce-
28 ment officers and intelligence analysts and designed to prepare for
29 and thwart acts of terrorism; and

30 (D) assist Department analysts in preparing products derived
31 from information within the scope of the information sharing envi-
32 ronment, including homeland security information, terrorism infor-
33 mation, and weapons of mass destruction information, that are
34 tailored to State, local, and tribal emergency response providers
35 and assist in the dissemination of the products through appro-
36 priate Department channels.

37 (b) ELIGIBILITY.—To be eligible for selection as an Information Sharing
38 Fellow under the Homeland Security Information Sharing Fellows Program,
39 an individual shall—

40 (1) have homeland security-related responsibilities;

41 (2) be eligible for an appropriate security clearance;

1 (3) possess a valid need for access to classified information, as deter-
2 mined by the Under Secretary for Intelligence and Analysis;

3 (4) be an employee of—

4 (A) a State, local, or regional fusion center;

5 (B) a State or local law enforcement or other government entity
6 that serves a major metropolitan area, suburban area, or rural
7 area, as determined by the Secretary;

8 (C) a State or local law enforcement or other government entity
9 with port, border, or agricultural responsibilities, as determined by
10 the Secretary;

11 (D) a tribal law enforcement or other authority; or

12 (E) another entity the Secretary determines is appropriate; and

13 (5) have undergone appropriate privacy and civil liberties training
14 that is developed, supported, or sponsored by the Privacy Officer and
15 the Officer for Civil Rights and Civil Liberties, in consultation with the
16 Privacy and Civil Liberties Oversight Board established under section
17 1061 of the National Security Intelligence Reform Act of 2004 (42
18 U.S.C. 2000ee).

19 (e) OPTIONAL PARTICIPATION.—A State, local, or tribal law enforcement
20 or other government entity shall not be required to participate in the Home-
21 land Security Information Sharing Fellows Program.

22 (d) PROCEDURES FOR NOMINATION AND SELECTION.—

23 (1) IN GENERAL.—The Under Secretary for Intelligence and Anal-
24 ysis shall establish procedures to provide for the nomination and selec-
25 tion of individuals to participate in the Homeland Security Information
26 Sharing Fellows Program.

27 (2) LIMITATIONS.—The Under Secretary for Intelligence and Anal-
28 ysis shall—

29 (A) select law enforcement officers and intelligence analysts rep-
30 resenting a broad cross-section of State, local, and tribal agencies;
31 and

32 (B) ensure that the number of Information Sharing Fellows se-
33 lected does not impede the activities of the Office of Intelligence
34 and Analysis.

35 § 10514. Rural Policing Institute

36 (a) DEFINITION OF RURAL.—In this section, the term “rural” means an
37 area—

38 (1) that is not located in a metropolitan statistical area, as defined
39 by the Office of Management and Budget; or

1 (2) that is located in a metropolitan statistical area and a county,
2 borough, parish, or area under the jurisdiction of an Indian tribe with
3 a population of not more than 50,000.

4 (b) IN GENERAL.—The Secretary shall establish a Rural Policing Insti-
5 tute, which shall be administered by the Federal Law Enforcement Training
6 Center, to target training to law enforcement agencies and other emergency
7 response providers located in rural areas. The Secretary, through the Rural
8 Policing Institute, shall—

9 (1) evaluate the needs of law enforcement agencies and other emer-
10 gency response providers in rural areas;

11 (2) develop expert training programs designed to address the needs
12 of law enforcement agencies and other emergency response providers in
13 rural areas as identified in the evaluation conducted under paragraph
14 (1), including training programs about intelligence-led policing and pro-
15 tections for privacy, civil rights, and civil liberties;

16 (3) provide the training programs developed under paragraph (2) to
17 law enforcement agencies and other emergency response providers in
18 rural areas; and

19 (4) conduct outreach efforts to ensure that local and tribal govern-
20 ments in rural areas are aware of the training programs developed
21 under paragraph (2) so they can avail themselves of the programs.

22 (c) CURRICULA.—The training at the Rural Policing Institute established
23 under subsection (b) shall—

24 (1) be configured in a manner so as not to duplicate or displace a
25 law enforcement or emergency response program of the Federal Law
26 Enforcement Training Center or a local or tribal government entity in
27 existence on August 3, 2007; and

28 (2) to the maximum extent practicable, be delivered in a cost-effec-
29 tive manner at facilities of the Department, on closed military installa-
30 tions with adequate training facilities, or at facilities operated by the
31 participants.

32 **§ 10515. Interagency Threat Assessment and Coordination**
33 **Group**

34 (a) IN GENERAL.—To improve the sharing of information within the
35 scope of the information sharing environment established under section
36 11908 of this title with State, local, tribal, and private-sector officials, the
37 Director of National Intelligence, through the program manager for the in-
38 formation sharing environment, in coordination with the Secretary, shall co-
39 ordinate and oversee the creation of an Interagency Threat Assessment and
40 Coordination Group (in this section referred to as “ITACG”).

41 (b) COMPOSITION OF ITACG.—The ITACG shall consist of—

1 (1) an ITACG Advisory Council to set policy and develop processes
2 for the integration, analysis, and dissemination of federally coordinated
3 information within the scope of the information sharing environment,
4 including homeland security information, terrorism information, and
5 weapons of mass destruction information; and

6 (2) an ITACG Detail comprised of State, local, and tribal homeland
7 security and law enforcement officers and intelligence analysts detailed
8 to work in the National Counterterrorism Center with Federal intel-
9 ligence analysts for the purpose of integrating, analyzing, and assisting
10 in the dissemination of federally coordinated information within the
11 scope of the information sharing environment, including homeland se-
12 curity information, terrorism information, and weapons of mass de-
13 struction information, through appropriate channels identified by the
14 ITACG Advisory Council.

15 (c) RESPONSIBILITIES OF SECRETARY.—The Secretary, or the Sec-
16 retary’s designee, in coordination with the Director of the National Counter-
17 terrorism Center and the ITACG Advisory Council, shall—

18 (1) create policies and standards for the creation of information
19 products derived from information within the scope of the information
20 sharing environment, including homeland security information, ter-
21 rorism information, and weapons of mass destruction information, that
22 are suitable for dissemination to State, local, and tribal governments
23 and the private sector;

24 (2) evaluate and develop processes for the timely dissemination of
25 federally coordinated information within the scope of the information
26 sharing environment, including homeland security information, ter-
27 rorism information, and weapons of mass destruction information, to
28 State, local, and tribal governments and the private sector;

29 (3) establish criteria and a methodology for indicating to State, local,
30 and tribal governments and the private sector the reliability of informa-
31 tion within the scope of the information sharing environment, including
32 homeland security information, terrorism information, and weapons of
33 mass destruction information, disseminated to them;

34 (4) educate the intelligence community about the requirements of
35 State, local, and tribal homeland security, law enforcement, and other
36 emergency response providers regarding information within the scope
37 of the information sharing environment, including homeland security
38 information, terrorism information, and weapons of mass destruction
39 information;

40 (5) establish and maintain the ITACG Detail, which shall assign an
41 appropriate number of State, local, and tribal homeland security and

1 law enforcement officers and intelligence analysts to work in the Na-
2 tional Counterterrorism Center who shall—

3 (A) educate and advise National Counterterrorism Center intel-
4 ligence analysts about the requirements of the State, local, and
5 tribal homeland security and law enforcement officers, and other
6 emergency response providers regarding information within the
7 scope of the information sharing environment, including homeland
8 security information, terrorism information, and weapons of mass
9 destruction information;

10 (B) assist National Counterterrorism Center intelligence ana-
11 lysts in integrating, analyzing, and otherwise preparing versions of
12 products derived from information within the scope of the informa-
13 tion sharing environment, including homeland security informa-
14 tion, terrorism information, and weapons of mass destruction in-
15 formation that are unclassified or classified at the lowest possible
16 level and suitable for dissemination to State, local, and tribal
17 homeland security and law enforcement agencies in order to help
18 deter and prevent terrorist attacks;

19 (C) implement, in coordination with National Counterterrorism
20 Center intelligence analysts, the policies, processes, procedures,
21 standards, and guidelines developed by the ITACG Advisory Coun-
22 cil;

23 (D) assist in the dissemination of products derived from infor-
24 mation within the scope of the information sharing environment,
25 including homeland security information, terrorism information,
26 and weapons of mass destruction information, to State, local, and
27 tribal jurisdictions only through appropriate channels identified by
28 the ITACG Advisory Council;

29 (E) make recommendations, as appropriate, to the Secretary or
30 the Secretary's designee, for the further dissemination of intel-
31 ligence products that could likely inform or improve the security
32 of a State, local, or tribal government (including a State, local, or
33 tribal law enforcement agency), or a private-sector entity; and

34 (F) report directly to the senior intelligence official from the
35 Department under paragraph (6);

36 (6) detail a senior intelligence official from the Department to the
37 National Counterterrorism Center, who shall—

38 (A) manage the day-to-day operations of the ITACG Detail;

39 (B) report directly to the Director of the National Counterter-
40 rorism Center or the Director's designee; and

1 (C) in coordination with the Director of the Federal Bureau of
2 Investigation, and subject to the approval of the Director of the
3 National Counterterrorism Center, select a deputy from the pool
4 of available detailees from the Federal Bureau of Investigation in
5 the National Counterterrorism Center;

6 (7) establish, in the ITACG Advisory Council, a mechanism to select
7 law enforcement officers and intelligence analysts for placement in the
8 National Counterterrorism Center consistent with paragraph (5), using
9 criteria developed by the ITACG Advisory Council that shall encourage
10 participation from a broadly representative group of State, local, and
11 tribal homeland security and law enforcement agencies; and

12 (8) compile an annual assessment of the ITACG Detail's perform-
13 ance, including summaries of customer feedback, in preparing, dissemi-
14 nating, and requesting the dissemination of intelligence products in-
15 tended for State, local and tribal government (including State, local,
16 and tribal law enforcement agencies), and private-sector entities.

17 (d) MEMBERSHIP.—The Secretary, or the Secretary's designee, shall
18 serve as the chair of the ITACG Advisory Council, which shall include—

19 (1) representatives of—

20 (A) the Department;

21 (B) the Federal Bureau of Investigation;

22 (C) the National Counterterrorism Center;

23 (D) the Department of Defense;

24 (E) the Department of Energy;

25 (F) the Department of State; and

26 (G) other Federal entities as appropriate;

27 (2) the program manager of the information sharing environment,
28 designated under section 11908(d) of this title, or the program man-
29 ager's designee; and

30 (3) executive level law enforcement and intelligence officials from
31 State, local, and tribal governments.

32 (e) CRITERIA.—The Secretary, in consultation with the Director of Na-
33 tional Intelligence, the Attorney General, and the program manager of the
34 information sharing environment established under section 11908 of this
35 title, shall—

36 (1) establish procedures for selecting members of the ITACG Advi-
37 sory Council and for the proper handling and safeguarding of products
38 derived from information within the scope of the information sharing
39 environment, including homeland security information, terrorism infor-
40 mation, and weapons of mass destruction information, by those mem-
41 bers; and

1 (2) ensure that at least 50 percent of the members of the ITACG
2 Advisory Council are from State, local, and tribal governments.

3 (f) OPERATIONS.—

4 (1) IN GENERAL.—The ITACG Advisory Council shall meet regu-
5 larly, but not less than quarterly, at the facilities of the National
6 Counterterrorism Center of the Office of the Director of National Intel-
7 ligence.

8 (2) MANAGEMENT.—Pursuant to section 119(f)(1)(E) of the Na-
9 tional Security Act of 1947 (50 U.S.C. 3056(f)(1)(E)), the Director of
10 the National Counterterrorism Center, acting through the senior intel-
11 ligence official from the Department of Homeland Security detailed
12 pursuant to subsection (c)(6), shall ensure that—

13 (A) the products derived from information within the scope of
14 the information sharing environment, including homeland security
15 information, terrorism information, and weapons of mass destruc-
16 tion information, prepared by the National Counterterrorism Cen-
17 ter and the ITACG Detail for distribution to State, local, and trib-
18 al homeland security and law enforcement agencies, reflect the re-
19 quirements of the agencies and are produced consistently with the
20 policies, processes, procedures, standards, and guidelines estab-
21 lished by the ITACG Advisory Council;

22 (B) in consultation with the ITACG Advisory Council and con-
23 sistent with sections 102A(f)(1)(B)(iii) and 119(f)(1)(E) of the
24 National Security Act of 1947 (50 U.S.C. 3024(f)(1)(B)(iii),
25 3056(f)(1)(E)), all products described in subparagraph (A) are
26 disseminated through existing channels of the Department and the
27 Department of Justice and other appropriate channels to State,
28 local, and tribal government officials and other entities;

29 (C) all detailees under subsection (c)(5) have appropriate access
30 to all relevant information within the scope of the information
31 sharing environment, including homeland security information, ter-
32 rorism information, and weapons of mass destruction information,
33 available at the National Counterterrorism Center in order to ac-
34 complish the objectives under subsection (c)(5);

35 (D) all detailees under subsection (c)(5) have the appropriate
36 security clearances and are trained in the procedures for handling,
37 processing, storing, and disseminating classified products derived
38 from information within the scope of the information sharing envi-
39 ronment, including homeland security information, terrorism infor-
40 mation, and weapons of mass destruction information; and

1 (E) all detailees under subsection (c)(5) complete appropriate
2 privacy and civil liberties training.

3 (g) INAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of title
4 5 shall not apply to the ITACG or any subsidiary groups of the ITACG.

5 **§ 10516. Classified Information Advisory Officer**

6 (a) DESIGNATION.—The Secretary shall identify and designate in the De-
7 partment a Classified Information Advisory Officer.

8 (b) RESPONSIBILITIES.—The responsibilities of the Classified Information
9 Advisory Officer are as follows:

10 (1) To develop and disseminate educational materials and to develop
11 and administer training programs to assist State, local, and tribal gov-
12 ernments (including State, local, and tribal law enforcement agencies),
13 and private-sector entities—

14 (A) in developing plans and policies to respond to requests re-
15 lated to classified information without communicating the informa-
16 tion to individuals who lack appropriate security clearances;

17 (B) regarding the appropriate procedures for challenging classi-
18 fication designations of information received by personnel of the
19 entities; and

20 (C) on the means by which the personnel may apply for security
21 clearances.

22 (2) To inform the Under Secretary for Intelligence and Analysis on
23 policies and procedures that could facilitate the sharing of classified in-
24 formation with the personnel, as appropriate.

25 **§ 10517. Annual report and briefing on intelligence activi-**
26 **ties of the Department**

27 (a) IN GENERAL.—For each fiscal year and along with the budget mate-
28 rials submitted in support of the budget of the Department pursuant to sec-
29 tion 1105(a) of title 31, the Under Secretary for Intelligence and Analysis
30 shall submit to the congressional intelligence committees a report for that
31 fiscal year on each intelligence activity of each intelligence component of the
32 Department, as designated by the Under Secretary, that includes the fol-
33 lowing:

34 (1) The amount of funding requested for each intelligence activity.

35 (2) The number of full-time employees funded to perform each intel-
36 ligence activity.

37 (3) The number of full-time contractor employees (or the equivalent
38 of full-time in the case of part-time contractor employees) funded to
39 perform, or in support of, each intelligence activity.

40 (4) A determination as to whether each intelligence activity is pre-
41 dominantly in support of national intelligence or departmental mission.

1 (5) The total number of analysts of the Intelligence Enterprise of the
2 Department who perform—

3 (A) strategic analysis; or

4 (B) operational analysis.

5 (b) BRIEFING ON DEPARTMENT INTELLIGENCE ACTIVITIES

6 (1) DEFINITIONS.—In this subsection:

7 (A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term
8 “appropriate congressional committees” means—

9 (i) the congressional intelligence committees;

10 (ii) the Committee on Homeland Security and Government
11 Affairs and the Committee on Appropriations of the Senate;
12 and

13 (iii) the Committee on Homeland Security and the Com-
14 mittee on Appropriations of the House of Representatives.

15 (B) COMPONENT OF THE DEPARTMENT.—The term “component
16 of the department” means the following components of the De-
17 partment:

18 (i) The Cybersecurity and Infrastructure Security Agency
19 Threat Management Division.

20 (ii) The Federal Emergency Management Agency Protec-
21 tion and National Preparedness Office of Counterterrorism
22 and Security Preparedness.

23 (iii) The Transportation Security Administration Office of
24 Intelligence and Analysis.

25 (iv) The United States Citizenship and Immigration Serv-
26 ices Fraud Detection and National Security Directorate,
27 Field Operations Directorate, and Collateral Duty Intelligence.

28 (v) The United States Customs and Border Protection Of-
29 fice of Intelligence.

30 (vi) The United States Immigration and Customs Enforce-
31 ment Homeland Security Investigations, Office of Intel-
32 ligence, and Special Agent in Charge Intelligence Program.

33 (C) INTELLIGENCE ACTIVITY.—The term “intelligence activity”
34 shall be interpreted consistent with how the term is used in section
35 502 of the National Security Act of 1947 (50 U.S.C. 3092).

36 (2) BRIEFING.—

37 (A) WHEN PROVIDED.—Not less frequently than once each year
38 thereafter, the Chief Intelligence Officer of the Department shall
39 provide the appropriate congressional committees a briefing on
40 new intelligence activities commenced by any component of the
41 Department and any that have been terminated.

- 1 (B) CONTENTS.—Each briefing shall include the following:
- 2 (i) A comprehensive description of all intelligence activities
- 3 conducted during the period by any component of the Depart-
- 4 ment that conducts intelligence activities.
- 5 (ii) With respect to each intelligence activity, a description
- 6 of the activity, including at a minimum—
- 7 (I) the nature of the activity;
- 8 (II) the component undertaking the activity;
- 9 (III) the legal authority for the activity; and
- 10 (IV) the source of funding for the activity.
- 11 (iii) A description and the quantity of any types of finished
- 12 intelligence products or intelligence information reports pro-
- 13 duced or contributed to by a component of the Department
- 14 that conducts intelligence activities during the period specified
- 15 in the briefing.
- 16 (iv) An identification of any external or internal guidelines,
- 17 policies, processes, practices, or programs governing the col-
- 18 lection, retention, analysis, or dissemination by the component
- 19 of information regarding United States citizens, lawful per-
- 20 manent residents of the United States, or individuals located
- 21 in the United States.
- 22 (C) FORM.—The briefing may be provided in classified form.

23 **§ 10518. Data framework**

- 24 (a) DEFINITIONS.—In this section:
- 25 (1) HOMELAND SECURITY INFORMATION.—The term “homeland se-
- 26 curity information” has the meaning given the term in section 11907
- 27 of this title.
- 28 (2) NATIONAL INTELLIGENCE.—The term “national intelligence” has
- 29 the meaning given the term in section 3 of the National Security Act
- 30 of 1947 (50 U.S.C. 3003).
- 31 (3) TERRORISM INFORMATION.—The term “terrorism information”
- 32 has the meaning given the term in section 11908 of this title.
- 33 (b) DEVELOPMENT.—
- 34 (1) IN GENERAL.—The Secretary shall develop a data framework to
- 35 integrate existing Department datasets and systems, as appropriate,
- 36 for access by authorized personnel in a manner consistent with relevant
- 37 legal authorities and privacy, civil rights, and civil liberties policies and
- 38 protections.
- 39 (2) REQUIREMENTS.—In developing the framework, the Secretary
- 40 shall ensure, in accordance with all applicable statutory and regulatory
- 41 requirements, that the following information is included:

1 (A) All information acquired, held, or obtained by an office or
2 component of the Department that falls within the scope of the
3 information sharing environment, including homeland security in-
4 formation, terrorism information, weapons of mass destruction in-
5 formation, and national intelligence.

6 (B) Information or intelligence relevant to priority mission
7 needs and capability requirements of the Homeland Security En-
8 terprise, as determined appropriate by the Secretary.

9 (e) ACCESS.—

10 (1) IN GENERAL.—The Secretary shall ensure that the data frame-
11 work required under this section is accessible to employees of the De-
12 partment who the Secretary determines—

13 (A) have an appropriate security clearance;

14 (B) are assigned to perform a function that requires access to
15 information in the framework; and

16 (C) are trained in applicable standards for safeguarding and
17 using the information.

18 (2) GUIDANCE.—The Secretary shall—

19 (A) issue guidance for Department employees authorized to ac-
20 cess and contribute to the data framework pursuant to paragraph
21 (1); and

22 (B) ensure that the guidance enforces a duty to share between
23 offices and components of the Department when accessing or con-
24 tributing to the framework for mission needs.

25 (3) EFFICIENCY.—The Secretary shall promulgate data standards
26 and instruct components of the Department to make available informa-
27 tion through the data framework required under this section in a ma-
28 chine-readable standard format, to the greatest extent practicable.

29 (d) EXCLUSION OF INFORMATION.—The Secretary may exclude informa-
30 tion from the data framework required under this section if the Secretary
31 determines inclusion of the information may—

32 (1) jeopardize the protection of sources, methods, or activities;

33 (2) compromise a criminal or national security investigation;

34 (3) be inconsistent with other Federal laws or regulations; or

35 (4) be duplicative or not serve an operational purpose if included in
36 the framework.

37 (e) SAFEGUARDS.—The Secretary shall incorporate into the data frame-
38 work required under this section systems capabilities for auditing and ensur-
39 ing the security of information included in the framework. The capabilities
40 shall include the following:

41 (1) Mechanisms for identifying insider threats.

1 (2) Mechanisms for identifying security risks.

2 (3) Safeguards for privacy, civil rights, and civil liberties.

3 (f) DEADLINE FOR IMPLEMENTATION.—Not later than 2 years after De-
4 cember 19, 2018, the Secretary shall ensure the data framework required
5 under this section has the ability to include appropriate information in exist-
6 ence in the Department to meet the critical mission operations of the De-
7 partment.

8 (g) NOTICE TO CONGRESS.—

9 (1) STATUS UPDATES.—The Secretary shall submit to the appro-
10 priate congressional committees regular updates on the status of the
11 data framework until the framework is fully operational.

12 (2) OPERATIONAL NOTIFICATION.—Not later than 60 days after the
13 date on which the data framework required under this section is fully
14 operational, the Secretary shall provide notice to the appropriate con-
15 gressional committees that the data framework is fully operational.

16 (3) VALUE ADDED.—The Secretary shall annually brief Congress on
17 component use of the data framework required under this section to
18 support operations that disrupt terrorist activities and incidents in the
19 homeland.

20 § 10519. Procedures for sharing information

21 The Secretary shall establish procedures on the use of information shared
22 under this chapter that—

23 (1) limit the re-dissemination of the information to ensure that it is
24 not used for an unauthorized purpose;

25 (2) ensure the security and confidentiality of the information;

26 (3) protect the constitutional and statutory rights of individuals who
27 are subjects of the information; and

28 (4) provide data integrity through the timely removal and destruc-
29 tion of obsolete or erroneous names and information.

30 § 10520. Privacy Officer

31 (a) APPOINTMENT AND RESPONSIBILITIES.—The Secretary shall appoint
32 a senior official in the Department, who shall report directly to the Sec-
33 retary, to assume primary responsibility for privacy policy, including—

34 (1) ensuring that the use of technologies sustain, and do not erode,
35 privacy protections relating to the use, collection, and disclosure of per-
36 sonal information;

37 (2) ensuring that personal information contained in Privacy Act sys-
38 tems of records is handled in full compliance with fair information
39 practices as set out in section 552a of title 5 (known as the Privacy
40 Act of 1974);

1 (3) evaluating legislative and regulatory proposals involving collec-
2 tion, use, and disclosure of personal information by the Federal Gov-
3 ernment;

4 (4) conducting a privacy impact assessment of proposed rules of the
5 Department on the privacy of personal information, including the type
6 of personal information collected and the number of people affected;

7 (5) coordinating with the Officer for Civil Rights and Civil Liberties
8 to ensure that—

9 (A) programs, policies, and procedures involving civil rights,
10 civil liberties, and privacy considerations are addressed in an inte-
11 grated and comprehensive manner; and

12 (B) Congress receives appropriate reports on the programs, poli-
13 cies, and procedures; and

14 (6) preparing a report to Congress on an annual basis on activities
15 of the Department that affect privacy, including complaints of privacy
16 violations, implementation of section 552a of title 5 (known as the Pri-
17 vacy Act of 1974), internal controls, and other matters.

18 (b) AUTHORITY TO INVESTIGATE.—

19 (1) IN GENERAL.—The senior official appointed under subsection (a)
20 may—

21 (A) have access to all records, reports, audits, reviews, docu-
22 ments, papers, recommendations, and other materials available to
23 the Department that relate to programs and operations with re-
24 spect to the responsibilities of the senior official under this section;

25 (B) make investigations and reports relating to the administra-
26 tion of the programs and operations of the Department that are,
27 in the senior official's judgment, necessary or desirable;

28 (C) subject to the approval of the Secretary, require by sub-
29 poena the production, by any person other than a Federal agency,
30 of all information, documents, reports, answers, records, accounts,
31 papers, and other data and documentary evidence necessary to the
32 performance of the responsibilities of the senior official under this
33 section; and

34 (D) administer to, or take from, a person an oath, affirmation,
35 or affidavit, whenever necessary to the performance of the respon-
36 sibilities of the senior official under this section.

37 (2) ENFORCEMENT OF SUBPOENAS.—A subpoena issued under para-
38 graph (1)(C) shall, in the case of contumacy or refusal to obey, be en-
39 forceable by order of an appropriate United States district court.

40 (3) EFFECT OF OATHS.—An oath, affirmation, or affidavit adminis-
41 tered or taken under paragraph (1)(D) by or before an employee of the

1 Privacy Office designated for that purpose by the senior official ap-
2 pointed under subsection (a) shall have the same force and effect as
3 if administered or taken by or before an officer having a seal of office.

4 (c) SUPERVISION AND COORDINATION.—

5 (1) IN GENERAL.—The senior official appointed under subsection (a)
6 shall—

7 (A) report to, and be under the general supervision of, the Sec-
8 retary; and

9 (B) coordinate activities with the Inspector General of the De-
10 partment in order to avoid duplication of effort.

11 (2) COORDINATION WITH INSPECTOR GENERAL.—

12 (A) IN GENERAL.—Except as provided in subparagraph (B), the
13 senior official appointed under subsection (a) may investigate a
14 matter relating to possible violations or abuse concerning the ad-
15 ministration of a program or operation of the Department relevant
16 to the purposes under this section.

17 (B) COORDINATION.—

18 (i) REFERRAL TO INSPECTOR GENERAL.—Before initiating
19 an investigation described under subparagraph (A), the senior
20 official shall refer the matter and all related complaints, alle-
21 gations, and information to the Inspector General of the De-
22 partment.

23 (ii) DETERMINATION.—Not later than 30 days after the re-
24 ceipt of a matter referred under clause (i), the Inspector Gen-
25 eral shall—

26 (I) make a determination regarding whether the In-
27 spector General intends to initiate an audit or investiga-
28 tion of the matter referred under clause (i); and

29 (II) notify the senior official of that determination.

30 (iii) NOTIFICATION THAT AUDIT NOT INITIATED.—If the
31 Inspector General notifies the senior official that the Inspec-
32 tor General intends to initiate an audit or investigation, but
33 does not initiate that audit or investigation within 90 days
34 after providing that notification, the Inspector General shall
35 further notify the senior official that an audit or investigation
36 was not initiated. The further notification under this clause
37 shall be made not later than 3 days after the end of that 90-
38 day period.

39 (iv) INVESTIGATION BY SENIOR OFFICIAL.—The senior offi-
40 cial may investigate a matter referred under clause (i) if—

1 (I) the Inspector General notifies the senior official
2 under clause (ii) that the Inspector General does not in-
3 tend to initiate an audit or investigation relating to that
4 matter; or

5 (II) the Inspector General provides a further notifica-
6 tion under clause (iii) relating to that matter.

7 (v) TRAINING.—An employee of the Office of Inspector
8 General who audits or investigates a matter referred under
9 clause (i) shall be required to receive adequate training on
10 privacy laws, rules, and regulations, to be provided by an en-
11 tity approved by the Inspector General in consultation with
12 the senior official appointed under subsection (a).

13 (d) NOTIFICATION TO CONGRESS ON REMOVAL.—If the Secretary re-
14 moves the senior official appointed under subsection (a) or transfers that
15 senior official to another position or location within the Department, the
16 Secretary shall—

17 (1) promptly submit a written notification of the removal or transfer
18 to both Houses of Congress; and

19 (2) include in the notification the reasons for the removal or trans-
20 fer.

21 (e) REPORTS BY SENIOR OFFICIAL TO CONGRESS.—The senior official
22 appointed under subsection (a) shall—

23 (1) submit reports directly to Congress regarding performance of the
24 responsibilities of the senior official under this section, without prior
25 comment or amendment by the Secretary, Deputy Secretary of Home-
26 land Security, or any other officer or employee of the Department or
27 the Office of Management and Budget; and

28 (2) inform the Committee on Homeland Security and Governmental
29 Affairs of the Senate and the Committee on Homeland Security of the
30 House of Representatives not later than—

31 (A) 30 days after the Secretary disapproves the senior official's
32 request for a subpoena under subsection (b)(1)(C) or the Sec-
33 retary substantively modifies the requested subpoena; or

34 (B) 45 days after the senior official's request for a subpoena
35 under subsection (b)(1)(C), if that subpoena has neither been ap-
36 proved nor disapproved by the Secretary.

37 **Chapter 107—Cybersecurity and** 38 **Infrastructure Security**

Subchapter I—General

Sec.

10701. Definitions.

10702. Responsibilities.

- 10703. Authority not affected.
- 10704. Enhancement of Federal and non-Federal cybersecurity.
- 10705. Recruitment and retention.
- 10706. National Cybersecurity and Communications Integration Center.
- 10707. Plans.
- 10708. Strategy.
- 10709. NET Guard.
- 10710. Clearances.
- 10711. Federal intrusion detection and prevention system.
- 10712. National asset database.
- 10713. Prohibition on new regulatory authority.

Subchapter II—Critical Infrastructure Information

- 10731. Definitions.
- 10732. Designation of critical infrastructure protection program.
- 10733. Protection of voluntarily shared critical infrastructure information.
- 10734. No private right of action.

Subchapter III—Cyber Response and Recovery

- 10741. Definitions
- 10742. Declaration.
- 10743. Cyber Response and Recovery Fund.
- 10744. Notification and reporting.
- 10745. Rule of construction.
- 10746. Authorization of appropriations.
- 10747. Sunset.

Subchapter IV—Cyber Incident Reporting

- 10761. Definitions.
- 10762. Cyber incident review.
- 10763. Required reporting of certain cyber incidents.
- 10764. Voluntary reporting of other cyber incidents.
- 10765. Noncompliance with required reporting.
- 10766. Disclosure, retention, and use.
- 10767. Cyber Incident Reporting Council.
- 10768. Federal sharing of incident reports.

Subchapter V—Cybersecurity Information Sharing

- 10781. Definitions
- 10782. Procedures for sharing information by Federal Government.
- 10783. Authorization for preventing, detecting, analyzing, and mitigating cybersecurity threats.
- 10784. Sharing of cyber threat indicators and defensive measures with Federal Government.
- 10785. Protection from liability.
- 10786. Oversight of Government activities.
- 10787. Report on cybersecurity threats.
- 10788. Exception to limitation on authority of Secretary of Defense to disseminate information.
- 10789. Construction and preemption.
- 10790. Effective period.

Subchapter VI—Cybersecurity Enhancement**Part A—Federal Cybersecurity Enhancement**

- 10801. Definitions.
- 10802. Advanced internal defenses.
- 10803. Federal cybersecurity requirements.
- 10804. Assessment; reports.
- 10805. Report of security vulnerabilities on appropriate information systems.
- 10806. Bug bounty pilot program.
- 10807. Pilot program on public-private partnerships with internet ecosystem companies to detect and disrupt adversary cyber operations.
- 10808. CyberSentry program.
- 10809. Inventory of cryptographic systems; migration to post-quantum cryptography.
- 10810. Competition relating to cybersecurity vulnerabilities.
- 10811. Ransomware threat mitigation activities.
- 10812. National cybersecurity preparedness consortium.

Part B—Other Areas

- 10821. Enhancement of emergency services.
- 10822. Improving cybersecurity in the health care industry.
- 10823. K–12 education cybersecurity initiative.

10824. Federal Clearinghouse on School Safety Evidence-Based Practices.
 10825. Report and briefing on school and daycare protection.

Subchapter VII—Secure Handling of Ammonium Nitrate

10841. Definitions.
 10842. Regulation of the sale and transfer of ammonium nitrate.
 10843. Inspection and auditing of records.
 10844. Administrative provisions.
 10845. Theft reporting requirement.
 10846. Prohibitions and penalty.
 10847. Protection from civil liability.
 10848. Preemption of other laws.

Subchapter VIII—Chemical Facilities

10861. Definitions.
 10862. Chemical Facility Anti-Terrorism Standards Program.
 10863. Protection and sharing of information.
 10864. Civil enforcement.
 10865. Whistleblower protections.
 10866. Relationship to other laws.
 10867. CFATS regulations.
 10868. Small covered chemical facilities.
 10869. Outreach to chemical facilities of interest.
 10870. Termination.

Subchapter IX—Miscellaneous

10881. Duties and authorities relating to .gov internet domain.
 10882. Intelligence and cybersecurity diversity fellowship program.
 10883. Cybersecurity State Coordinator.
 10884. Sector Risk Management Agencies.
 10885. National Cyber Director.
 10886. Apprehension and prosecution of international cyber criminals.
 10887. President’s Cup Cybersecurity Competition.
 10888. Incentive pay for positions requiring significant cyber skills.

Subchapter I—General

§ 10701. Definitions

In this subchapter, subchapters II and III, and sections 10761 through 10767 of this title:

(1) AGENCY.—The term “Agency” means the Cybersecurity and Infrastructure Security Agency.

(2) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term “appropriate congressional committee” means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives.

(3) CLOUD SERVICE PROVIDER.—The term “cloud service provider” means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating to that publication.

(4) CRITICAL INFRASTRUCTURE INFORMATION.—The term “critical infrastructure information” means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including—

1 (A) actual, potential, or threatened interference with, attack on,
2 compromise of, or incapacitation of critical infrastructure or pro-
3 tected systems by either physical or computer-based attack or
4 other similar conduct (including the misuse of or unauthorized ac-
5 cess to all types of communications and data transmission sys-
6 tems) that violates Federal, State, or local law, harms interstate
7 commerce of the United States, or threatens public health or safe-
8 ty;

9 (B) the ability of critical infrastructure or a protected system
10 to resist interference, compromise, or incapacitation, including any
11 planned or past assessment, projection, or estimate of the vulner-
12 ability of critical infrastructure or a protected system, including
13 security testing, risk evaluation, risk management planning, or
14 risk audit; and

15 (C) a planned or past operational problem or solution regarding
16 critical infrastructure or a protected system, including repair, re-
17 covery, reconstruction, insurance, or continuity, to the extent it is
18 related to interference, compromise, or incapacitation.

19 (5) CYBER THREAT INDICATOR.—The term “cyber threat indicator”
20 means information that is necessary to describe or identify—

21 (A) malicious reconnaissance, including anomalous patterns of
22 communication that appear to be transmitted for the purpose of
23 gathering technical information relating to a cybersecurity threat
24 or security vulnerability;

25 (B) a method of defeating a security control or exploitation of
26 a security vulnerability;

27 (C) a security vulnerability, including anomalous activity that
28 appears to indicate the existence of a security vulnerability;

29 (D) a method of causing a user with legitimate access to an in-
30 formation system or information that is stored on, processed by,
31 or transiting an information system to unwittingly enable the de-
32 feat of a security control or exploitation of a security vulnerability;

33 (E) malicious cyber command and control;

34 (F) the actual or potential harm caused by an incident, includ-
35 ing a description of the information exfiltrated as a result of a
36 particular cybersecurity threat;

37 (G) any other attribute of a cybersecurity threat, if disclosure
38 of the attribute is not otherwise prohibited by law; or

39 (H) any combination of subparagraphs (A) through (G).

40 (6) CYBERSECURITY PURPOSE.—The term “cybersecurity purpose”
41 means the purpose of protecting an information system or information

1 that is stored on, processed by, or transiting an information system
2 from a cybersecurity threat or security vulnerability.

3 (7) CYBERSECURITY RISK.—The term “cybersecurity risk”—

4 (A) means threats to and vulnerabilities of information or infor-
5 mation systems and any related consequences caused by or result-
6 ing from unauthorized access, use, disclosure, degradation, disrup-
7 tion, modification, or destruction of the information or information
8 systems, including related consequences caused by an act of ter-
9 rorism; and

10 (B) does not include an action that solely involves a violation
11 of a consumer term of service or a consumer licensing agreement.

12 (8) CYBERSECURITY THREAT.—

13 (A) IN GENERAL.—Except as provided in subparagraph (B), the
14 term “cybersecurity threat” means an action, not protected by the
15 1st amendment of the Constitution, on or through an information
16 system that may result in an unauthorized effort to adversely im-
17 pact the security, availability, confidentiality, or integrity of an in-
18 formation system or information that is stored on, processed in,
19 or transiting an information system.

20 (B) EXCLUSION.—The term “cybersecurity threat” does not in-
21 clude any action that solely involves a violation of a consumer
22 term of service or a consumer licensing agreement.

23 (9) DEFENSIVE MEASURE.—

24 (A) IN GENERAL.—Except as provided in subparagraph (B), the
25 term “defensive measure” means an action, device, procedure, sig-
26 nature, technique, or other measure applied to an information sys-
27 tem or information that is stored on, processed by, or transiting
28 an information system that detects, prevents, or mitigates a known
29 or suspected cybersecurity threat or security vulnerability.

30 (B) EXCLUSION.—The term “defensive measure” does not in-
31 clude a measure that destroys, renders unusable, provides unau-
32 thorized access to, or substantially harms an information system
33 or information stored on, processed by, or transiting the informa-
34 tion system not owned by—

35 (i) the private entity (as defined in section 1501 of this
36 title) operating the measure; or

37 (ii) another entity or Federal entity that may provide con-
38 sent and has provided consent to that private entity for oper-
39 ation of the measure.

40 (10) DIRECTOR.—The term “Director” means the Director of the
41 Cybersecurity and Infrastructure Security Agency.

1 (11) HOMELAND SECURITY ENTERPRISE.—In this section, the term
2 “Homeland Security Enterprise” means relevant governmental and
3 nongovernmental entities involved in homeland security, including Fed-
4 eral, State, local, and Tribal government officials, private-sector rep-
5 resentatives, academics, and other policy experts.

6 (12) INCIDENT.—The term “incident” means an occurrence that ac-
7 tually or imminently jeopardizes, without lawful authority —

8 (A) the integrity, confidentiality, or availability of information
9 on an information system; or

10 (B) an information system.

11 (13) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The
12 term “Information Sharing and Analysis Organization” means a formal
13 or informal entity or collaboration created or employed by public- or
14 private-sector organizations, for purposes of—

15 (A) gathering and analyzing critical infrastructure information,
16 including information relating to cybersecurity risks and incidents,
17 to better understand security problems and interdependencies re-
18 lating to critical infrastructure, including cybersecurity risks and
19 incidents, and protected systems, so as to ensure the availability,
20 integrity, and reliability of the infrastructure and systems;

21 (B) communicating or disclosing critical infrastructure informa-
22 tion, including cybersecurity risks and incidents, to help prevent,
23 detect, mitigate, or recover from the effects of an interference,
24 compromise, or incapacitation problem relating to critical infra-
25 structure, including cybersecurity risks and incidents, or protected
26 systems; and

27 (C) voluntarily disseminating critical infrastructure information,
28 including cybersecurity risks and incidents, to its members, the
29 Federal Government, State and local governments, or other enti-
30 ties that may be of assistance in carrying out the purposes speci-
31 fied in subparagraphs (A) and (B).

32 (14) INFORMATION SYSTEM.—The term “information system”—

33 (A) has the meaning given the term in section 3502 of title 44;
34 and

35 (B) includes industrial control systems such as supervisory con-
36 trol and data acquisition systems, distributed control systems, and
37 programmable logic controllers.

38 (15) INTELLIGENCE COMMUNITY.—The term “intelligence commu-
39 nity” has the meaning given that term in section 3 of the National Se-
40 curity Act of 1947 (50 U.S.C. 3003).

1 (16) MALICIOUS CYBER COMMAND AND CONTROL.—The term “malicious
2 cious cyber command and control” means a method for unauthorized
3 remote identification of, access to, or use of, an information system or
4 information that is stored on, processed by, or transiting an informa-
5 tion system.

6 (17) MALICIOUS RECONNAISSANCE.—The term “malicious reconnais-
7 sance” means a method for actively probing or passively monitoring an
8 information system for the purpose of discerning security vulnerabilities
9 of the information system, if the method is associated with a known
10 or suspected cybersecurity threat.

11 (18) MANAGED SERVICE PROVIDER.—The term “managed service
12 provider” means an entity that delivers services, such as network, ap-
13 plication, infrastructure, or security services, via ongoing and regular
14 support and active administration on the premises of a customer, in the
15 data center of the entity (such as hosting), or in a third party data
16 center.

17 (19) MONITOR.—The term “monitor” means to acquire, identify, or
18 scan, or to possess, information that is stored on, processed by, or
19 transiting an information system.

20 (20) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The
21 term “national cybersecurity asset response activities” means—

22 (A) furnishing cybersecurity technical assistance to entities af-
23 fected by cybersecurity risks to protect assets, mitigate
24 vulnerabilities, and reduce impacts of cyber incidents;

25 (B) identifying other entities that may be at risk of an incident
26 and assessing risk to the same or similar vulnerabilities referred
27 to in subparagraph (A);

28 (C) assessing potential cybersecurity risks to a sector or region,
29 including potential cascading effects, and developing courses of ac-
30 tion to mitigate the risks;

31 (D) facilitating information sharing and operational coordina-
32 tion with threat response; and

33 (E) providing guidance on how best to utilize Federal resources
34 and capabilities in a timely, effective manner to speed recovery
35 from cybersecurity risks.

36 (21) NATIONAL SECURITY SYSTEM.—The term “national security
37 system” had the meaning given the term in section 11103 of title 40.

38 (22) RANSOMWARE ATTACK.—The term “ransomware attack”—

39 (A) means an incident that includes the use or threat of use of
40 unauthorized or malicious code on an information system, or the
41 use or threat of use of another digital mechanism such as a denial

1 of service attack, to interrupt or disrupt the operations of an in-
2 formation system or compromise the confidentiality, availability, or
3 integrity of electronic data stored on, processed by, or transiting
4 an information system to extort a demand for a ransom payment;
5 and

6 (B) does not include an event in which the demand for payment
7 is—

8 (i) not genuine; or

9 (ii) made in good faith by an entity in response to a spe-
10 cific request by the owner or operator of the information sys-
11 tem.

12 (23) SECTOR RISK MANAGEMENT AGENCY.—The term “Sector Risk
13 Management Agency” means a Federal department or agency, des-
14 ignated by law or Presidential directive, with responsibility for pro-
15 viding institutional knowledge and specialized expertise of a sector, as
16 well as leading, facilitating, or supporting programs and associated ac-
17 tivities of its designated critical infrastructure sector in the all-hazards
18 environment in coordination with the Department.

19 (24) SECURITY CONTROL.—The term “security control” means the
20 management, operational, and technical controls used to protect
21 against an unauthorized effort to adversely affect the confidentiality,
22 integrity, and availability of an information system or its information.

23 (25) SECURITY VULNERABILITY.—The term “security vulnerability”
24 means any attribute of hardware, software, process, or procedure that
25 could enable or facilitate the defeat of a security control.

26 (26) SHARING.—The term “sharing” means providing, receiving, and
27 disseminating.

28 (27) SLTT ENTITY.—The term “SLTT entity” means a domestic
29 government entity that is a State government, local government, Tribal
30 government, territorial government, or any subdivision of any of those
31 governments.

32 (28) SUPPLY CHAIN COMPROMISE.—The term “supply chain com-
33 promise” means an incident in the supply chain of an information sys-
34 tem that an adversary can leverage or does leverage to compromise the
35 confidentiality, integrity, or availability of the information system or
36 the information the system processes, stores, or transmits and can
37 occur at any point during the life cycle.

38 § 10702. Responsibilities

39 (a) DIRECTOR.—

40 (1) IN GENERAL.—The Director shall—

1 (A) lead cybersecurity and critical infrastructure security pro-
2 grams, operations, and associated policy for the Agency, including
3 national cybersecurity asset response activities;

4 (B) coordinate with Federal entities, including Sector Risk
5 Management Agencies, and non-Federal entities, including inter-
6 national entities, to carry out the cybersecurity and critical infra-
7 structure activities of the Agency, as appropriate;

8 (C) carry out the responsibilities of the Secretary to secure Fed-
9 eral information and information systems consistent with law, in-
10 cluding subchapter II of chapter 35 of title 44 and subchapter IV
11 of this chapter, including by carrying out a periodic strategic as-
12 sessment of the related programs and activities of the Agency to
13 ensure the programs and activities contemplate the innovation of
14 information systems and changes in cybersecurity risks and cyber-
15 security threats;

16 (D) coordinate a national effort to secure and protect against
17 critical infrastructure risks, consistent with subsection (b)(1)(E);

18 (E) on request, provide analyses, expertise, and other technical
19 assistance to critical infrastructure owners and operators and,
20 where appropriate, provide those analyses, expertise, and other
21 technical assistance in coordination with Sector Risk Management
22 Agencies and other Federal departments and agencies;

23 (F) develop and utilize mechanisms for active and frequent col-
24 laboration between the Agency and Sector Risk Management
25 Agencies to ensure appropriate coordination, situational aware-
26 ness, and communications with Sector Risk Management Agencies;

27 (G) maintain and utilize mechanisms for the regular and ongo-
28 ing consultation and collaboration among the divisions of the
29 Agency to further operational coordination, integrated situational
30 awareness, and improved integration across the Agency in accord-
31 ance with this title;

32 (H) develop, coordinate, and implement—

33 (i) comprehensive strategic plans for the activities of the
34 Agency; and

35 (ii) risk assessments by and for the Agency;

36 (I) carry out emergency communications responsibilities, in ac-
37 cordance with chapter 123 of this title;

38 (J) carry out cybersecurity, infrastructure security, and emer-
39 gency communications stakeholder outreach and engagement and
40 coordinate that outreach and engagement with critical infrastruc-
41 ture Sector Risk Management Agencies, as appropriate;

1 (K) provide education, training, and capacity development to
2 Federal and non-Federal entities to enhance the security and resil-
3 iency of domestic and global cybersecurity and infrastructure secu-
4 rity;

5 (L) appoint a Cybersecurity State Coordinator in each State, as
6 described in section 10883 of this title;

7 (M) carry out the duties and authorities relating to the .gov
8 internet domain, as described in section 10881 of this title; and

9 (N) carry out other duties and powers prescribed by law or dele-
10 gated by the Secretary.

11 (2) CENTRAL LOCATIONS AND CO-LOCATION.—

12 (A) CENTRAL LOCATIONS.—To the maximum extent practicable,
13 the Director shall examine the establishment of central locations
14 in geographical regions with a significant Agency presence.

15 (B) CO-LOCATION.—When establishing the central locations de-
16 scribed in subparagraph (A), the Director shall coordinate with
17 component heads and the Under Secretary for Management to co-
18 locate or partner on new real property leases, renew occupancy
19 agreements for existing leases, or agree to extend or newly occupy
20 Federal space or new construction.

21 (b) SECRETARY.—

22 (1) IN GENERAL.—The responsibilities of the Secretary relating to
23 cybersecurity and infrastructure security shall include the following:

24 (A) Accessing, receiving, and analyzing law enforcement infor-
25 mation, intelligence information, and other information from Fed-
26 eral Government agencies, State, local, tribal, and territorial gov-
27 ernment agencies, including law enforcement agencies, and pri-
28 vate-sector entities, and integrating that information, in support of
29 the mission responsibilities of the Department, to—

30 (i) identify and assess the nature and scope of terrorist
31 threats to the homeland;

32 (ii) detect and identify threats of terrorism against the
33 United States; and

34 (iii) understand those threats in light of actual and poten-
35 tial vulnerabilities of the homeland.

36 (B) Carrying out comprehensive assessments of the
37 vulnerabilities of the key resources and critical infrastructure of
38 the United States, including the performance of risk assessments
39 to determine the risks posed by particular types of terrorist at-
40 tacks in the United States, including an assessment of the prob-
41 ability of success of those attacks and the feasibility and potential

1 efficacy of various countermeasures to those attacks. At the discre-
2 tion of the Secretary, the assessments may be carried out in co-
3 ordination with Sector Risk Management Agencies.

4 (C) Integrating relevant information, analysis, and vulnerability
5 assessments, regardless of whether the information, analysis, or
6 assessments are provided or produced by the Department, in order
7 to make recommendations, including prioritization, for protective
8 and support measures by the Department, other Federal Govern-
9 ment agencies, State, local, tribal, and territorial government
10 agencies and authorities, the private sector, and other entities re-
11 garding terrorist and other threats to homeland security.

12 (D) Ensuring, pursuant to section 10502 of this title, the timely
13 and efficient access by the Department to all information nec-
14 essary to discharge the responsibilities under this chapter, includ-
15 ing obtaining that information from other Federal Government
16 agencies.

17 (E) Developing, in coordination with the Sector Risk Manage-
18 ment Agencies with available expertise, a comprehensive national
19 plan for securing the key resources and critical infrastructure of
20 the United States, including power production, generation, and
21 distribution systems, information technology and telecommuni-
22 cations systems (including satellites), electronic financial and prop-
23 erty record storage and transmission systems, emergency commu-
24 nications systems, and the physical and technological assets that
25 support such systems.

26 (F) Recommending measures necessary to protect the key re-
27 sources and critical infrastructure of the United States in coordi-
28 nation with other Federal Government agencies, including Sector
29 Risk Management Agencies, and in cooperation with State, local,
30 tribal, and territorial government agencies and authorities, the pri-
31 vate sector, and other entities.

32 (G) Reviewing, analyzing, and making recommendations for im-
33 provements to the policies and procedures governing the sharing
34 of information relating to homeland security in the Federal Gov-
35 ernment and between Federal Government agencies and State,
36 local, tribal, and territorial government agencies and authorities.

37 (H) Disseminating, as appropriate, information analyzed by the
38 Department in the Department to other Federal Government
39 agencies with responsibilities relating to homeland security, and to
40 State, local, tribal, and territorial government agencies and pri-
41 vate-sector entities with those responsibilities, to assist in the de-

1 terrence, prevention, or preemption of, or response to, terrorist at-
2 tacks against the United States.

3 (I) Consulting with State, local, tribal, and territorial govern-
4 ment agencies and private-sector entities to ensure appropriate ex-
5 changes of information, including law enforcement-related infor-
6 mation, relating to threats of terrorism against the United States.

7 (J) Ensuring that material received pursuant to this subtitle
8 (except subchapters III through V of this chapter) is protected
9 from unauthorized disclosure and handled and used only for the
10 performance of official duties.

11 (K) Requesting additional information from other Federal Gov-
12 ernment agencies, State, local, tribal, and territorial government
13 agencies, and the private sector relating to threats of terrorism in
14 the United States, or relating to other areas of responsibility as-
15 signed by the Secretary, including the entry into cooperative
16 agreements through the Secretary to obtain the information.

17 (L) Establishing and utilizing, in conjunction with the Chief In-
18 formation Officer of the Department, a secure communications
19 and information technology infrastructure, including data-mining
20 and other advanced analytical tools, to access, receive, and analyze
21 data and information in furtherance of the responsibilities under
22 this section, and to disseminate information acquired and analyzed
23 by the Department, as appropriate.

24 (M) Coordinating training and other support to the elements
25 and personnel of the Department, other Federal Government agen-
26 cies, and State, local, tribal, and territorial government agencies
27 that provide information to the Department, or are consumers of
28 information provided by the Department, to facilitate the identi-
29 fication and sharing of information revealed in their ordinary du-
30 ties and the optimal utilization of information received from the
31 Department.

32 (N) Coordinating with Federal, State, local, tribal, and terri-
33 torial law enforcement agencies, and the private sector, as appro-
34 priate.

35 (O) Exercising the authorities and oversight of the functions,
36 personnel, assets, and liabilities of those components transferred
37 to the Department pursuant to section 10501(e) of this title.

38 (P) Carrying out the functions of the National Cybersecurity
39 and Communications Integration Center under section 10706 of
40 this title.

1 (Q) Carrying out the requirements of the Chemical Facility
2 Anti-Terrorism Standards Program established under subchapter
3 VII of this chapter and the secure handling of ammonium nitrate
4 program established under subchapter VI of this chapter, or any
5 successor programs.

6 (R) Encouraging and building cybersecurity awareness and com-
7 petency across the United States and developing, attracting, and
8 retaining the cybersecurity workforce necessary for the cybersecu-
9 rity related missions of the Department, including by—

10 (i) overseeing elementary and secondary cybersecurity edu-
11 cation and awareness related programs at the Agency;

12 (ii) leading efforts to develop, attract, and retain the cyber-
13 security workforce necessary for the cybersecurity related
14 missions of the Department;

15 (iii) encouraging and building cybersecurity awareness and
16 competency across the United States; and

17 (iv) carrying out cybersecurity related workforce develop-
18 ment activities, including through—

19 (I) increasing the pipeline of future cybersecurity pro-
20 fessionals through programs focused on elementary and
21 secondary education, postsecondary education, and work-
22 force development; and

23 (II) building awareness of and competency in cyberse-
24 curity across the civilian Federal Government workforce.

25 (2) REALLOCATION.—The Secretary may reallocate within the Agen-
26 cy the functions specified in subsections (d) and (e), consistent with the
27 responsibilities provided in paragraph (1), on certifying to and briefing
28 the appropriate congressional committees, and making known to the
29 public, at least 60 days prior to the reallocation, that the reallocation
30 is necessary for carrying out the activities of the Agency.

31 (3) STAFF.—

32 (A) IN GENERAL.—The Secretary shall provide the Agency with
33 a staff of analysts having appropriate expertise and experience to
34 assist the Agency in discharging the responsibilities of the Agency
35 under this section.

36 (B) PRIVATE-SECTOR ANALYSTS.—Analysts under this sub-
37 section may include analysts from the private sector.

38 (C) SECURITY CLEARANCES.—Analysts under this subsection
39 shall possess security clearances appropriate for their work under
40 this section.

41 (4) DETAIL OF PERSONNEL.—

1 (A) IN GENERAL.—To assist the Agency in discharging the re-
2 sponsibilities of the Agency under this section, personnel of the
3 Federal agencies described in subparagraph (B) may be detailed
4 to the Agency for the performance of analytic functions and re-
5 lated duties.

6 (B) AGENCIES.—The Federal agencies referred to in subpara-
7 graph (A) are—

- 8 (i) the Department of State;
- 9 (ii) the Central Intelligence Agency;
- 10 (iii) the Federal Bureau of Investigation;
- 11 (iv) the National Security Agency;
- 12 (v) the National Geospatial-Intelligence Agency;
- 13 (vi) the Defense Intelligence Agency;
- 14 (vii) Sector Risk Managment Agencies; and
- 15 (viii) any other agency of the Federal Government the
16 President considers appropriate.

17 (C) INTERAGENCY AGREEMENTS.—The Secretary and the head
18 of a Federal agency described in subparagraph (B) may enter into
19 agreements for the purpose of detailing personnel under this para-
20 graph.

21 (D) REIMBURSABLE OR NON-REIMBURSABLE BASIS.—The detail
22 of personnel under this paragraph may be on a reimbursable or
23 non-reimbursable basis.

24 (e) PRIVACY OFFICER.—The responsibilities of the Privacy Officer of the
25 Agency include—

26 (1) ensuring that the use of technologies by the Agency sustain, and
27 do not erode, privacy protections relating to the use, collection, and dis-
28 closure of personal information;

29 (2) ensuring that personal information contained in systems of
30 records of the Agency is handled in full compliance as specified in sec-
31 tion 552 of title 5;

32 (3) evaluating legislation and regulatory proposals involving collec-
33 tion, use, and disclosure of personal information by the Agency; and

34 (4) conducting a privacy impact assessment of proposed rules of the
35 Agency on the privacy of personal information, including the type of
36 personal information collected and the number of people affected.

37 (d) EXECUTIVE ASSISTANT DIRECTOR FOR CYBERSECURITY.—The Exec-
38 utive Assistant Director for Cybersecurity shall—

39 (1) direct the cybersecurity efforts of the Agency;

40 (2) carry out activities, at the direction of the Director, relating to
41 the security of Federal information and Federal information systems

1 consistent with law, including subchapter II of chapter 35 of title 44
2 and subchapter IV of this chapter;

3 (3) fully participate in the mechanisms required under subsection
4 (a)(1)(G); and

5 (4) carry out such other duties and powers as prescribed by the Di-
6 rector.

7 (e) EXECUTIVE ASSISTANT DIRECTOR FOR INFRASTRUCTURE SEC-
8 RITY.—The Executive Assistant Director for Infrastructure Security shall—

9 (1) direct the critical infrastructure security efforts of the Agency;

10 (2) carry out, at the direction of the Director, subchapters V and
11 VI of this chapter;

12 (3) fully participate in the mechanisms required under subsection
13 (a)(1)(G); and

14 (4) carry out such other duties and powers as prescribed by the Di-
15 rector.

16 **§ 10703. Authority not affected**

17 Nothing in this chapter may be construed as affecting in any manner the
18 authority, existing on November 15, 2018, of another component of the De-
19 partment or another Federal department or agency, including the authority
20 provided to the Sector Risk Management Agency specified in section
21 61003(c) of division F of the Fixing America’s Surface Transportation Act
22 (Public Law 114–94, 129 Stat. 1778).

23 **§ 10704. Enhancement of Federal and non-Federal cyberse-** 24 **curity**

25 In carrying out the responsibilities under section 10702 of this title, the
26 Director shall—

27 (1) as appropriate, provide to State and local government entities,
28 and on request to private entities that own or operate critical informa-
29 tion systems—

30 (A) analysis and warnings related to threats to, and
31 vulnerabilities of, critical information systems; and

32 (B) crisis management support in response to threats to, or at-
33 tacks on, critical information systems;

34 (2) as appropriate, provide technical assistance, on request, to the
35 private sector and other government entities, with respect to emergency
36 recovery plans to respond to major failures of critical information sys-
37 tems; and

38 (3) fulfill the responsibilities of the Secretary to protect Federal in-
39 formation systems under subchapter II of chapter 35 of title 44.

40 **§ 10705. Recruitment and retention**

41 (a) DEFINITIONS.—In this section:

1 (1) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appro-
2 priate committees of Congress” means the Committee on Homeland Se-
3 curity and Governmental Affairs and the Committee on Appropriations
4 of the Senate and the Committee on Homeland Security and the Com-
5 mittee on Appropriations of the House of Representatives.

6 (2) COLLECTIVE BARGAINING AGREEMENT.—The term “collective
7 bargaining agreement” has the same meaning given that term in sec-
8 tion 7103(a)(8) of title 5.

9 (3) EXCEPTED SERVICE.—The term “excepted service” has the same
10 meaning given that term in section 2103 of title 5.

11 (4) PREFERENCE ELIGIBLE.—The term “preference eligible” has the
12 same meaning given that term in section 2108 of title 5.

13 (5) QUALIFIED POSITION.—The term “qualified position” means a
14 position, designated by the Secretary for the purpose of this section,
15 in which the incumbent performs, manages, or supervises functions
16 that execute the responsibilities of the Department relating to cyberse-
17 curity.

18 (6) SENIOR EXECUTIVE SERVICE.—The term “Senior Executive
19 Service” has the same meaning given that term in section 2101a of
20 title 5.

21 (b) GENERAL AUTHORITY OF SECRETARY.—

22 (1) ESTABLISH POSITIONS, APPOINT PERSONNEL, AND FIX RATES OF
23 PAY.—

24 (A) IN GENERAL.—The Secretary may—

25 (i) establish, as positions in the excepted service, such
26 qualified positions in the Department as the Secretary deter-
27 mines necessary to carry out the responsibilities of the De-
28 partment relating to cybersecurity, including positions for-
29 merly identified as—

30 (I) senior level positions designated under section
31 5376 of title 5; and

32 (II) positions in the Senior Executive Service;

33 (ii) appoint an individual to a qualified position (after tak-
34 ing into consideration the availability of preference eligibles
35 for appointment to the position); and

36 (iii) subject to the requirements of paragraphs (2) and (3),
37 fix the compensation of an individual for service in a qualified
38 position.

39 (B) CONSTRUCTION WITH OTHER LAWS.—The authority of the
40 Secretary under this subsection applies without regard to any

1 other law relating to the appointment, number, classification, or
2 compensation of employees.

3 (2) BASIC PAY.—

4 (A) AUTHORITY TO FIX RATES OF BASIC PAY.—In accordance
5 with this section, the Secretary shall fix the rates of basic pay for
6 any qualified position established under paragraph (1) in relation
7 to the rates of pay provided for employees in comparable positions
8 in the Department of Defense and subject to the same limitations
9 on maximum rates of pay established for those employees by law
10 or regulation.

11 (B) PREVAILING RATE SYSTEMS.—The Secretary may, con-
12 sistent with section 5341 of title 5, adopt such provisions of that
13 title as provide for prevailing rate systems of basic pay and may
14 apply those provisions to qualified positions for employees in or
15 under which the Department may employ individuals described by
16 section 5342(a)(2)(A) of title 5.

17 (3) ADDITIONAL COMPENSATION, INCENTIVES, AND ALLOWANCES.—

18 (A) ADDITIONAL COMPENSATION BASED ON TITLE 5 AUTHOR-
19 IZATION.—The Secretary may provide employees in qualified posi-
20 tions compensation (in addition to basic pay), including benefits,
21 incentives, and allowances, consistent with, and not in excess of
22 the level authorized for, comparable positions authorized by title
23 5.

24 (B) ALLOWANCES IN NONFOREIGN AREAS.—An employee in a
25 qualified position whose rate of basic pay is fixed under paragraph
26 (2)(A) is eligible for an allowance under section 5941 of title 5,
27 on the same basis and to the same extent as if the employee was
28 an employee covered by section 5941, including eligibility condi-
29 tions, allowance rates, and all other terms and conditions in law
30 or regulation.

31 (4) PLAN FOR EXECUTION OF AUTHORITIES.—The Secretary shall
32 submit a report to the appropriate committees of Congress with a plan
33 for the use of the authorities provided under this subsection.

34 (5) COLLECTIVE BARGAINING AGREEMENTS.—Nothing in paragraph
35 (1) may be construed to impair the continued effectiveness of a collec-
36 tive bargaining agreement with respect to an office, component, sub-
37 component, or equivalent of the Department that is a successor to an
38 office, component, subcomponent, or equivalent of the Department cov-
39 ered by the agreement before the succession.

1 (6) REQUIRED REGULATIONS.—The Secretary, in coordination with
2 the Director of the Office of Personnel Management, shall prescribe
3 regulations for the administration of this section.

4 (e) ANNUAL REPORT.—Not later than December 18, 2018, the Secretary
5 shall submit to the appropriate committees of Congress a detailed report
6 that—

7 (1) discusses the process used by the Secretary in accepting applica-
8 tions, assessing candidates, ensuring adherence to veterans' preference,
9 and selecting applicants for vacancies to be filled by an individual for
10 a qualified position;

11 (2) describes—

12 (A) how the Secretary plans to fulfill the critical need of the De-
13 partment to recruit and retain employees in qualified positions;

14 (B) the measures that will be used to measure progress; and

15 (C) any actions taken during the reporting period to fulfill that
16 critical need;

17 (3) discusses how the planning and actions taken under paragraph
18 (2) are integrated into the strategic workforce planning of the Depart-
19 ment;

20 (4) provides metrics on actions occurring during the reporting pe-
21 riod, including—

22 (A) the number of employees in qualified positions hired by oc-
23 cupation and grade and level or pay band;

24 (B) the placement of employees in qualified positions by direc-
25 torate and office in the Department;

26 (C) the total number of veterans hired;

27 (D) the number of separations of employees in qualified posi-
28 tions by occupation and grade and level or pay band;

29 (E) the number of retirements of employees in qualified posi-
30 tions by occupation and grade and level or pay band; and

31 (F) the number and amounts of recruitment, relocation, and re-
32 tention incentives paid to employees in qualified positions by occu-
33 pation and grade and level or pay band; and

34 (5) describes the training provided to supervisors of employees in
35 qualified positions at the Department on the use of the new authorities.

36 (d) THREE-YEAR PROBATIONARY PERIOD.—The probationary period for
37 all employees hired under the authority established in this section is 3 years.

38 (e) INCUMBENTS OF EXISTING COMPETITIVE SERVICE POSITIONS.—

39 (1) IN GENERAL.—An individual serving in a position on December
40 18, 2014, who is selected to be converted to a position in the excepted
41 service under this section shall have the right to refuse the conversion.

1 (2) SUBSEQUENT CONVERSION.—After the date on which an indi-
2 vidual who refuses a conversion under paragraph (1) stops serving in
3 the position selected to be converted, the position may be converted to
4 a position in the excepted service.

5 (f) REPORT.—The Agency shall submit a report regarding the availability
6 of, and benefits (including cost savings and security) of using, cybersecurity
7 personnel and facilities outside of the National Capital Region (as defined
8 in section 2674 of title 10) to serve the Federal and national need to—

9 (1) the Subcommittee on Homeland Security of the Committee on
10 Appropriations and the Committee on Homeland Security and Govern-
11 mental Affairs of the Senate; and

12 (2) the Subcommittee on Homeland Security of the Committee on
13 Appropriations and the Committee on Homeland Security of the House
14 of Representatives.

15 **§ 10706. National Cybersecurity and Communications Inte-**
16 **gration Center**

17 (a) DEFINITIONS OF CYBERSECURITY VULNERABILITY.—In this section,
18 the term “cybersecurity vulnerability” has the meaning given the term “se-
19 curity vulnerability” in section 10701 of this title.

20 (b) FUNCTIONS.—The cybersecurity functions of the Center shall in-
21 clude—

22 (1) being a Federal civilian interface for the multi-directional and
23 cross-sector sharing of information relating to cyber threat indicators,
24 defensive measures, cybersecurity risks, incidents, analysis, and warn-
25 ings for Federal and non-Federal entities, including the implementation
26 of subchapter V of this chapter;

27 (2) providing shared situational awareness to enable real-time, inte-
28 grated, and operational actions across the Federal Government and
29 non-Federal entities to address cybersecurity risks and incidents to
30 Federal and non-Federal entities;

31 (3) coordinating the sharing of information relating to cyber threat
32 indicators, defensive measures, cybersecurity risks, and incidents across
33 the Federal Government;

34 (4) facilitating cross-sector coordination to address cybersecurity
35 risks and incidents, including cybersecurity risks and incidents that
36 may be related to or could have consequential impacts across multiple
37 sectors;

38 (5)(A) conducting integration and analysis, including cross-sector in-
39 tegration and analysis, of cyber threat indicators, defensive measures,
40 cybersecurity risks, and incidents;

1 (B) sharing mitigation protocols to counter cybersecurity
2 vulnerabilities pursuant to subsection (m), as appropriate; and

3 (C) sharing the analysis conducted under subparagraph (A) and
4 mitigation protocols to counter cybersecurity vulnerabilities in accord-
5 ance with subparagraph (B), as appropriate, with Federal and non-
6 Federal entities;

7 (6) on request, providing operational and timely technical assistance,
8 risk management support, and incident response capabilities to Federal
9 and non-Federal entities with respect to cyber threat indicators, defen-
10 sive measures, cybersecurity risks, and incidents, which may include at-
11 tribution, mitigation, and remediation, which may take the form of con-
12 tinuous monitoring and detection of cybersecurity risks to critical infra-
13 structure entities that own or operate industrial control systems that
14 support national critical functions;

15 (7) providing information and recommendations on security and re-
16 siliency measures to Federal and non-Federal entities, including infor-
17 mation and recommendations to—

18 (A) facilitate information security;

19 (B) strengthen information systems against cybersecurity risks
20 and incidents; and

21 (C) share cyber threat indicators and defensive measures;

22 (8) engaging with international partners, in consultation with other
23 appropriate agencies, to—

24 (A) collaborate on cyber threat indicators, defensive measures,
25 and information relating to cybersecurity risks and incidents; and

26 (B) enhance the security and resiliency of global cybersecurity;

27 (9) sharing cyber threat indicators, defensive measures, mitigation
28 protocols to counter cybersecurity vulnerabilities, as appropriate, and
29 other information relating to cybersecurity risks and incidents with
30 Federal and non-Federal entities, including across sectors of critical in-
31 frastructure, and with State and major urban area fusion centers, as
32 appropriate;

33 (10) participating, as appropriate, in national exercises run by the
34 Department;

35 (11) in coordination with the Emergency Communications Division,
36 assessing and evaluating consequence, vulnerability, and threat infor-
37 mation regarding cyber incidents to public safety communications to
38 help facilitate continuous improvements to the security and resiliency
39 of the communications;

1 (12) detecting, identifying, and receiving information for a cyberse-
2 curity purpose about security vulnerabilities relating to critical infra-
3 structure in information systems and devices; and

4 (13) receiving, aggregating, and analyzing reports related to covered
5 cyber incidents (as defined in section 10761 of this title) submitted by
6 covered entities (as defined in section 10761 of this title) and reports
7 related to ransom payments (as defined in section 10761 of this title)
8 submitted by covered entities (as defined in section 10761 of this title)
9 in furtherance of the activities specified in sections subsections (b) and
10 (d) of section 10702 and 10762 of this title, this subsection, and any
11 other authorized activity of the Director, to enhance the situational
12 awareness of cybersecurity threats across critical infrastructure sectors.

13 (c) COMPOSITION.—

14 (1) IN GENERAL.—The Center is composed of—

15 (A) appropriate representatives of Federal entities, such as—

16 (i) Sector Risk Management Agencies;

17 (ii) civilian and law enforcement agencies; and

18 (iii) elements of the intelligence community;

19 (B) appropriate representatives of non-Federal entities, such
20 as—

21 (i) State, local, and tribal governments;

22 (ii) Information Sharing and Analysis Organizations, in-
23 cluding information sharing and analysis centers;

24 (iii) owners and operators of critical information systems;

25 and

26 (iv) private entities, including cybersecurity specialists;

27 (C) components in the Center that carry out cybersecurity and
28 communications activities;

29 (D) a designated Federal official for operational coordination
30 with and across each sector;

31 (E) an entity that collaborates with State and local govern-
32 ments, including an entity that collaborates with election officials,
33 on cybersecurity risks and incidents, and has entered into a vol-
34 untary information sharing relationship with the Center; and

35 (F) other appropriate representatives or entities, as determined
36 by the Secretary.

37 (2) INCIDENTS.—In the event of an incident, during exigent cir-
38 cumstances the Secretary may grant a Federal or non-Federal entity
39 immediate temporary access to the Center.

40 (d) PRINCIPLES.—In carrying out the functions under subsection (b), the
41 Center shall ensure—

- 1 (1) to the extent practicable, that—
- 2 (A) timely, actionable, and relevant cyber threat indicators, de-
3 fensive measures, and information related to cybersecurity risks,
4 incidents, and analysis is shared;
- 5 (B) when appropriate, cyber threat indicators, defensive meas-
6 ures, and information related to cybersecurity risks, incidents, and
7 analysis is integrated with other relevant information and tailored
8 to the specific characteristics of a sector;
- 9 (C) activities are prioritized and conducted based on the level
10 of risk;
- 11 (D) industry sector-specific, academic, and national laboratory
12 expertise is sought and receives appropriate consideration;
- 13 (E) continuous, collaborative, and inclusive coordination oc-
14 curs—
- 15 (i) across sectors; and
- 16 (ii) with—
- 17 (I) sector coordinating councils;
- 18 (II) Information Sharing and Analysis Organizations;
- 19 and
- 20 (III) other appropriate non-Federal partners;
- 21 (F) as appropriate, the Center works to develop and use mecha-
22 nisms for sharing information related to cyber threat indicators,
23 defensive measures, cybersecurity risks, and incidents that are
24 technology-neutral, interoperable, real-time, cost-effective, and re-
25 silient;
- 26 (G) the Center works with other agencies to reduce unneces-
27 sarily duplicative sharing of information related to cyber threat in-
28 dicators, defensive measures, cybersecurity risks, and incidents;
- 29 (H) the Center designates an agency contact for non-Federal
30 entities; and
- 31 (I) activities of the Center address the security of both informa-
32 tion technology and operational technology, including industrial
33 control systems;
- 34 (2) that information related to cyber threat indicators, defensive
35 measures, cybersecurity risks, and incidents is appropriately safe-
36 guarded against unauthorized access or disclosure; and
- 37 (3) that activities conducted by the Center comply with all policies,
38 regulations, and laws that protect the privacy and civil liberties of
39 United States persons, including by working with the Privacy Officer
40 appointed under section 10520 of this title to ensure that the Center

1 follows the policies and procedures specified in subsections (c) and
2 (e)(5)(C) of section 10784 of this title.

3 (e) CYBER HUNT AND INCIDENT RESPONSE TEAMS.—

4 (1) IN GENERAL.—The Center shall maintain cyber hunt and inci-
5 dent response teams for the purpose of leading Federal asset response
6 activities and providing timely technical assistance to Federal and non-
7 Federal entities, including across all critical infrastructure sectors, re-
8 garding actual or potential security incidents, as appropriate and on re-
9 quest, including—

10 (A) assistance to asset owners and operators in restoring serv-
11 ices following a cyber incident;

12 (B) identification and analysis of cybersecurity risk and unau-
13 thorized cyber activity;

14 (C) mitigation strategies to prevent, deter, and protect against
15 cybersecurity risks;

16 (D) recommendations to asset owners and operators for improv-
17 ing overall network and control systems security to lower cyberse-
18 curity risks, and other recommendations, as appropriate; and

19 (E) such other capabilities as the Secretary determines appro-
20 priate.

21 (2) ASSOCIATED METRICS.—The Center shall—

22 (A) define the goals and desired outcomes for each cyber hunt
23 and incident response team; and

24 (B) develop metrics—

25 (i) to measure the effectiveness and efficiency of each cyber
26 hunt and incident response team in achieving the goals and
27 desired outcomes defined under subparagraph (A); and

28 (ii) that—

29 (I) are quantifiable and actionable; and

30 (II) the Center shall use to improve the effectiveness
31 and accountability of, and service delivery by, cyber hunt
32 and incident response teams.

33 (3) CYBERSECURITY SPECIALISTS.—After notice to, and with the ap-
34 proval of, the entity requesting action by or technical assistance from
35 the Center, the Secretary may include cybersecurity specialists from the
36 private sector on a cyber hunt and incident response team.

37 (f) NO RIGHT OR BENEFIT.—

38 (1) IN GENERAL.—The provision of assistance or information to, and
39 inclusion in the Center, or any team or activity of the Center, of, gov-
40 ernmental or private entities under this section shall be at the sole and

1 unreviewable discretion of the Director of the Cybersecurity and Infra-
2 structure Security Agency.

3 (2) CERTAIN ASSISTANCE OR INFORMATION.—Providing a govern-
4 mental or private entity certain assistance or information or including
5 the entity in the Center or a team or activity of the Center, pursuant
6 to this section, shall not create a right or benefit, substantive or proce-
7 dural, to similar assistance or information for any other governmental
8 or private entity.

9 (g) AUTOMATED INFORMATION SHARING.—

10 (1) IN GENERAL.—The Director, in coordination with industry and
11 other stakeholders, shall develop capabilities making use of existing in-
12 formation technology industry standards and best practices, as appro-
13 priate, that support and rapidly advance the development, adoption,
14 and implementation of automated mechanisms for the sharing of cyber
15 threat indicators and defensive measures in accordance with subchapter
16 V of this chapter.

17 (2) ANNUAL REPORT.—The Director shall submit to the Committee
18 on Homeland Security and Governmental Affairs of the Senate and the
19 Committee on Homeland Security of the House of Representatives an
20 annual report on the status and progress of the development of the ca-
21 pabilities described in paragraph (1). The reports shall be required
22 until the capabilities are fully implemented.

23 (h) VOLUNTARY INFORMATION SHARING PROCEDURES AND RELATION-
24 SHIPS.—

25 (1) PROCEDURES.—

26 (A) IN GENERAL.—The Center may enter into a voluntary in-
27 formation sharing relationship with any consenting non-Federal
28 entity for the sharing of cyber threat indicators and defensive
29 measures for cybersecurity purposes in accordance with this sec-
30 tion. Nothing in this subsection may be construed to require any
31 non-Federal entity to enter into an information sharing relation-
32 ship with the Center or any other entity. The Center may termi-
33 nate a voluntary information sharing relationship under this sub-
34 section, at the sole and unreviewable discretion of the Secretary,
35 acting through the Director, for any reason, including if the Cen-
36 ter determines that the non-Federal entity with which the Center
37 has entered into the relationship has violated the terms of this
38 subsection.

39 (B) NATIONAL SECURITY.—The Secretary may decline to enter
40 into a voluntary information sharing relationship under this sub-
41 section, at the sole and unreviewable discretion of the Secretary,

1 acting through the Director, for any reason, including if the Sec-
2 retary determines that declining to enter into the relationship is
3 appropriate for national security.

4 (2) RELATIONSHIPS.—A voluntary information sharing relationship
5 under this subsection may be characterized as an agreement described
6 as follows:

7 (A) For the use of a non-Federal entity, the Center shall make
8 available a standard agreement, consistent with this section, on
9 the Department’s website.

10 (B) At the request of a non-Federal entity, and if determined
11 appropriate by the Center, at the sole and unreviewable discretion
12 of the Secretary, acting through the Director, the Department
13 shall negotiate a non-standard agreement, consistent with this sec-
14 tion.

15 (C) An agreement between the Center and a non-Federal entity
16 that was entered into, or that was in effect, before December 18,
17 2015, shall be deemed in compliance with the requirements of this
18 subsection. An agreement under this subsection shall include the
19 relevant privacy protections as in effect under the Cooperative Re-
20 search and Development Agreement for Cybersecurity Information
21 Sharing and Collaboration, as of December 31, 2014. Nothing in
22 this subsection may be construed to require a non-Federal entity
23 to enter into either a standard or negotiated agreement to be in
24 compliance with this subsection.

25 (i) DIRECT REPORTING.—The Secretary shall develop policies and proce-
26 dures for direct reporting to the Secretary by the Director of the Center
27 regarding significant cybersecurity risks and incidents.

28 (j) REPORTS ON INTERNATIONAL COOPERATION.—The Secretary periodi-
29 cally shall submit to the Committee on Homeland Security and Govern-
30 mental Affairs of the Senate and the Committee on Homeland Security of
31 the House of Representatives a report on the range of efforts underway to
32 bolster cybersecurity collaboration with relevant international partners in ac-
33 cordance with subsection (b)(8).

34 (k) OUTREACH.—The Secretary, acting through the Director, shall—

35 (1) disseminate to the public information about how to voluntarily
36 share cyber threat indicators and defensive measures with the Center;
37 and

38 (2) enhance outreach to critical infrastructure owners and operators
39 for purposes of sharing cyber threat indicators and defensive measures
40 with the Center.

41 (l) CYBERSECURITY OUTREACH.—

1 (1) DEFINITIONS.—For purposes of this subsection, the terms
2 “small business concern” and “small business development center”
3 have the meanings given the terms in section 3 of the Small Business
4 Act (15 U.S.C. 632).

5 (2) PROVIDE ASSISTANCE.—The Secretary may leverage small busi-
6 ness development centers to provide assistance to small business con-
7 cerns by disseminating information on cyber threat indicators, defense
8 measures, cybersecurity risks, incidents, analyses, and warnings to help
9 small business concerns in developing or enhancing cybersecurity infra-
10 structure, awareness of cyber threat indicators, and cyber training pro-
11 grams for employees.

12 (m) COORDINATED VULNERABILITY DISCLOSURE.—The Secretary, in co-
13 ordination with industry and other stakeholders, may develop and adhere to
14 Department policies and procedures for coordinating vulnerability disclo-
15 sures.

16 (n) PROTOCOLS TO COUNTER CERTAIN CYBERSECURITY
17 VULNERABILITIES.—The Director may, as appropriate, identify, develop,
18 and disseminate actionable protocols to mitigate cybersecurity vulnerabilities
19 to information systems and industrial control systems, including in cir-
20 cumstances in which the vulnerabilities exist because software or hardware
21 is no longer supported by a vendor.

22 (o) SUBPOENA AUTHORITY.—

23 (1) DEFINITION OF COVERED DEVICE OR SYSTEM.—In this sub-
24 section, the term “covered device or system”—

25 (A) means a device or system commonly used to perform indus-
26 trial, commercial, scientific, or governmental functions or proc-
27 esses that relate to critical infrastructure, including operational
28 and industrial control systems, distributed control systems, and
29 programmable logic controllers; but

30 (B) does not include personal devices and systems, such as con-
31 sumer mobile devices, home computers, residential wireless rout-
32 ers, or residential internet enabled consumer devices.

33 (2) AUTHORITY.—

34 (A) IN GENERAL.—If the Director identifies a system connected
35 to the internet with a specific security vulnerability and has reason
36 to believe the security vulnerability relates to critical infrastructure
37 and affects a covered device or system, and the Director is unable
38 to identify the entity at risk that owns or operates the covered de-
39 vice or system, the Director may issue a subpoena for the produc-
40 tion of information necessary to identify and notify the entity at
41 risk, to carry out a function authorized under subsection (b)(12).

1 (B) LIMIT ON INFORMATION.—A subpoena issued pursuant to
2 subparagraph (A) may seek information—

3 (i) only in the categories set forth in subparagraphs (A),
4 (B), (D), and (E) of section 2703(e)(2) of title 18; and

5 (ii) for not more than 20 covered devices.

6 (C) LIABILITY PROTECTIONS FOR DISCLOSING PROVIDERS.—
7 The provisions of section 2703(e) of title 18, shall apply to a sub-
8 poena issued pursuant to subparagraph (A).

9 (3) COORDINATION.—

10 (A) IN GENERAL.—If the Director exercises the subpoena au-
11 thority under this subsection, and in the interest of avoiding inter-
12 ference with ongoing law enforcement investigations, the Director
13 shall coordinate the issuance of a subpoena with the Department
14 of Justice, including the Federal Bureau of Investigation, pursu-
15 ant to interagency procedures that the Director, in coordination
16 with the Attorney General, shall develop.

17 (B) CONTENTS.—The inter-agency procedures developed under
18 this paragraph shall provide that a subpoena issued by the Direc-
19 tor under this subsection shall be—

20 (i) issued to carry out a function described in subsection
21 (b)(12); and

22 (ii) subject to the limitations described in this subsection.

23 (4) NONCOMPLIANCE.—If a person, partnership, corporation, asso-
24 ciation, or entity fails to comply with a duly served subpoena issued
25 pursuant to this subsection, the Director may request that the Attorney
26 General seek enforcement of the subpoena in any judicial district in
27 which the person, partnership, corporation, association, or entity re-
28 sides, is found, or transacts business.

29 (5) NOTICE.—Not later than 7 days after the date on which the Di-
30 rector receives information obtained through a subpoena issued pursu-
31 ant to this subsection, the Director shall notify any entity identified by
32 information obtained pursuant to the subpoena regarding the subpoena
33 and the identified vulnerability.

34 (6) AUTHENTICATION.—

35 (A) IN GENERAL.—A subpoena issued pursuant to this sub-
36 section shall be authenticated with a cryptographic digital signa-
37 ture of an authorized representative of the Agency, or other com-
38 parable successor technology, that allows the Agency to dem-
39 onstrate that the subpoena was issued by the Agency and has not
40 been altered or modified since the issuance.

1 (B) INVALIDATED IF NOT AUTHENTICATED.—A subpoena
2 issued pursuant to this subsection that is not authenticated in ac-
3 cordance with subparagraph (A) shall not be considered to be valid
4 by the recipient of the subpoena.

5 (7) PROCEDURES.—The Director shall establish internal procedures
6 and associated training, applicable to employees and operations of the
7 Agency, regarding subpoenas issued pursuant to this subsection, which
8 shall address the following:

9 (A) The protection of and restriction on dissemination of non-
10 public information obtained through the subpoena, including a re-
11 quirement that the Agency not disseminate nonpublic information
12 obtained through the subpoena that identifies the party that is
13 subject to the subpoena or the entity at risk identified by informa-
14 tion obtained, except that the Agency may share the nonpublic in-
15 formation with the Department of Justice for the purpose of en-
16 forcing the subpoena in accordance with paragraph (4), and may
17 share with a Federal agency the nonpublic information of the enti-
18 ty at risk if—

19 (i) the Agency identifies or is notified of a cybersecurity in-
20 cident involving the entity that relates to the vulnerability
21 that led to the issuance of the subpoena;

22 (ii) the Director determines that sharing the nonpublic in-
23 formation with another Federal department or agency is nec-
24 essary to allow the department or agency to take a law en-
25 forcement or national security action, consistent with the
26 interagency procedures under paragraph (3)(A), or actions re-
27 lated to mitigating or otherwise resolving the incident;

28 (iii) the entity to which the information pertains is notified
29 of the Director’s determination, to the extent practicable con-
30 sistent with national security or law enforcement interests,
31 consistent with the interagency procedures; and

32 (iv) the entity consents, except that the entity’s consent
33 shall not be required if another Federal department or agency
34 identifies the entity to the Agency in connection with a sus-
35 pected cybersecurity incident.

36 (B) The restriction on the use of information obtained through
37 the subpoena for a cybersecurity purpose.

38 (C) The retention and destruction of nonpublic information ob-
39 tained through the subpoena, including—

1 (i) destruction of information that the Director determines
2 is unrelated to critical infrastructure immediately on pro-
3 viding notice to the entity pursuant to paragraph (5); and

4 (ii) destruction of any personally identifiable information
5 not later than 6 months after the date on which the Director
6 receives information obtained through the subpoena, unless
7 otherwise agreed to by the individual identified by the sub-
8 poena respondent.

9 (D) The processes for providing notice to each party that is sub-
10 ject to the subpoena and each entity identified by information ob-
11 tained under the subpoena.

12 (E) The processes and criteria for conducting critical infrastruc-
13 ture security risk assessments to determine whether a subpoena is
14 necessary prior to being issued pursuant to this subsection.

15 (F) The information to be provided to an entity at risk at the
16 time of the notice of the vulnerability, which shall include—

17 (i) a discussion or statement that responding to, or subse-
18 quent engagement with, the Agency, is voluntary; and

19 (ii) to the extent practicable, information regarding the
20 process through which the Director identifies security
21 vulnerabilities.

22 (8) LIMITATION ON PROCEDURES.—The internal procedures estab-
23 lished pursuant to paragraph (7) may not require an owner or operator
24 of critical infrastructure to take any action as a result of a notice of
25 vulnerability made pursuant to this chapter.

26 (9) REVIEW OF PROCEDURES.—Not later than 1 year after January
27 1, 2021, the Privacy Officer of the Agency shall—

28 (A) review the internal procedures established pursuant to para-
29 graph (7) to ensure that—

30 (i) the procedures are consistent with fair information
31 practices; and

32 (ii) the operations of the Agency comply with the proce-
33 dures; and

34 (B) notify the Committee on Homeland Security and Govern-
35 mental Affairs of the Senate and the Committee on Homeland Se-
36 curity of the House of Representatives of the results of the review
37 under subparagraph (A).

38 (10) PUBLICATION OF INFORMATION.—Not later than 120 days
39 after establishing the internal procedures under paragraph (7), the Di-
40 rector shall publish information on the website of the Agency regarding

1 the subpoena process under this subsection, including information re-
2 garding the following:

- 3 (A) The internal procedures.
- 4 (B) The purpose for subpoenas issued pursuant to this sub-
5 section.
- 6 (C) The subpoena process.
- 7 (D) The criteria for the critical infrastructure security risk as-
8 sessment conducted prior to issuing a subpoena.
- 9 (E) Policies and procedures on retention and sharing of data
10 obtained by subpoenas.
- 11 (F) Guidelines on how entities contacted by the Director may
12 respond to notice of a subpoena.

13 (11) ANNUAL REPORTS.—The Director shall annually submit to the
14 Committee on Homeland Security and Governmental Affairs of the
15 Senate and the Committee on Homeland Security of the House of Rep-
16 resentatives a report (which may include a classified annex but with the
17 presumption of declassification) on the use of subpoenas issued pursu-
18 ant to this subsection, which shall include the following:

- 19 (A) A discussion of the following:
- 20 (i) The effectiveness of the use of the subpoenas to miti-
21 gate critical infrastructure security vulnerabilities.
- 22 (ii) The critical infrastructure security risk assessment
23 process conducted for subpoenas issued under this subsection.
- 24 (iii) The number of subpoenas issued during the preceding
25 year.
- 26 (iv) To the extent practicable, the number of vulnerable
27 covered devices or systems mitigated under this subsection by
28 the Agency during the preceding year.
- 29 (v) The number of entities notified by the Director under
30 this subsection, and their responses, during the preceding
31 year.

32 (B) For each subpoena issued under this subsection, the fol-
33 lowing:

- 34 (i) Information relating to the source of the security vul-
35 nerability detected, identified, or received by the Director.
- 36 (ii) Information relating to the steps taken to identify the
37 entity at risk prior to issuing the subpoena.
- 38 (iii) A description of the outcome of the subpoena, includ-
39 ing discussion on the resolution or mitigation of the critical
40 infrastructure security vulnerability.

1 (12) PUBLICATION OF ANNUAL REPORTS.—The Director shall pub-
2 lish a version of the annual report required under paragraph (11) on
3 the website of the Agency, which shall, at a minimum, include the find-
4 ings described in clauses (iii), (iv), and (v) of subparagraph (A) of
5 paragraph (11).

6 (13) PROHIBITION ON USE OF INFORMATION FOR UNAUTHORIZED
7 PURPOSES.—Any information obtained pursuant to a subpoena issued
8 under this subsection may not be provided to another Federal depart-
9 ment or agency for a purpose other than a cybersecurity purpose or
10 for the purpose of enforcing a subpoena issued pursuant to this sub-
11 section.

12 (p) INDUSTRIAL CONTROL SYSTEMS.—The Director shall maintain capa-
13 bilities to identify and address threats and vulnerabilities to products and
14 technologies intended for use in the automated control of critical infrastruc-
15 ture processes. In carrying out this subsection, the Director shall—

16 (1) lead Federal Government efforts, in consultation with Sector
17 Risk Management Agencies, as appropriate, to identify and mitigate cy-
18 bersecurity threats to industrial control systems, including supervisory
19 control and data acquisition systems;

20 (2) maintain threat hunting and incident response capabilities to re-
21 spond to industrial control system cybersecurity risks and incidents;

22 (3) provide cybersecurity technical assistance to industry end-users,
23 product manufacturers, Sector Risk Management Agencies, other Fed-
24 eral agencies, and other industrial control system stakeholders to iden-
25 tify, evaluate, assess, and mitigate vulnerabilities;

26 (4) collect, coordinate, and provide vulnerability information to the
27 industrial control systems community by, as appropriate, working close-
28 ly with security researchers, industry end-users, product manufactur-
29 ers, Sector Risk Management Agencies, other Federal agencies, and
30 other industrial control systems stakeholders; and

31 (5) conduct such other efforts and assistance as the Secretary deter-
32 mines appropriate.

33 (q) COORDINATION ON CYBERSECURITY FOR SLTT ENTITIES.— The
34 Center shall, on request and to the extent practicable, and in coordination
35 as appropriate with Federal and non-Federal entities, such as the Multi-
36 State Information Sharing and Analysis Center—

37 (1) conduct exercises with SLTT entities;

38 (2) provide operational and technical cybersecurity training to SLTT
39 entities to address cybersecurity risks or incidents, with or without re-
40 imbursement, related to—

41 (A) cyber threat indicators;

- 1 (B) defensive measures;
- 2 (C) cybersecurity risks;
- 3 (D) vulnerabilities; and
- 4 (E) incident response and management;
- 5 (3) to increase situational awareness and help prevent incidents, as-
- 6 sist SLTT entities in sharing, in real time, with the Federal Govern-
- 7 ment as well as among SLTT entities, actionable—
- 8 (A) cyber threat indicators;
- 9 (B) defensive measures;
- 10 (C) information about cybersecurity risks; and
- 11 (D) information about incidents;
- 12 (4) provide SLTT entities notifications containing specific incident
- 13 and malware information that may affect them or their residents;
- 14 (5) provide to, and periodically update, SLTT entities via an easily
- 15 accessible platform and other means—
- 16 (A) information about tools;
- 17 (B) information about products;
- 18 (C) resources;
- 19 (D) policies;
- 20 (E) guidelines;
- 21 (F) controls; and
- 22 (G) other cybersecurity standards and best practices and proce-
- 23 dures related to information security, including, as appropriate, in-
- 24 formation produced by other Federal agencies;
- 25 (6) work with senior SLTT entity officials, including chief informa-
- 26 tion officers and senior election officials and through national associa-
- 27 tions, to coordinate the effective implementation by SLTT entities of
- 28 tools, products, resources, policies, guidelines, controls, and procedures
- 29 related to information security to secure the information systems, in-
- 30 cluding election systems, of SLTT entities;
- 31 (7) provide operational and technical assistance to SLTT entities to
- 32 implement tools, products, resources, policies, guidelines, controls, and
- 33 procedures on information security;
- 34 (8) assist SLTT entities in developing policies and procedures for co-
- 35 ordinating vulnerability disclosures consistent with international and
- 36 national standards in the information technology industry; and
- 37 (9) promote cybersecurity education and awareness through engage-
- 38 ments with Federal agencies and non-Federal entities.
- 39 (r) REPORTS.—Not later than 1 year after June 21, 2022, and every 2
- 40 years thereafter, the Secretary shall submit to the Committee on Homeland
- 41 Security and Governmental Affairs of the Senate and the Committee on

1 Homeland Security of the House of Representatives a report on the services
2 and capabilities that the Agency directly and indirectly provides to SLTT
3 entities.

4 **§ 10707. Plans**

5 (a) DEFINITION OF AGENCY INFORMATION SYSTEM.—In this section, the
6 term “agency information system” means an information system used or op-
7 erated by an agency or by another entity on behalf of an agency.

8 (b) INTRUSION ASSESSMENT PLAN.—

9 (1) REQUIREMENT.—The Secretary, in coordination with the Direc-
10 tor of the Office of Management and Budget, shall—

11 (A) develop and implement an intrusion assessment plan to
12 proactively detect, identify, and remove intruders in agency infor-
13 mation systems on a routine basis; and

14 (B) update the plan as necessary.

15 (2) EXCEPTION.—The intrusion assessment plan required under
16 paragraph (1) shall not apply to the Department of Defense, a national
17 security system, or an element of the intelligence community.

18 (c) CYBER INCIDENT RESPONSE PLANS.—The Director shall, in coordi-
19 nation with appropriate Federal departments and agencies, State and local
20 governments, sector coordinating councils, Information Sharing and Anal-
21 ysis Organizations, owners and operators of critical infrastructure, and
22 other appropriate entities and individuals, develop, update not less often
23 than biennially, maintain, and exercise adaptable cyber incident response
24 plans to address cybersecurity risks to critical infrastructure. The Director,
25 in consultation with relevant Sector Risk Management Agencies and the Na-
26 tional Cyber Director, shall develop mechanisms to engage with stakeholders
27 to educate the stakeholders regarding Federal Government cybersecurity
28 roles and responsibilities for cyber incident response.

29 (d) NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination
30 with the heads of other appropriate Federal departments and agencies, and
31 in accordance with the National Cybersecurity Incident Response Plan re-
32 quired under subsection (c), shall regularly update, maintain, and exercise
33 the Cyber Incident Annex to the National Response Framework of the De-
34 partment.

35 (e) HOMELAND SECURITY STRATEGY TO IMPROVE THE CYBERSECURITY
36 OF STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS

37 (1) IN GENERAL

38 (A) DEVELOPMENT AND AVAILABILITY.—Not later than Decem-
39 ber 27, 2022, the Secretary, acting through the Director, shall, in
40 coordination with the heads of appropriate Federal agencies,
41 State, local, Tribal, and territorial governments, and other stake-

1 holders, as appropriate, develop and make publicly available a
2 Homeland Security Strategy to Improve the Cybersecurity of
3 State, Local, Tribal, and Territorial Governments.

4 (B) RECOMMENDATIONS AND REQUIREMENTS.—The strategy
5 required under subparagraph (A) shall provide recommendations
6 relating to the ways in which the Federal Government should sup-
7 port and promote the ability of State, local, Tribal, and territorial
8 governments to identify, mitigate against, protect against, detect,
9 respond to, and recover from cybersecurity risks, cybersecurity
10 threats, and incidents.

11 (2) CONTENTS.—The strategy required under paragraph (1) shall—

12 (A) identify capability gaps in the ability of State, local, Tribal,
13 and territorial governments to identify, protect against, detect, re-
14 spond to, and recover from cybersecurity risks, cybersecurity
15 threats, incidents, and ransomware incidents;

16 (B) identify Federal resources and capabilities that are available
17 or could be made available to State, local, Tribal, and territorial
18 governments to help those governments identify, protect against,
19 detect, respond to, and recover from cybersecurity risks, cyberse-
20 curity threats, incidents, and ransomware incidents;

21 (C) identify and assess the limitations of Federal resources and
22 capabilities available to State, local, Tribal, and territorial govern-
23 ments to help those governments identify, protect against, detect,
24 respond to, and recover from cybersecurity risks, cybersecurity
25 threats, incidents, and ransomware incidents and make rec-
26 ommendations to address such limitations;

27 (D) identify opportunities to improve the coordination of the
28 Agency with Federal and non-Federal entities, such as the Multi-
29 State Information Sharing and Analysis Center, to improve—

30 (i) incident exercises, information sharing and incident no-
31 tification procedures;

32 (ii) the ability for State, local, Tribal, and territorial gov-
33 ernments to voluntarily adapt and implement guidance in
34 Federal binding operational directives; and

35 (iii) opportunities to leverage Federal schedules for cyberse-
36 curity investments undersection 502 of title 40;

37 (E) recommend new initiatives the Federal Government should
38 undertake to improve the ability of State, local, Tribal, and terri-
39 torial governments to identify, protect against, detect, respond to,
40 and recover from cybersecurity risks, cybersecurity threats, inci-
41 dents, and ransomware incidents;

1 (F) set short-term and long-term goals that will improve the
2 ability of State, local, Tribal, and territorial governments to iden-
3 tify, protect against, detect, respond to, and recover from cyberse-
4 curity risks, cybersecurity threats, incidents, and ransomware inci-
5 dents; and

6 (G) set dates, including interim benchmarks, as appropriate for
7 State, local, Tribal, and territorial governments to establish base-
8 line capabilities to identify, protect against, detect, respond to, and
9 recover from cybersecurity risks, cybersecurity threats, incidents,
10 and ransomware incidents.

11 (3) CONSIDERATIONS.—In developing the strategy required under
12 paragraph (1), the Director, in coordination with the heads of appro-
13 priate Federal agencies, State, local, Tribal, and territorial govern-
14 ments, and other stakeholders, as appropriate, shall consider—

15 (A) lessons learned from incidents that have affected State,
16 local, Tribal, and territorial governments, and exercises with Fed-
17 eral and non-Federal entities;

18 (B) the impact of incidents that have affected State, local, Trib-
19 al, and territorial governments, including the resulting costs to the
20 governments;

21 (C) the information related to the interest and ability of state
22 and non-state threat actors to compromise information systems
23 owned or operated by State, local, Tribal, and territorial govern-
24 ments; and

25 (D) emerging cybersecurity risks and cybersecurity threats to
26 State, local, Tribal, and territorial governments resulting from the
27 deployment of new technologies.

28 (4) EXEMPTION.—Chapter 35 of title 44 shall not apply to any action
29 to implement this subsection.

30 (f) NATIONAL CYBER EXERCISE PROGRAM.—

31 (1) DEFINITIONS.—In this subsection:

32 (A) PRIVATE ENTITY.—The term “private entity” has the
33 meaning given that term in section 10801 of this title.

34 (B) STATE.—The term “State” means a State, the District of
35 Columbia, Puerto Rico, Guam, American Samoa, the Virgin Is-
36 lands, the Northern Mariana Islands, and any other territory (in-
37 cluding a possession) of the United States.

38 (2) IN GENERAL.—

39 (A) ESTABLISHMENT.—There is in the Agency the National
40 Cyber Exercise Program (referred to in this subsection as the

1 “Exercise Program”) to evaluate the National Cyber Incident Re-
2 sponse Plan, and other related plans and strategies.

3 (B) REQUIREMENTS.—

4 (i) IN GENERAL.—The Exercise Program shall be—

5 (I) based on current risk assessments, including cred-
6 ible threats, vulnerabilities, and consequences;

7 (II) designed, to the extent practicable, to simulate the
8 partial or complete incapacitation of a government or
9 critical infrastructure network resulting from a cyber in-
10 cident;

11 (III) designed to provide for the systematic evaluation
12 of cyber readiness and enhance operational under-
13 standing of the cyber incident response system and rel-
14 evant information sharing agreements; and

15 (IV) designed to promptly develop after-action reports
16 and plans that can quickly incorporate lessons learned
17 into future operations.

18 (ii) MODEL EXERCISE SELECTION.—The Exercise Program
19 shall—

20 (I) include a selection of model exercises that govern-
21 ment and private entities can readily adapt for use; and

22 (II) aid the governments and private entities with the
23 design, implementation, and evaluation of exercises
24 that—

25 (aa) conform to the requirements described in
26 clause (i);

27 (bb) are consistent with any applicable national,
28 State, local, or Tribal strategy or plan; and

29 (cc) provide for systematic evaluation of readi-
30 ness.

31 (C) CONSULTATION.—In carrying out the Exercise Program,
32 the Director may consult with appropriate representatives from
33 Sector Risk Management Agencies, the Office of the National
34 Cyber Director, cybersecurity research stakeholders, and Sector
35 Coordinating Councils.

36 (3) RULE OF CONSTRUCTION.—Nothing in this section shall be con-
37 strued to affect the authorities or responsibilities of the Administrator
38 of the Federal Emergency Management Agency pursuant to subsections
39 (a) and (b) of section 20508 of this title.

1 **§ 10708. Strategy**

2 (a) DEVELOPMENT OF STRATEGY.—The Secretary shall develop a depart-
3 mental strategy to carry out cybersecurity responsibilities as set forth by
4 law.

5 (b) CONTENTS.—The strategy required under subsection (a) shall include
6 the following:

7 (1) Strategic and operational goals and priorities to successfully exe-
8 cute the full range of the Secretary’s cybersecurity responsibilities.

9 (2) Information on the programs, policies, and activities that are re-
10 quired to successfully execute the full range of the Secretary’s cyberse-
11 curity responsibilities, including programs, policies, and activities in
12 furtherance of the following:

13 (A) Cybersecurity functions set forth in section 10706 of this
14 title.

15 (B) Cybersecurity investigation capabilities.

16 (C) Cybersecurity research and development.

17 (D) Engagement with international cybersecurity partners.

18 (d) CONSIDERATIONS.—In developing the strategy required under sub-
19 section (a), the Secretary shall—

20 (1) consider—

21 (A) the cybersecurity strategy for the Homeland Security Enter-
22 prise published by the Secretary in November 2011;

23 (B) the Department of Homeland Security Fiscal Years 2014–
24 2018 Strategic Plan; and

25 (C) the most recent quadrennial homeland security review
26 issued pursuant to section 11706 of this title; and

27 (2) include information on the roles and responsibilities of compo-
28 nents and offices of the Department, to the extent practicable, to carry
29 out the strategy.

30 (d) IMPLEMENTATION PLAN.—Not later than 90 days after the develop-
31 ment of the strategy required under subsection (a), the Secretary shall issue
32 an implementation plan for the strategy that includes the following:

33 (1) Strategic objectives and corresponding tasks.

34 (2) Projected timelines and costs for the tasks.

35 (3) Metrics to evaluate performance of the tasks.

36 (e) CONGRESSIONAL OVERSIGHT.—The Secretary shall submit to Con-
37 gress for assessment the following:

38 (1) A copy of the strategy required under subsection (a), on
39 issuance.

1 (2) A copy of the implementation plan required under subsection (d),
2 on issuance, together with detailed information on any associated legis-
3 lative or budgetary proposals.

4 (f) CLASSIFIED INFORMATION.—The strategy required under subsection
5 (a) shall be in an unclassified form but may contain a classified annex.

6 (g) RULE OF CONSTRUCTION.—Nothing in this section may be construed
7 as permitting the Department to engage in monitoring, surveillance,
8 exfiltration, or other collection activities for the purpose of tracking an indi-
9 vidual’s personally identifiable information.

10 **§ 10709. NET Guard**

11 The Director may establish a national technology guard, to be known as
12 “NET Guard”, comprised of local teams of volunteers with expertise in rel-
13 evant areas of science and technology, to assist local communities to respond
14 and recover from attacks on information systems and communications net-
15 works.

16 **§ 10710. Clearances**

17 The Secretary shall make available the process of application for security
18 clearances under Executive Order 13549 (50 U.S.C. 3161 note) or any suc-
19 cessor Executive order to appropriate representatives of sector coordinating
20 councils, sector Information Sharing and Analysis Organizations, owners
21 and operators of critical infrastructure, and any other person the Secretary
22 determines appropriate.

23 **§ 10711. Federal intrusion detection and prevention system**

24 (a) DEFINITIONS.—In subsections (a) through (f) of this section:

25 (1) AGENCY.—The term “agency” has the meaning given the term
26 in section 3502 of title 44.

27 (2) AGENCY INFORMATION.—The term “agency information” means
28 information collected or maintained by or on behalf of an agency.

29 (3) AGENCY INFORMATION SYSTEM.—The term “agency information
30 system” has the meaning given the term in section 10707 of this title.

31 (b) DEPLOYMENT, OPERATION, AND MAINTENANCE OF CAPABILITIES.—

32 (1) IN GENERAL.—The Secretary shall deploy, operate, and main-
33 tain, to make available for use by any agency, with or without reim-
34 bursement—

35 (A) a capability to detect cybersecurity risks in network traffic
36 transiting or traveling to or from an agency information system;
37 and

38 (B) a capability to—

39 (i) prevent network traffic associated with those cybersecu-
40 rity risks from transiting or traveling to or from an agency
41 information system; or

1 (ii) modify the network traffic to remove the cybersecurity
2 risk.

3 (2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy
4 new technologies and modify existing technologies to the intrusion de-
5 tection and prevention capabilities described in paragraph (1) as appro-
6 priate to improve the intrusion detection and prevention capabilities.

7 (c) ACTIVITIES.—In carrying out subsection (b), the Secretary—

8 (1) may access, and the head of an agency may disclose to the Sec-
9 retary or a private entity providing assistance to the Secretary under
10 paragraph (2), information transiting or traveling to or from an agency
11 information system, regardless of the location from which the Secretary
12 or a private entity providing assistance to the Secretary under para-
13 graph (2) accesses the information, notwithstanding another law that
14 would otherwise restrict or prevent the head of an agency from dis-
15 closing the information to the Secretary or a private entity providing
16 assistance to the Secretary under paragraph (2);

17 (2) may enter into contracts or other agreements with, or otherwise
18 request and obtain the assistance of, private entities to deploy, operate,
19 and maintain technologies in accordance with subsection (b);

20 (3) may retain, use, and disclose information obtained through the
21 conduct of activities authorized under this section only to protect infor-
22 mation and information systems from cybersecurity risks;

23 (4) shall regularly assess, through operational test and evaluation in
24 real world or simulated environments, available advanced protective
25 technologies to improve detection and prevention capabilities, including
26 commercial and noncommercial technologies and detection technologies
27 beyond signature-based detection, and acquire, test, and deploy the
28 technologies when appropriate;

29 (5) shall establish a pilot through which the Secretary may acquire,
30 test, and deploy, as rapidly as possible, technologies described in para-
31 graph (4); and

32 (6) shall periodically update the privacy impact assessment required
33 under section 208(b) of the E-Government Act of 2002 (44 U.S.C.
34 3501 note).

35 (d) PRINCIPLES.—In carrying out subsection (b), the Secretary shall en-
36 sure that—

37 (1) activities carried out under this section are reasonably necessary
38 for the purpose of protecting agency information and agency informa-
39 tion systems from a cybersecurity risk;

1 (2) information accessed by the Secretary will be retained no longer
2 than reasonably necessary for the purpose of protecting agency infor-
3 mation and agency information systems from a cybersecurity risk;

4 (3) notice has been provided to users of an agency information sys-
5 tem concerning access to communications of users of the agency infor-
6 mation system for the purpose of protecting agency information and
7 the agency information system; and

8 (4) the activities are implemented pursuant to policies and proce-
9 dures governing the operation of the intrusion detection and prevention
10 capabilities.

11 (e) PRIVATE ENTITIES.—

12 (1) CONDITIONS.—A private entity described in subsection (c)(2)
13 may not—

14 (A) disclose any network traffic transiting or traveling to or
15 from an agency information system to any entity other than the
16 Department or the agency that disclosed the information under
17 subsection (c)(1), including personal information of a specific indi-
18 vidual or information that identifies a specific individual not di-
19 rectly related to a cybersecurity risk; or

20 (B) use any network traffic transiting or traveling to or from
21 an agency information system to which the private entity gains ac-
22 cess in accordance with this section for any purpose other than to
23 protect agency information and agency information systems
24 against cybersecurity risks or to administer a contract or other
25 agreement entered into pursuant to subsection (c)(2) or as part
26 of another contract with the Secretary.

27 (2) LIMITATION ON LIABILITY.—No cause of action shall lie in any
28 court against a private entity for assistance provided to the Secretary
29 in accordance with this section and any contract or agreement entered
30 into pursuant to subsection (c)(2).

31 (3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be
32 construed to authorize an Internet service provider to break a user
33 agreement with a customer without the consent of the customer.

34 (f) PRIVACY OFFICER REVIEW.—The Privacy Officer appointed under
35 section 10520 of this title, in consultation with the Attorney General, shall
36 review the policies and guidelines for the program carried out under this
37 section to ensure that the policies and guidelines are consistent with applica-
38 ble privacy laws, including those governing the acquisition, interception, re-
39 tention, use, and disclosure of communications.

40 (g) AGENCY RESPONSIBILITIES.—

1 (1) DEFINITION OF AGENCY INFORMATION SYSTEM.—In this sub-
2 section, the term “agency information system” means an information
3 system owned or operated by an agency.

4 (2) IN GENERAL.—Except as provided in paragraph (3)—

5 (A) the head of each agency shall apply and continue to utilize
6 the intrusion detection and prevention capabilities to all informa-
7 tion traveling between an agency information system and another
8 information system; and

9 (B) not later than 6 months after the date on which the Sec-
10 retary makes available improvements to the intrusion detection
11 and prevention capabilities pursuant to subsection (b)(2), the head
12 of each agency shall apply and continue to utilize the improved in-
13 trusion detection and prevention capabilities.

14 (3) EXCEPTION.—The requirements under paragraph (2) shall not
15 apply to the Department of Defense, a national security system, or an
16 element of the intelligence community.

17 (4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be
18 construed to limit an agency from applying the intrusion detection and
19 prevention capabilities to an information system other than an agency
20 information system under subsection (b)(1) at the discretion of the
21 head of the agency or as provided in relevant policies, directives, and
22 guidelines.

23 (h) RULE OF CONSTRUCTION.—Nothing in subsection (i) shall be con-
24 strued to affect the limitation of liability of a private entity for assistance
25 provided to the Secretary under subsection (c)(2) if the assistance was ren-
26 dered before the termination date under subsection (i) or otherwise during
27 a period in which the assistance was authorized.

28 (i) TERMINATION.—The requirements under subsections (a) through (f)
29 terminate on September 30, 2023.

30 **§ 10712. National asset database**

31 (a) ESTABLISHMENT.—

32 (1) NATIONAL ASSET DATABASE.—The Secretary shall establish and
33 maintain a national database of each system or asset that—

34 (A) the Secretary, in consultation with appropriate homeland se-
35 curity officials of the States, determines to be vital and the loss,
36 interruption, incapacity, or destruction of which would have a neg-
37 ative or debilitating effect on the economic security, public health,
38 or safety of the United States, a State, or a local government; or

39 (B) the Secretary determines is appropriate for inclusion in the
40 database.

1 (2) PRIORITIZED CRITICAL INFRASTRUCTURE LIST.—In accordance
2 with Homeland Security Presidential Directive–7, as in effect on Janu-
3 ary 1, 2007, the Secretary shall establish and maintain a single classi-
4 fied prioritized list of systems and assets included in the database
5 under paragraph (1) that the Secretary determines would, if destroyed
6 or disrupted, cause national or regional catastrophic effects.

7 (b) USE OF DATABASE.—The Secretary shall use the database estab-
8 lished under subsection (a)(1) in the development and implementation of
9 Department plans and programs as appropriate.

10 (c) MAINTENANCE OF DATABASE.—

11 (1) IN GENERAL.—The Secretary shall maintain and annually up-
12 date the database established under subsection (a)(1) and the list es-
13 tablished under subsection (a)(2), including—

14 (A) establishing data collection guidelines and providing the
15 guidelines to the appropriate homeland security official of each
16 State;

17 (B) regularly reviewing the guidelines established under sub-
18 paragraph (A), including by consulting with the appropriate home-
19 land security officials of States, to solicit feedback about the
20 guidelines, as appropriate;

21 (C) after providing the homeland security official of a State
22 with the guidelines under subparagraph (A), allowing the official
23 a reasonable amount of time to submit to the Secretary data rec-
24 ommended by the official for inclusion in the database established
25 under subsection (a)(1);

26 (D) examining the contents and identifying submissions made
27 by the official that are described incorrectly or that do not meet
28 the guidelines established under subparagraph (A); and

29 (E) providing to the appropriate homeland security official of
30 each relevant State a list of submissions identified under subpara-
31 graph (D) for review and possible correction before the Secretary
32 finalizes the decision of which submissions will be included in the
33 database established under subsection (a)(1).

34 (2) ORGANIZATION OF INFORMATION IN DATABASE.—The Secretary
35 shall organize the contents of the database established under subsection
36 (a)(1) and the list established under subsection (a)(2) as the Secretary
37 determines is appropriate. Any organizational structure of the contents
38 shall include the categorization of the contents—

39 (A) according to the sectors listed in the National Infrastruc-
40 ture Protection Plan developed pursuant to Homeland Security
41 Presidential Directive–7; and

1 (B) by the State and county of their location.

2 (3) PRIVATE-SECTOR INTEGRATION.—The Secretary shall identify
3 and evaluate methods, including the Department’s Protected Critical
4 Infrastructure Information Program, to acquire relevant private-sector
5 information for the purpose of using that information to generate a
6 database or list, including the database established under subsection
7 (a)(1) and the list established under subsection (a)(2).

8 (4) RETENTION OF CLASSIFICATION.—The classification of informa-
9 tion required to be provided to Congress, the Department, or another
10 department or agency under this section by a Sector Risk Management
11 Agency, including the assignment of a level of classification of the in-
12 formation, shall be binding on Congress, the Department, and that
13 other Federal agency.

14 (d) REPORTS.—

15 (1) ANNUAL REPORT REQUIRED.—The Secretary shall submit annu-
16 ally to the Committee on Homeland Security and Governmental Affairs
17 of the Senate and the Committee on Homeland Security of the House
18 of Representatives a report on the database established under sub-
19 section (a)(1) and the list established under subsection (a)(2).

20 (2) CONTENTS.—Each report shall include the following:

21 (A) The name, location, and sector classification of each of the
22 systems and assets on the list established under subsection (a)(2).

23 (B) The name, location, and sector classification of each of the
24 systems and assets on the list that are determined by the Sec-
25 retary to be most at risk to terrorism.

26 (C) Any significant challenges in compiling the list of the sys-
27 tems and assets included on the list or in the database established
28 under subsection (a)(1).

29 (D) Any significant changes from the preceding report in the
30 systems and assets included on the list or in the database.

31 (E) If appropriate, the extent to which the database and the list
32 have been used, individually or jointly, for allocating funds by the
33 Federal Government to prevent, reduce, mitigate, or respond to
34 acts of terrorism.

35 (F) The amount of coordination between the Department and
36 the private sector, through an entity of the Department that meets
37 with representatives of private-sector industries for purposes of co-
38 ordination, for the purpose of ensuring the accuracy of the data-
39 base and list.

40 (G) Other information the Secretary deems relevant.

1 (3) CLASSIFIED INFORMATION.—The report shall be submitted in
2 unclassified form but may contain a classified annex.

3 (e) NATIONAL INFRASTRUCTURE PROTECTION CONSORTIUM.—The Sec-
4 retary may establish the National Infrastructure Protection Consortium.
5 The National Infrastructure Protection Consortium may advise the Sec-
6 retary on the best way to identify, generate, organize, and maintain a data-
7 base or list of systems and assets established by the Secretary, including
8 the database established under subsection (a)(1) and the list established
9 under subsection (a)(2). If the Secretary establishes the National Infra-
10 structure Protection Consortium, the Consortium may—

11 (1) be composed of national laboratories, Federal agencies, State and
12 local homeland security organizations, academic institutions, or na-
13 tional Centers of Excellence that have demonstrated experience working
14 with and identifying critical infrastructure and key resources; and

15 (2) provide input to the Secretary on any request pertaining to the
16 contents of the database or the list.

17 **§ 10713. Prohibition on new regulatory authority**

18 (a) NATIONAL CYBERSECURITY PROTECTION ACT OF 2014.—Nothing in
19 the National Cybersecurity Protection Act of 2014 (Public Law 113–282,
20 128 Stat. 3066) or the amendments made by the Act shall be construed—

21 (1) to grant the Secretary any authority to promulgate regulations
22 or set standards relating to the cybersecurity of private-sector critical
23 infrastructure that was not in effect on December 17, 2014; or

24 (2) to require any private entity—

25 (A) to request assistance from the Secretary; or

26 (B) that requested assistance from the Secretary to implement
27 any measure or recommendation suggested by the Secretary.

28 (b) SECTION 1716(B) OF THE WILLIAM. M. (MAC) THORNBERRY NA-
29 TIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2021.—Nothing
30 in section 1716 of the William M. (Mac) Thornberry National Defense Au-
31 thorization Act for Fiscal Year 2021 (Public Law 116–263, div. A, title
32 XVII, 134 Stat. 4094) or the amendments made by that section shall be
33 construed—

34 (1) to grant the Secretary or the head of any other Federal agency
35 or department any authority to promulgate regulations or set standards
36 relating to the cybersecurity of private-sector critical infrastructure
37 that was not in effect on December 31, 2020; or

38 (2) to require any private entity—

39 (A) to request assistance from the Director; or

40 (B) to implement any measure or recommendation suggested by
41 the Director.

Subchapter II—Critical Infrastructure Information

§ 10731. Definitions

In this subchapter:

(1) AGENCY.—The term “agency” has the meaning given the term in section 551 of title 5.

(2) COVERED FEDERAL AGENCY.—The term “covered Federal agency” means the Department.

(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term “critical infrastructure information” has the meaning given the term in section 10701 of this title.

(4) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.—The term “critical infrastructure protection program” means a component or bureau of a covered Federal agency that has been designated by the President or an agency head to receive critical infrastructure information.

(5) PROTECTED SYSTEM.—The term “protected system”—

(A) means a service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes a physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(6) VOLUNTARY.—

(A) IN GENERAL.—The term “voluntary”, in the case of a submittal of critical infrastructure information to a covered Federal agency, means the submittal of the information in the absence of the agency’s exercise of legal authority to compel access to, or submission of, the information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) EXCLUSIONS.—The term “voluntary”—

(i) in the case of an action brought under the securities laws as is defined in section 3(a) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a))—

(I) does not include information or statements contained in documents or materials filed with the Securities

1 and Exchange Commission, or with Federal banking reg-
2 ulators, under section 12(i) of the Securities Exchange
3 Act of 1934 (15 U.S.C. 78l(i)); and

4 (II) with respect to the submittal of critical infrastruc-
5 ture information, does not include a disclosure or writing
6 that when made accompanied the solicitation of an offer
7 or a sale of securities; and

8 (ii) does not include information or statements submitted
9 or relied upon as a basis for making licensing or permitting
10 determinations, or during regulatory proceedings.

11 **§ 10732. Designation of critical infrastructure protection**
12 **program**

13 A critical infrastructure protection program may be designated as such
14 by one of the following:

15 (1) The President.

16 (2) The Secretary.

17 **§ 10733. Protection of voluntarily shared critical infrastruc-**
18 **ture information**

19 (a) PROTECTION.—

20 (1) DEFINITION OF EXPRESS STATEMENT.—For purposes of para-
21 graph (2), the term “express statement”, with respect to information
22 or records, means—

23 (A) in the case of written information or records, a written
24 marking on the information or records substantially similar to the
25 following: “This information is voluntarily submitted to the Fed-
26 eral Government in expectation of protection from disclosure as
27 provided by the Critical Infrastructure Information Act of 2002.”;
28 or

29 (B) in the case of oral information, a similar written statement
30 submitted within a reasonable period following the oral commu-
31 nication.

32 (2) IN GENERAL.—Notwithstanding another law, critical infrastruc-
33 ture information (including the identity of the submitting person or en-
34 tity) that is voluntarily submitted to a covered Federal agency for use
35 by that agency regarding the security of critical infrastructure and pro-
36 tected systems, analysis, warning, interdependency study, recovery, re-
37 constitution, or other informational purpose, when accompanied by an
38 express statement specified in paragraph (1)—

39 (A) shall be exempt from disclosure under section 552 of title
40 5 (known as the Freedom of Information Act);

1 (B) shall not be subject to agency rules or judicial doctrine re-
2 garding ex parte communications with a decision-making official;

3 (C) shall not, without the written consent of the person or enti-
4 ty submitting the information, be used directly by the agency, an-
5 other Federal, State, or local authority, or a third party, in a civil
6 action arising under Federal or State law if the information is
7 submitted in good faith;

8 (D) shall not, without the written consent of the person or enti-
9 ty submitting the information, be used or disclosed by an officer
10 or employee of the United States for purposes other than the pur-
11 poses of this subchapter, except—

12 (i) in furtherance of an investigation or the prosecution of
13 a criminal act; or

14 (ii) when disclosure of the information would be—

15 (I) to either House of Congress, or to the extent of
16 matter within its jurisdiction, a committee or sub-
17 committee of Congress (including a joint committee or
18 subcommittee); or

19 (II) to the Comptroller General, or an authorized rep-
20 resentative of the Comptroller General, in the course of
21 the performance of the duties of the Government Ac-
22 countability Office;

23 (E) shall not, if provided to a State or local government or gov-
24 ernment agency—

25 (i) be made available pursuant to State or local law requir-
26 ing disclosure of information or records;

27 (ii) otherwise be disclosed or distributed to a party by the
28 State or local government or government agency without the
29 written consent of the person or entity submitting the infor-
30 mation; or

31 (iii) be used other than for the purpose of protecting crit-
32 ical infrastructure or protected systems, or in furtherance of
33 an investigation or the prosecution of a criminal act; and

34 (F) does not constitute a waiver of an applicable privilege or
35 protection provided under law, such as trade secret protection.

36 (b) LIMITATION.—A communication of critical infrastructure information
37 to a covered Federal agency made pursuant to this subchapter shall not be
38 considered to be an action subject to the requirements of chapter 10 of title
39 5.

40 (c) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section
41 shall be construed to limit or otherwise affect the ability of a State, local,

1 or Federal Government entity, agency, or authority, or a third party, under
2 applicable law, to obtain critical infrastructure information in a manner not
3 covered by subsection (a), including information lawfully and properly dis-
4 closed generally or broadly to the public and to use the information in any
5 manner permitted by law. For purposes of this section, a permissible use
6 of independently obtained information includes the disclosure of the infor-
7 mation under section 2302(b)(8) of title 5.

8 (d) TREATMENT OF VOLUNTARY SUBMITTAL OF INFORMATION.—The
9 voluntary submittal to the Government of information or records that are
10 protected from disclosure by this subchapter shall not be construed to con-
11 stitute compliance with a requirement to submit the information to a Fed-
12 eral agency under any other provision of law.

13 (e) PROCEDURES.—

14 (1) IN GENERAL.—The Secretary shall, in consultation with appro-
15 priate representatives of the National Security Council and the Office
16 of Science and Technology Policy, establish uniform procedures for the
17 receipt, care, and storage by Federal agencies of critical infrastructure
18 information that is voluntarily submitted to the Government.

19 (2) ELEMENTS.—The procedures established under paragraph (1)
20 shall include mechanisms regarding—

21 (A) the acknowledgement of receipt by Federal agencies of crit-
22 ical infrastructure information that is voluntarily submitted to the
23 Government;

24 (B) the maintenance of the identification of the information as
25 voluntarily submitted to the Government for purposes of, and sub-
26 ject to, this subchapter;

27 (C) the care and storage of the information; and

28 (D) the protection and maintenance of the confidentiality of the
29 information so as to permit the sharing of the information within
30 the Federal Government and with State and local governments,
31 and the issuance of notices and warnings related to the protection
32 of critical infrastructure and protected systems, in a manner to
33 protect from public disclosure the identity of the submitting per-
34 son or entity, or information that is proprietary, business sensitive,
35 relates specifically to the submitting person or entity, or is other-
36 wise not appropriately in the public domain.

37 (f) PENALTIES.—Whoever, being an officer or employee of the United
38 States or of any department or agency thereof, knowingly publishes, di-
39 vulges, discloses, or makes known in any manner or to any extent not au-
40 thorized by law, any critical infrastructure information protected from dis-
41 closure by this subchapter coming to him or her in the course of this em-

1 ployment or official duties or by reason of any examination or investigation
2 made by, or return, report, or record made to or filed with, the department
3 or agency or officer or employee thereof, shall be fined under title 18, im-
4 prisoned not more than 1 year, or both, and shall be removed from office
5 or employment.

6 (g) **AUTHORITY TO ISSUE WARNINGS.**—The Federal Government may
7 provide advisories, alerts, and warnings to relevant companies, targeted sec-
8 tors, other governmental entities, or the general public regarding potential
9 threats to critical infrastructure as appropriate. In issuing a warning, the
10 Federal Government shall take appropriate actions to protect from disclo-
11 sure—

12 (1) the source of voluntarily submitted critical infrastructure infor-
13 mation that forms the basis for the warning; or

14 (2) information that is proprietary, business sensitive, relates specifi-
15 cally to the submitting person or entity, or is otherwise not appro-
16 priately in the public domain.

17 (h) **AUTHORITY TO DELEGATE.**—The President may delegate authority
18 to a critical infrastructure protection program, designated under section
19 10732 of this title, to enter into a voluntary agreement to promote critical
20 infrastructure security, including with an Information Sharing and Analysis
21 Organization, or a plan of action as otherwise defined in section 708 of the
22 Defense Production Act of 1950 (50 U.S.C. 4558).

23 **§ 10734. No private right of action**

24 Nothing in this subchapter may be construed to create a private right of
25 action for enforcement of a provision of this subtitle (except chapter 129).

26 **Subchapter III—Cyber Response and** 27 **Recovery**

28 **§ 10741. Definitions**

29 For the purposes of this subchapter:

30 (1) **ASSET RESPONSE ACTIVITY.**—The term “asset response activity”
31 means an activity to support an entity impacted by an incident with
32 the response to, remediation of, or recovery from, the incident, includ-
33 ing—

34 (A) furnishing technical and advisory assistance to the entity to
35 protect the assets of the entity, mitigate vulnerabilities, and reduce
36 the related impacts;

37 (B) assessing potential risks to the critical infrastructure sector
38 or geographic region impacted by the incident, including potential
39 cascading effects of the incident on other critical infrastructure
40 sectors or geographic regions;

1 (C) developing courses of action to mitigate the risks assessed
2 under subparagraph (B);

3 (D) facilitating information sharing and operational coordina-
4 tion with entities performing threat response activities; and

5 (E) providing guidance on how best to use Federal resources
6 and capabilities in a timely, effective manner to speed recovery
7 from the incident.

8 (2) DECLARATION.—The term “declaration” means a declaration of
9 the Secretary under section 10742(a)(1) of this title.

10 (3) DIRECTOR.—The term “Director” means the Director of the Cy-
11 bersecurity and Infrastructure Security Agency.

12 (4) FEDERAL AGENCY.—The term “Federal agency” has the mean-
13 ing given the term “agency” in section 3502 of title 44.

14 (5) FUND.—The term “Fund” means the Cyber Response and Re-
15 recovery Fund under section 10743(a) of this title.

16 (6) INCIDENT.—The term “incident” has the meaning given the
17 term “agency” in section 3552 of title 44.

18 (7) RENEWAL.—The term “renewal” means a renewal of a declara-
19 tion under section 10742(d) of this title.

20 (8) SIGNIFICANT INCIDENT.—The term “significant incident”—

21 (A) means an incident or a group of related incidents that re-
22 sults, or is likely to result, in demonstrable harm to—

23 (i) the national security interests, foreign relations, or
24 economy of the United States; or

25 (ii) the public confidence, civil liberties, or public health
26 and safety of the people of the United States; and

27 (B) does not include an incident or a portion of a group of re-
28 lated incidents that occurs on—

29 (i) a national security system (as defined in section 3552
30 of title 44); or

31 (ii) an information system described in paragraph (2) or

32 (3) of section 3553(e) of title 44.

33 § 10742. Declaration

34 (a) IN GENERAL.—

35 (1) DECLARATION.—The Secretary, in consultation with the Na-
36 tional Cyber Director, may make a declaration of a significant incident
37 in accordance with this section for the purpose of enabling the activities
38 described in this subchapter if the Secretary determines—

39 (A) a specific significant incident—

40 (i) has occurred; or

41 (ii) is likely to occur imminently; and

1 (B) otherwise available resources, other than the Fund, are like-
2 ly insufficient to respond effectively to, or to mitigate effectively,
3 the specific significant incident described in subparagraph (A).

4 (2) PROHIBITION ON DELEGATION.—The Secretary may not delegate
5 the authority provided to the Secretary under paragraph (1).

6 (b) ASSET RESPONSE ACTIVITIES.—On a declaration, the Director shall
7 coordinate—

8 (1) the asset response activities of each Federal agency in response
9 to the specific significant incident associated with the declaration; and

10 (2) with appropriate entities, which may include—

11 (A) public and private entities and State and local governments
12 with respect to the asset response activities of those entities and
13 governments; and

14 (B) Federal, State, local, and Tribal law enforcement agencies
15 with respect to investigations and threat response activities of
16 those law enforcement agencies; and

17 (3) Federal, State, local, and Tribal emergency management and re-
18 sponse agencies.

19 (c) DURATION.—Subject to subsection (d), a declaration shall terminate
20 on the earlier of—

21 (1) a determination by the Secretary that the declaration is no
22 longer necessary; or

23 (2) the expiration of the 120-day period beginning on the date on
24 which the Secretary makes the declaration.

25 (d) RENEWAL.—The Secretary, without delegation, may renew a declara-
26 tion as necessary.

27 (e) PUBLICATION.—

28 (1) WHEN AND WHERE DECLARATION OR RENEWAL MUST BE PUB-
29 LISHED.—Not later than 72 hours after a declaration or a renewal, the
30 Secretary shall publish the declaration or renewal in the Federal Reg-
31 ister.

32 (2) WHAT MAY NOT BE INCLUDED.—A declaration or renewal pub-
33 lished under paragraph (1) may not include the name of any affected
34 individual or private company.

35 (f) ADVANCE ACTIONS.—

36 (1) IN GENERAL.—The Secretary—

37 (A) shall assess the resources available to respond to a potential
38 declaration; and

39 (B) may take actions before and while a declaration is in effect
40 to arrange or procure additional resources for asset response ac-
41 tivities or technical assistance the Secretary determines necessary,

1 which may include entering into standby contracts with private en-
2 tities for cybersecurity services or incident responders in the event
3 of a declaration.

4 (2) EXPENDITURE OF FUNDS.—An expenditure from the Fund for
5 the purpose of paragraph (1)(B) shall be made from amounts available
6 in the Fund. Amounts available in the Fund shall be in addition to any
7 other appropriations available to the Cybersecurity and Infrastructure
8 Security Agency for that purpose.

9 **§ 10743. Cyber Response and Recovery Fund**

10 (a) IN GENERAL.—There is a Cyber Response and Recovery Fund, which
11 shall be available for—

12 (1) the coordination of activities described in section 10742(b) of this
13 title;

14 (2) response and recovery support for the specific significant incident
15 associated with a declaration to Federal, State, local, and Tribal enti-
16 ties and public and private entities on a reimbursable or non-reimburs-
17 able basis, including through asset response activities and technical as-
18 sistance, such as—

19 (A) vulnerability assessments and mitigation;

20 (B) technical incident mitigation;

21 (C) malware analysis;

22 (D) analytic support;

23 (E) threat detection and hunting; and

24 (F) network protections;

25 (3) as the Director determines appropriate, grants for, or cooperative
26 agreements with, Federal, State, local, and Tribal entities and public
27 and private entities to respond to, and recover from, the specific signifi-
28 cant incident associated with a declaration, such as—

29 (A) hardware or software to replace, update, improve, harden,
30 or enhance the functionality of existing hardware, software, or sys-
31 tems; and

32 (B) technical contract personnel support; and

33 (4) advance actions taken by the Secretary under section
34 10742(f)(1)(B) of this title.

35 (b) DEPOSITS AND EXPENDITURES.—

36 (1) IN GENERAL.—Amounts shall be deposited in the Fund from—

37 (A) appropriations to the Fund for activities of the Fund; and

38 (B) reimbursement from Federal agencies for the activities de-
39 scribed in paragraphs (1), (2) and (4) of subsection (a), which
40 shall only be from amounts made available in advance in appro-
41 priations Acts for the reimbursement.

1 (2) EXPENDITURES.—An expenditure from the Fund for the pur-
2 poses of this subchapter shall be made from amounts available in the
3 Fund from a deposit described in paragraph (1). Amounts available in
4 the Fund shall be in addition to any other appropriations available to
5 the Cybersecurity and Infrastructure Security Agency for those pur-
6 poses.

7 (c) AMOUNTS SUPPLEMENT, NOT SUPPLANT, OTHER FUNDING.—
8 Amounts in the Fund shall be used to supplement, not supplant, other Fed-
9 eral, State, local, or Tribal funding for activities in response to a declara-
10 tion.

11 (d) REPORTING.—The Secretary shall require an entity that receives
12 amounts from the Fund to submit a report to the Secretary that details the
13 specific use of the amounts.

14 **§ 10744. Notification and reporting**

15 (a) NOTIFICATION.—On a declaration or renewal, the Secretary shall im-
16 mediately notify the National Cyber Director and appropriate congressional
17 committees and include in the notification—

18 (1) an estimation of the planned duration of the declaration;

19 (2) with respect to a notification of a declaration, the reason for the
20 declaration, including information relating to the specific significant in-
21 cident or imminent specific significant incident, including—

22 (A) the operational or mission impact or anticipated impact of
23 the specific significant incident on Federal and non-Federal enti-
24 ties;

25 (B) if known, the perpetrator of the specific significant incident;
26 and

27 (C) the scope of the Federal and non-Federal entities impacted
28 or anticipated to be impacted by the specific significant incident
29 malware analysis;

30 (3) with respect to a notification of a renewal, the reason for the re-
31 newal;

32 (4) justification as to why available resources, other than the Fund,
33 are insufficient to respond to or mitigate the specific significant inci-
34 dent; and

35 (5) a description of the coordination activities described in section
36 10742(b) of this title that the Secretary anticipates the Director will
37 perform.

38 (b) REPORT TO CONGRESS.—Not later than 180 days after the date of
39 a declaration or renewal, the Secretary shall submit to the appropriate con-
40 gressional committees a report that includes—

1 (1) the reason for the declaration or renewal, including information
2 and intelligence relating to the specific significant incident that led to
3 the declaration or renewal;

4 (2) the use of any funds from the Fund for the purpose of respond-
5 ing to the incident or threat described in paragraph (1);

6 (3) a description of the actions, initiatives, and projects undertaken
7 by the Department and State and local governments and public and
8 private entities in responding to and recovering from the specific sig-
9 nificant incident described in paragraph (1);

10 (4) an accounting of the specific obligations and outlays of the Fund;
11 and

12 (5) an analysis of—

13 (A) the impact of the specific significant incident described in
14 paragraph (1) on Federal and non-Federal entities;

15 (B) the impact of the declaration or renewal on the response to,
16 and recovery from, the specific significant incident described in
17 paragraph (1); and

18 (C) the impact of the funds made available from the Fund as
19 a result of the declaration or renewal on the recovery from, and
20 response to, the specific significant incident described in para-
21 graph (1).

22 (e) CLASSIFICATION.— Each notification made under subsection (a) and
23 each report submitted under subsection (b)—

24 (1) shall be in an unclassified form with appropriate markings to in-
25 dicate information that is exempt from disclosure under section 552 of
26 title 5 (known as the Freedom of Information Act); and

27 (2) may include a classified annex.

28 (d) CONSOLIDATED REPORT.—The Secretary shall not be required to
29 submit multiple reports under subsection (b) for multiple declarations or re-
30 newals if the Secretary determines that the declarations or renewals sub-
31 stantively relate to the same specific significant incident.

32 (e) EXEMPTION.—The requirements of subchapter I of chapter 35 of title
33 44 shall not apply to the voluntary collection of information by the Depart-
34 ment during an investigation of, a response to, or an immediate post-re-
35 sponse review of, the specific significant incident leading to a declaration or
36 renewal.

37 **§ 10745. Rule of construction**

38 Nothing in this subchapter shall be construed to impair or limit the abil-
39 ity of the Director to carry out the authorized activities of the Cybersecurity
40 and Infrastructure Security Agency.

1 **§ 10746. Authorization of appropriations**

2 There is authorized to be appropriated to the Fund \$20,000,000 for fiscal
3 year 2022 and each fiscal year thereafter until September 30, 2028, which
4 shall remain available until September 30, 2028.

5 **§ 10747. Sunset**

6 The authorities granted to the Secretary or the Director under this sub-
7 chapter shall expire on November 15, 2028.

8 **Subchapter IV—Cyber Incident Reporting**

9 **§ 10761. Definitions**

10 In this subchapter:

11 (1) CENTER.—The term “Center” means the center established
12 under section 10706 of this title.

13 (2) COUNCIL.—The term “Council” means the Cyber Incident Re-
14 porting Council described in section 10767 of this title.

15 (3) COVERED CYBER INCIDENT.—The term “covered cyber incident”
16 means a substantial cyber incident experienced by a covered entity that
17 satisfies the definition and criteria established by the Director in the
18 final rule issued pursuant to section 10763(b) of this title.

19 (4) COVERED ENTITY.—The term “covered entity” means an entity
20 in a critical infrastructure sector, as defined in Presidential Policy Di-
21 rective 21, that satisfies the definition established by the Director in
22 the final rule issued pursuant to section 10763(b) of this title.

23 (5) CYBER INCIDENT.—The term “cyber incident”—

24 (A) has the meaning given the term “incident” in section 10701
25 of this title; and

26 (B) does not include an occurrence that imminently, but not ac-
27 tually, jeopardizes—

28 (i) information on information systems; or

29 (ii) information systems.

30 (6) CYBER THREAT.—The term “cyber threat” has the meaning
31 given the term “cybersecurity threat” in section 10701 of this title.

32 (7) FEDERAL ENTITY.—The term “Federal entity” has the meaning
33 given the term in section 10781 of this title.

34 (8) RANSOM PAYMENT.—The term “ransom payment” means the
35 transmission of any money or other property or asset, including virtual
36 currency, or any portion thereof, which has at any time been delivered
37 as ransom in connection with a ransomware attack.

38 (9) SIGNIFICANT CYBER INCIDENT.—The term “significant cyber in-
39 cident” means a cyber incident, or a group of related cyber incidents,
40 that the Secretary determines is likely to result in demonstrable harm
41 to the national security interests, foreign relations, or economy of the

1 United States or to the public confidence, civil liberties, or public
2 health and safety of the people of the United States.

3 (10) VIRTUAL CURRENCY.—The term “virtual currency” means the
4 digital representation of value that functions as a medium of exchange,
5 a unit of account, or a store of value.

6 (11) VIRTUAL CURRENT ADDRESS.—The term “virtual currency ad-
7 dress” means a unique public cryptographic key identifying the location
8 to which a virtual currency payment can be made.

9 **§ 10762. Cyber incident review**

10 (a) CENTER ACTIVITIES.—The Center shall—

11 (1) receive, aggregate, analyze, and secure, using processes con-
12 sistent with the processes developed pursuant to subchapter V and sec-
13 tions 10801 through 10804 and 10821 of this title, reports from cov-
14 ered entities related to a covered cyber incident to assess the effective-
15 ness of security controls, to identify tactics, techniques, and procedures
16 adversaries use to overcome those controls, and for other cybersecurity
17 purposes, including to assess potential impact of cyber incidents on
18 public health and safety and to enhance situational awareness of cyber
19 threats across critical infrastructure sectors;

20 (2) coordinate and share information with appropriate Federal de-
21 partments and agencies to identify and track ransom payments, includ-
22 ing those utilizing virtual currencies;

23 (3) leverage information gathered about cyber incidents to—

24 (A) enhance the quality and effectiveness of information sharing
25 and coordination efforts with appropriate entities, including agen-
26 cies, sector coordinating councils, Information Sharing and Anal-
27 ysis Organizations, State, local, Tribal, and territorial govern-
28 ments, technology providers, critical infrastructure owners and op-
29 erators, cybersecurity and cyber incident response firms, and secu-
30 rity researchers; and

31 (B) provide appropriate entities, including sector coordinating
32 councils, Information Sharing and Analysis Organizations, State,
33 local, Tribal, and territorial governments, technology providers, cy-
34 bersecurity and cyber incident response firms, and security re-
35 searchers, with timely, actionable, and anonymized reports of
36 cyber incident campaigns and trends, including, to the maximum
37 extent practicable, related contextual information, cyber threat in-
38 dicators, and defensive measures, pursuant to section 10766 of this
39 title;

40 (4) establish mechanisms to receive feedback from stakeholders on
41 how the Agency can most effectively receive covered cyber incident re-

1 ports, ransom payment reports, and other voluntarily provided informa-
2 tion, and how the Agency can most effectively support private sector
3 cybersecurity;

4 (5) facilitate the timely sharing, on a voluntary basis, between rel-
5 evant critical infrastructure owners and operators of information relat-
6 ing to covered cyber incidents and ransom payments, particularly with
7 respect to ongoing cyber threats or security vulnerabilities, and identify
8 and disseminate ways to prevent or mitigate similar cyber incidents in
9 the future;

10 (6) for a covered cyber incident, including a ransomware attack, that
11 also satisfies the definition of a significant cyber incident, or is part
12 of a group of related cyber incidents that together satisfy that defini-
13 tion, conduct a review of the details surrounding the covered cyber inci-
14 dent or group of those incidents and identify and disseminate ways to
15 prevent or mitigate similar incidents in the future;

16 (7) with respect to covered cyber incident reports under
17 sections 10763(a) and 10764 of this title involving an ongoing cyber
18 threat or security vulnerability, immediately review those reports for
19 cyber threat indicators that can be anonymized and disseminated, with
20 defensive measures, to appropriate stakeholders, in coordination with
21 other divisions in the Agency, as appropriate;

22 (8) publish quarterly unclassified, public reports that describe aggre-
23 gated, anonymized observations, findings, and recommendations based
24 on covered cyber incident reports, which may be based on the unclassi-
25 fied information contained in the briefings required under subsection
26 (c);

27 (9) proactively identify opportunities, consistent with the protections
28 in section 10766 of this title, to leverage and utilize data on cyber inci-
29 dents in a manner that enables and strengthens cybersecurity research
30 carried out by academic institutions and other private sector organiza-
31 tions, to the greatest extent practicable; and

32 (10) in accordance with section 10766 of this title and subsection (b)
33 of this section, as soon as possible but not later than 24 hours after
34 receiving a covered cyber incident report, ransom payment report, vol-
35 untarily submitted information pursuant to section 10764 of this title,
36 or information received pursuant to a request for information or sub-
37 poena under section 10765 of this title, make available the information
38 to appropriate Sector Risk Management Agencies and other appro-
39 priate Federal agencies.

40 (b) INFORMATION SHARING.—The President or a designee of the Presi-
41 dent—

1 (1) may establish a specific time requirement for sharing information
2 under subsection (a)(10); and

3 (2) shall determine the appropriate Federal agencies under sub-
4 section (a)(10).

5 (c) PERIODIC BRIEFINGS.—Not later than 60 days after the effective
6 date of the final rule required undersection 10763(b) of this title, and on
7 the 1st day of each month thereafter, the Director, in consultation with the
8 National Cyber Director, the Attorney General, and the Director of National
9 Intelligence, shall provide to the majority leader of the Senate, the minority
10 leader of the Senate, the Speaker of the House of Representatives, the mi-
11 nority leader of the House of Representatives, the Committee on Homeland
12 Security and Governmental Affairs of the Senate, and the Committee on
13 Homeland Security of the House of Representatives a briefing that charac-
14 terizes the national cyber threat landscape, including the threat facing Fed-
15 eral agencies and covered entities, and applicable intelligence and law en-
16 forcement information, covered cyber incidents, and ransomware attacks, as
17 of the date of the briefing, which shall—

18 (1) include the total number of reports submitted undersections
19 10763 and 10764 of this titleduring the preceding month, including a
20 breakdown of required and voluntary reports;

21 (2) include any identified trends in covered cyber incidents and
22 ransomware attacks over the course of the preceding month and as
23 compared to previous reports, including any trends related to the infor-
24 mation collected in the reports submitted undersections 10763 and
25 10764 of this title, including—

26 (A) the infrastructure, tactics, and techniques malicious cyber
27 actors commonly use; and

28 (B) intelligence gaps that have impeded, or currently are imped-
29 ing, the ability to counter covered cyber incidents and ransomware
30 threats;

31 (3) include a summary of the known uses of the information in re-
32 ports submitted undersections 10763 and 10764 of this title; and

33 (4) include an unclassified portion, but may include a classified com-
34 ponent.

35 **§ 10763. Required reporting of certain cyber incidents**

36 (a) IN GENERAL.—

37 (1) Covered cyber incident reports.—

38 (A) IN GENERAL.—A covered entity that experiences a covered
39 cyber incident shall report the covered cyber incident to the Agen-
40 cy not later than 72 hours after the covered entity reasonably be-
41 lieves that the covered cyber incident has occurred.

1 (B) LIMITATION.—The Director may not require reporting
2 under subparagraph (A) any earlier than 72 hours after the covered
3 entity reasonably believes that a covered cyber incident has
4 occurred.

5 (2) RANSOM PAYMENT REPORTS.—

6 (A) IN GENERAL.—A covered entity that makes a ransom pay-
7 ment as the result of a ransomware attack against the covered en-
8 tity shall report the payment to the Agency not later than 24
9 hours after the ransom payment has been made.

10 (B) APPLICATION.—The requirements under subparagraph (A)
11 shall apply even if the ransomware attack is not a covered cyber
12 incident subject to the reporting requirements under paragraph
13 (1).

14 (3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly sub-
15 mit to the Agency an update or supplement to a previously submitted
16 covered cyber incident report if substantial new or different information
17 becomes available or if the covered entity makes a ransom payment
18 after submitting a covered cyber incident report required under para-
19 graph (1), until the date that the covered entity notifies the Agency
20 that the covered cyber incident at issue has concluded and has been
21 fully mitigated and resolved.

22 (4) PRESERVATION OF INFORMATION.—Any covered entity subject to
23 the requirements of paragraph (1), (2), or (3) shall preserve data rel-
24 evant to the covered cyber incident or ransom payment in accordance
25 with procedures established in the final rule issued pursuant to sub-
26 section (b).

27 (5) EXCEPTIONS.—

28 (A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM
29 PAYMENT.—If a covered entity is the victim of a covered cyber in-
30 cident and makes a ransom payment prior to the 72 hour require-
31 ment under paragraph (1), such that the reporting requirements
32 under paragraphs (1) and (2) both apply, the covered entity may
33 submit a single report to satisfy the requirements of both para-
34 graphs in accordance with procedures established in the final rule
35 issued pursuant to subsection (b).

36 (B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—

37 (i) IN GENERAL.—Subject to the limitation described in
38 clause (ii), where the Agency has an agreement in place that
39 satisfies the requirements of section 10768(b) of this title, the
40 requirements under paragraphs (1), (2), and (3) shall not
41 apply to a covered entity required by law, regulation, or con-

1 tract to report substantially similar information to another
2 Federal agency within a substantially similar timeframe.

3 (ii) LIMITATION.—The exemption in clause (i) shall take
4 effect with respect to a covered entity once an agency agree-
5 ment and sharing mechanism is in place between the Agency
6 and the respective Federal agency, pursuant to section
7 10768(b) of this title.

8 (iii) RULES OF CONSTRUCTION.—Nothing in this para-
9 graph shall be construed to—

10 (I) exempt a covered entity from the reporting require-
11 ments under paragraph (3) unless the supplemental re-
12 port also meets the requirements of clauses (i) and (ii)
13 of this subparagraph;

14 (II) prevent the Agency from contacting an entity sub-
15 mitting information to another Federal agency that is
16 provided to the Agency pursuant to section 10768 of this
17 title; or

18 (III) prevent an entity from communicating with the
19 Agency.

20 (C) DOMAIN NAME SYSTEM.—The requirements under para-
21 graphs (1), (2) and (3) shall not apply to a covered entity or the
22 functions of a covered entity that the Director determines con-
23 stitute critical infrastructure owned, operated, or governed by
24 multi-stakeholder organizations that develop, implement, and en-
25 force policies concerning the Domain Name System, such as the
26 Internet Corporation for Assigned Names and Numbers or the
27 Internet Assigned Numbers Authority.

28 (6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made
29 under paragraphs (1), (2), and (3) shall be made in the manner and
30 form, and within the time period in the case of reports made under
31 paragraph (3), prescribed in the final rule issued pursuant to sub-
32 section (b).

33 (7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect
34 on the dates prescribed in the final rule issued pursuant to subsection
35 (b).

36 (b) RULEMAKING.—

37 (1) NOTICE OF PROPOSED RULEMAKING.—Not later than March 15,
38 2024, the Director, in consultation with Sector Risk Management
39 Agencies, the Department of Justice, and other Federal agencies, shall
40 publish in the Federal Register a notice of proposed rulemaking to im-
41 plement subsection (a).

1 (2) FINAL RULE.—Not later than 18 months after publication of the
2 notice of proposed rulemaking under paragraph (1), the Director shall
3 issue a final rule to implement subsection (a).

4 (3) SUBSEQUENT RULEMAKINGS.—

5 (A) IN GENERAL.—The Director may issue regulations to
6 amend or revise the final rule issued pursuant to paragraph (2).

7 (B) PROCEDURES.—Any subsequent rules issued under sub-
8 paragraph (A) shall comply with the requirements underchapter 5
9 of title 5, including the issuance of a notice of proposed rule-
10 making under section 553 of title 5.

11 (c) ELEMENTS.—The final rule issued pursuant to subsection (b) shall be
12 composed of the following elements:

13 (1) A clear description of the types of entities that constitute covered
14 entities, based on—

15 (A) the consequences that disruption to or compromise of such
16 an entity could cause to national security, economic security, or
17 public health and safety;

18 (B) the likelihood that such an entity may be targeted by a ma-
19 licious cyber actor, including a foreign country; and

20 (C) the extent to which damage, disruption, or unauthorized ac-
21 cess to such an entity, including the accessing of sensitive cyberse-
22 curity vulnerability information or penetration testing tools or
23 techniques, will likely enable the disruption of the reliable oper-
24 ation of critical infrastructure.

25 (2) A clear description of the types of substantial cyber incidents
26 that constitute covered cyber incidents, which shall—

27 (A) at a minimum, require the occurrence of—

28 (i) a cyber incident that leads to substantial loss of con-
29 fidentiality, integrity, or availability of the information system
30 or network, or a serious impact on the safety and resiliency
31 of operational systems and processes;

32 (ii) a disruption of business or industrial operations, in-
33 cluding due to a denial of service attack, ransomware attack,
34 or exploitation of a zero day vulnerability, against—

35 (I) an information system or network; or

36 (II) an operational technology system or process; or

37 (iii) unauthorized access or disruption of business or indus-
38 trial operations due to loss of service facilitated through, or
39 caused by, a compromise of a cloud service provider, managed
40 service provider, or other third-party data hosting provider or
41 by a supply chain compromise;

1 (B) consider—

2 (i) the sophistication or novelty of the tactics used to per-
3 petrate the cyber incident, as well as the type, volume, and
4 sensitivity of the data at issue;

5 (ii) the number of individuals directly or indirectly affected
6 or potentially affected by the cyber incident; and

7 (iii) potential impacts on industrial control systems, such
8 as supervisory control and data acquisition systems, distrib-
9 uted control systems, and programmable logic controllers; and

10 (C) exclude—

11 (i) any event where the cyber incident is perpetrated in
12 good faith by an entity in response to a specific request by
13 the owner or operator of the information system; and

14 (ii) the threat of disruption as extortion, as described
15 in section 10701 of this title.

16 (3) A requirement that, if a covered cyber incident or a ransom pay-
17 ment occurs following an exempted threat described in paragraph
18 (2)(C)(ii), the covered entity shall comply with the requirements in this
19 subchapter in reporting the covered cyber incident or ransom payment.

20 (4) A clear description of the specific required contents of a report
21 pursuant to subsection (a)(1), which shall include the following infor-
22 mation, to the extent applicable and available, with respect to a covered
23 cyber incident:

24 (A) A description of the covered cyber incident, including—

25 (i) identification and a description of the function of the af-
26 fected information systems, networks, or devices that were, or
27 are reasonably believed to have been, affected by the cyber in-
28 cident;

29 (ii) a description of the unauthorized access with substan-
30 tial loss of confidentiality, integrity, or availability of the af-
31 fected information system or network or disruption of busi-
32 ness or industrial operations;

33 (iii) the estimated date range of the incident; and

34 (iv) the impact to the operations of the covered entity.

35 (B) Where applicable, a description of the vulnerabilities ex-
36 ploited and the security defenses that were in place, as well as the
37 tactics, techniques, and procedures used to perpetrate the covered
38 cyber incident.

39 (C) Where applicable, any identifying or contact information re-
40 lated to each actor reasonably believed to be responsible for the
41 cyber incident.

1 (D) Where applicable, identification of the category or cat-
2 egories of information that were, or are reasonably believed to
3 have been, accessed or acquired by an unauthorized person.

4 (E) The name and other information that clearly identifies the
5 covered entity impacted by the covered cyber incident, including,
6 as applicable, the State of incorporation or formation of the cov-
7 ered entity, trade names, legal names, or other identifiers.

8 (F) Contact information, such as telephone number or electronic
9 mail address, that the Agency may use to contact the covered enti-
10 ty or an authorized agent of the covered entity, or, where applica-
11 ble, the service provider of the covered entity acting with the ex-
12 press permission of, and at the direction of, the covered entity to
13 assist with compliance with the requirements of this subchapter.

14 (5) A clear description of the specific required contents of a report
15 pursuant to subsection (a)(2), which shall be the following information,
16 to the extent applicable and available, with respect to a ransom pay-
17 ment:

18 (A) A description of the ransomware attack, including the esti-
19 mated date range of the attack.

20 (B) Where applicable, a description of the vulnerabilities, tac-
21 tics, techniques, and procedures used to perpetrate the
22 ransomware attack.

23 (C) Where applicable, any identifying or contact information re-
24 lated to the actor or actors reasonably believed to be responsible
25 for the ransomware attack.

26 (D) The name and other information that clearly identifies the
27 covered entity that made the ransom payment or on whose behalf
28 the payment was made.

29 (E) Contact information, such as telephone number or electronic
30 mail address, that the Agency may use to contact the covered enti-
31 ty that made the ransom payment or an authorized agent of the
32 covered entity, or, where applicable, the service provider of the
33 covered entity acting with the express permission of, and at the
34 direction of, the covered entity to assist with compliance with the
35 requirements of this subchapter.

36 (F) The date of the ransom payment.

37 (G) The ransom payment demand, including the type of virtual
38 currency or other commodity requested, if applicable.

39 (H) The ransom payment instructions, including information re-
40 garding where to send the payment, such as the virtual currency

1 address or physical address the funds were requested to be sent
2 to, if applicable.

3 (I) The amount of the ransom payment.

4 (6) A clear description of the types of data required to be preserved
5 pursuant to subsection (a)(4), the period of time for which the data
6 is required to be preserved, and allowable uses, processes, and proce-
7 dures.

8 (7) Deadlines and criteria for submitting supplemental reports to the
9 Agency required under subsection (a)(3), which shall—

10 (A) be established by the Director in consultation with the
11 Council;

12 (B) consider any existing regulatory reporting requirements
13 similar in scope, purpose, and timing to the reporting require-
14 ments to which the covered entity may also be subject, and make
15 efforts to harmonize the timing and contents of the reports to the
16 maximum extent practicable;

17 (C) balance the need for situational awareness with the ability
18 of the covered entity to conduct cyber incident response and inves-
19 tigation; and

20 (D) provide a clear description of what constitutes substantial
21 new or different information.

22 (8) Procedures for—

23 (A) entities, including third parties pursuant to subsection
24 (d)(1), to submit reports required by paragraphs (1), (2), and (3)
25 of subsection (a), including the manner and form of the reports,
26 which shall include, at a minimum, a concise, user-friendly web-
27 based form;

28 (B) the Agency to carry out—

29 (i) the enforcement provisions of section 10765 of this title,
30 including with respect to the issuance, service, withdrawal, re-
31 ferral process, and enforcement of subpoenas, appeals, and
32 due process procedures;

33 (ii) other available enforcement mechanisms, including ac-
34 quisition, suspension, and debarment procedures; and

35 (iii) other aspects of noncompliance;

36 (C) implementing the exceptions provided in subsection (a)(5);
37 and

38 (D) protecting privacy and civil liberties consistent with proce-
39 sses adopted pursuant to section 10784(e) of this title and
40 anonymizing and safeguarding, or no longer retaining, information
41 received and disclosed through covered cyber incident reports and

1 ransom payment reports that is known to be personal information
2 of a specific individual or information that identifies a specific in-
3 dividual that is not directly related to a cybersecurity threat.

4 (9) Other procedural measures directly necessary to implement sub-
5 section (a).

6 (d) THIRD PARTY REPORT SUBMISSION AND RANSOM PAYMENT.—

7 (1) REPORT SUBMISSION.—A covered entity that is required to sub-
8 mit a covered cyber incident report or a ransom payment report may
9 use a third party, such as an incident response company, insurance
10 provider, service provider, Information Sharing and Analysis Organiza-
11 tion, or law firm, to submit the required report under subsection (a).

12 (2) RANSOM PAYMENT.—If a covered entity impacted by a
13 ransomware attack uses a third party to make a ransom payment, the
14 third party shall not be required to submit a ransom payment report
15 for itself under subsection (a)(2).

16 (3) DUTY TO REPORT.—Third-party reporting under this subpara-
17 graph does not relieve a covered entity from the duty to comply with
18 the requirements for covered cyber incident report or ransom payment
19 report submission.

20 (4) RESPONSIBILITY TO ADVISE.—Any third party used by a covered
21 entity that knowingly makes a ransom payment on behalf of a covered
22 entity impacted by a ransomware attack shall advise the impacted cov-
23 ered entity of the responsibilities of the impacted covered entity regard-
24 ing reporting ransom payments under this section.

25 (e) OUTREACH TO COVERED ENTITIES.—

26 (1) IN GENERAL.—The Agency shall conduct an outreach and edu-
27 cation campaign to inform likely covered entities, entities that offer or
28 advertise as a service to customers to make or facilitate ransom pay-
29 ments on behalf of covered entities impacted by ransomware attacks,
30 and other appropriate entities of the requirements of paragraphs (1),
31 (2), and (3) of subsection (a).

32 (2) ELEMENTS.—The outreach and education campaign under para-
33 graph (1) shall include the following:

34 (A) An overview of the final rule issued pursuant to subsection
35 (b).

36 (B) An overview of mechanisms to submit to the Agency covered
37 cyber incident reports, ransom payment reports, and information
38 relating to the disclosure, retention, and use of covered cyber inci-
39 dent reports and ransom payment reports under this section.

1 (C) An overview of the protections afforded to covered entities
2 for complying with the requirements under paragraphs (1), (2),
3 and (3) of subsection (a).

4 (D) An overview of the steps taken undersection 10765 of this
5 titlewhen a covered entity is not in compliance with the reporting
6 requirements under subsection (a).

7 (E) Specific outreach to cybersecurity vendors, cyber incident
8 response providers, cybersecurity insurance entities, and other en-
9 tities that may support covered entities.

10 (F) An overview of the privacy and civil liberties requirements
11 in this subchapter.

12 (3) COORDINATION.—In conducting the outreach and education cam-
13 paign required under paragraph (1), the Agency may coordinate with—

14 (A) the Critical Infrastructure Partnership Advisory Council es-
15 tablished undersection 10391 of this title;

16 (B) Information Sharing and Analysis Organizations;

17 (C) trade associations;

18 (D) information sharing and analysis centers;

19 (E) sector coordinating councils; and

20 (F) any other entity as determined appropriate by the Director.

21 (f) EXEMPTION.—Sections 3506(e), 3507, 3508, and 3509 of title 44shall
22 not apply to any action to carry out this section.

23 (g) RULE OF CONSTRUCTION.—Nothing in this section shall affect the au-
24 thorities of the Federal Government to implement the requirements of Exec-
25 utive Order 14028 (86 Fed. Reg. 26633), including changes to the Federal
26 Acquisition Regulations and remedies to include suspension and debarment.

27 (h) SAVINGS PROVISION.—Nothing in this section shall be construed to
28 supersede or to abrogate, modify, or otherwise limit the authority that is
29 vested in any officer or any agency of the United States Government to reg-
30 ulate or take action with respect to the cybersecurity of an entity.

31 **§ 10764. Voluntary reporting of other cyber incidents**

32 (a) IN GENERAL.—Entities may voluntarily report cyber incidents or ran-
33 som payments to the Agency that are not required under paragraph (1),
34 (2), or (3) ofsection 10763(a) of this title, but may enhance the situational
35 awareness of cyber threats.

36 (b) VOLUNTARY PROVISION OF ADDITIONAL INFORMATION IN REQUIRED
37 REPORTS.—Covered entities may voluntarily include in reports required
38 under paragraph (1), (2), or (3) ofsection 10763(a) of this titleinformation
39 that is not required to be included but may enhance the situational aware-
40 ness of cyber threats.

1 (c) APPLICATION OF SECTION 10766.—Section 10766 of this title shall
2 apply in the same manner and to the same extent to reports and informa-
3 tion submitted under subsections (a) and (b) as it applies to reports and
4 information submitted under section 10763 of this title.

5 **§ 10765. Noncompliance with required reporting**

6 (a) PURPOSE.—In the event that a covered entity that is required to sub-
7 mit a report under section 10763(a) of this title fails to comply with the re-
8 quirement to report, the Director may obtain information about the cyber
9 incident or ransom payment by engaging the covered entity directly to re-
10 quest information about the cyber incident or ransom payment, and if the
11 Director is unable to obtain information through the engagement, by issuing
12 a subpoena to the covered entity, pursuant to subsection (c), to gather infor-
13 mation sufficient to determine whether a covered cyber incident or ransom
14 payment has occurred.

15 (b) INITIAL REQUEST FOR INFORMATION.—

16 (1) IN GENERAL.—If the Director has reason to believe, whether
17 through public reporting or other information in the possession of the
18 Federal Government, including through analysis performed pursuant to
19 paragraph (1) or (2) of section 10762(a) of this title, that a covered en-
20 tity has experienced a covered cyber incident or made a ransom pay-
21 ment but failed to report the cyber incident or payment to the Agency
22 in accordance with section 10763(a) of this title, the Director may re-
23 quest additional information from the covered entity to confirm wheth-
24 er or not a covered cyber incident or ransom payment has occurred.

25 (2) TREATMENT.—Information provided to the Agency in response
26 to a request under paragraph (1) shall be treated as if it was submitted
27 through the reporting procedures established in section 10763 of this
28 title including that section 10766 of this title shall apply to the infor-
29 mation in the same manner and to the same extent to information sub-
30 mitted in response to requests under paragraph (1) as it applies to in-
31 formation submitted under section 10763 of this title.

32 (c) ENFORCEMENT.—

33 (1) IN GENERAL.—If, after the date that is 72 hours from the date
34 on which the Director made the request for information in subsection
35 (b), the Director has received no response from the covered entity from
36 which the information was requested, or received an inadequate re-
37 sponse, the Director may—

38 (A) issue—

39 (i) to the covered entity a subpoena to compel disclosure
40 of information the Director considers necessary to determine
41 whether a covered cyber incident or ransom payment has oc-

1 curred and obtain the information required to be reported
2 pursuant to section 10763 of this title; and

3 (ii) any implementing regulations; and

4 (B) assess potential impacts to national security, economic secu-
5 rity, or public health and safety.

6 (2) CIVIL ACTION.—

7 (A) IN GENERAL.—If a covered entity fails to comply with a
8 subpoena, the Director may refer the matter to the Attorney Gen-
9 eral to bring a civil action in a district court of the United States
10 to enforce the subpoena.

11 (B) VENUE.—An action under this paragraph may be brought
12 in the judicial district in which the covered entity against which
13 the action is brought resides, is found, or does business.

14 (C) CONTEMPT OF COURT.—A court may punish a failure to
15 comply with a subpoena issued under this subsection as contempt
16 of court.

17 (3) NON-DELEGATION.—The authority of the Director to issue a
18 subpoena under this subsection may not be delegated.

19 (4) AUTHENTICATION.—

20 (A) IN GENERAL.—Any subpoena issued electronically pursuant
21 to this subsection shall be authenticated with a cryptographic dig-
22 ital signature of an authorized representative of the Agency, or
23 other comparable successor technology, that allows the Agency to
24 demonstrate that the subpoena was issued by the Agency and has
25 not been altered or modified since issuance.

26 (B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued
27 electronically pursuant to this subsection that is not authenticated
28 in accordance with subparagraph (A) shall not be considered to be
29 valid by the recipient of the subpoena.

30 (d) PROVISION OF CERTAIN INFORMATION TO ATTORNEY GENERAL.—

31 (1) IN GENERAL.—Notwithstanding paragraph (b)(2) and section
32 10766(a)(5) of this title, if the Director determines, based on the infor-
33 mation provided in response to a subpoena issued pursuant to sub-
34 section (c), that the facts relating to the cyber incident or ransom pay-
35 ment at issue may constitute grounds for a regulatory enforcement ac-
36 tion or criminal prosecution, the Director may provide the information
37 to the Attorney General or the head of the appropriate Federal regu-
38 latory agency, who may use the information for a regulatory enforce-
39 ment action or criminal prosecution.

1 (2) CONSULTATION.—The Director may consult with the Attorney
2 General or the head of the appropriate Federal regulatory agency when
3 making the determination under paragraph (1).

4 (e) CONSIDERATIONS.—When determining whether to exercise the au-
5 thorities provided under this section, the Director shall take into consider-
6 ation—

7 (1) the complexity in determining if a covered cyber incident has oc-
8 curred; and

9 (2) prior interaction with the Agency or awareness of the covered en-
10 tity of the policies and procedures of the Agency for reporting covered
11 cyber incidents and ransom payments.

12 (f) EXCLUSIONS.—This section shall not apply to a State, local, Tribal,
13 or territorial government entity.

14 (g) REPORT TO CONGRESS.—The Director shall submit to Congress an
15 annual report on the number of times the Director—

16 (1) issued an initial request for information pursuant to subsection
17 (b);

18 (2) issued a subpoena pursuant to subsection (c); or

19 (3) referred a matter to the Attorney General for a civil action pur-
20 suant to subsection (c)(2).

21 (h) PUBLICATION OF ANNUAL REPORT.—The Director shall publish a
22 version of the annual report required under subsection (g) on the website
23 of the Agency, which shall include, at a minimum, the number of times the
24 Director—

25 (1) issued an initial request for information pursuant to subsection
26 (b); or

27 (2) issued a subpoena pursuant to subsection (c).

28 (i) ANONYMIZATION OF REPORTS.—The Director shall ensure any victim
29 information contained in a report required to be published under subsection
30 (h) be anonymized before the report is published.

31 **§ 10766. Information shared with or provided to the Federal**
32 **Government**

33 (a) DISCLOSURE, RETENTION, AND USE.—

34 (1) AUTHORIZED ACTIVITIES.—Information provided to the Agency
35 pursuant to section 10763 or 10764 of this title may be disclosed to, re-
36 tained by, and used by, consistent with otherwise applicable provisions
37 of Federal law, any Federal agency or department, component, officer,
38 employee, or agent of the Federal Government solely for—

39 (A) a cybersecurity purpose;

40 (B) the purpose of identifying—

1 (i) a cyber threat, including the source of the cyber threat;

2 or

3 (ii) a security vulnerability;

4 (C) the purpose of responding to, or otherwise preventing or
5 mitigating, a specific threat of death, a specific threat of serious
6 bodily harm, or a specific threat of serious economic harm, includ-
7 ing a terrorist act or use of a weapon of mass destruction;

8 (D) the purpose of responding to, investigating, prosecuting, or
9 otherwise preventing or mitigating, a serious threat to a minor, in-
10 cluding sexual exploitation and threats to physical safety; or

11 (E) the purpose of preventing, investigating, disrupting, or pros-
12 ecuting an offense arising out of a cyber incident reported pursu-
13 ant to section 10763 or 10764 of this title or any of the offenses
14 listed in section 10784(e)(5)(A)(v) of this title.

15 (2) AGENCY ACTIONS AFTER RECEIPT.—

16 (A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICA-
17 TORS.—On receiving a covered cyber incident or ransom payment
18 report submitted pursuant to this section, the Agency shall imme-
19 diately review the report to determine whether the cyber incident
20 that is the subject of the report is connected to an ongoing cyber
21 threat or security vulnerability and where applicable, use the re-
22 port to identify, develop, and rapidly disseminate to appropriate
23 stakeholders actionable, anonymized cyber threat indicators and
24 defensive measures.

25 (B) PRINCIPLES FOR SHARING SECURITY VULNERABILITIES.—
26 With respect to information in a covered cyber incident or ransom
27 payment report regarding a security vulnerability referred to in
28 paragraph (1)(B)(ii), the Director shall develop principles that
29 govern the timing and manner in which information relating to se-
30 curity vulnerabilities may be shared, consistent with common in-
31 dustry best practices and United States and international stand-
32 ards.

33 (3) PRIVACY AND CIVIL LIBERTIES.—Information contained in cov-
34 ered cyber incident and ransom payment reports submitted to the
35 Agency pursuant to section 10763 of this title shall be retained, used,
36 and disseminated, where permissible and appropriate, by the Federal
37 Government in accordance with processes to be developed for the pro-
38 tection of personal information consistent with processes adopted pur-
39 suant to section 10784 of this title and in a manner that protects per-
40 sonal information from unauthorized use or unauthorized disclosure.

1 (4) DIGITAL SECURITY.—The Agency shall ensure that reports sub-
2 mitted to the Agency pursuant to section 10763 of this title, and any
3 information contained in those reports, are collected, stored, and pro-
4 tected at a minimum in accordance with the requirements for moderate
5 impact Federal information systems, as described in Federal Informa-
6 tion Processing Standards Publication 199, or any successor document.

7 (5) PROHIBITION ON USE OF INFORMATION IN REGULATORY AC-
8 TIONS.—

9 (A) IN GENERAL.—A Federal, State, local, or Tribal govern-
10 ment shall not use information about a covered cyber incident or
11 ransom payment obtained solely through reporting directly to the
12 Agency in accordance with this subchapter to regulate, including
13 through an enforcement action, the activities of the covered entity
14 or entity that made a ransom payment unless the government en-
15 tity expressly allows entities to submit reports to the Agency to
16 meet regulatory reporting obligations of the entity.

17 (B) ALLOWANCE FOR REGULATIONS.—A report submitted to
18 the Agency pursuant to section 10763 or 10764 of this title may,
19 consistent with Federal or State regulatory authority specifically
20 relating to the prevention and mitigation of cybersecurity threats
21 to information systems, inform the development or implementation
22 of regulations relating to those systems.

23 (b) PROTECTIONS FOR REPORTING ENTITIES AND INFORMATION.—Re-
24 ports describing covered cyber incidents or ransom payments submitted to
25 the Agency by entities in accordance with section 10763 of this title, as well
26 as voluntarily-submitted cyber incident reports submitted to the Agency pur-
27 suant to section 10764 of this title, shall—

28 (1) be considered the commercial, financial, and proprietary informa-
29 tion of the covered entity when so designated by the covered entity;

30 (2) be exempt from disclosure under section 552(b)(3) of title 5, as
31 well as any provision of State, Tribal, or local freedom of information
32 law, open government law, open meetings law, open records law, sun-
33 shine law, or similar law requiring disclosure of information or records;

34 (3) be considered not to constitute a waiver of any applicable privi-
35 lege or protection provided by law, including trade secret protection;
36 and

37 (4) not be subject to a rule of any Federal agency or department
38 or any judicial doctrine regarding ex parte communications with a deci-
39 sion-making official.

40 (c) LIABILITY PROTECTIONS.—

1 (1) IN GENERAL.—No cause of action for the submission of a report
2 pursuant to section 10763(a) of this title that is submitted in conform-
3 ance with this subchapter and the rule promulgated under section
4 10763(b) of this title shall lie or be maintained in any court by any
5 person or entity and the action shall be promptly dismissed, except that
6 this subsection shall not apply with regard to an action by the Federal
7 Government pursuant to section 10765(c)(2) of this title.

8 (2) SCOPE.—The liability protections provided in this subsection
9 shall only apply to or affect litigation that is solely based on the sub-
10 mission of a covered cyber incident report or ransom payment report
11 to the Agency.

12 (3) RESTRICTIONS.—Notwithstanding paragraph (2), no report sub-
13 mitted to the Agency pursuant to this subchapter or any communica-
14 tion, document, material, or other record, created for the sole purpose
15 of preparing, drafting, or submitting the report, may be received in evi-
16 dence, subject to discovery, or otherwise used in any trial, hearing, or
17 other proceeding in or before any court, regulatory body, or other au-
18 thority of the United States, a State, or a political subdivision of a
19 State, provided that nothing in this subchapter shall create a defense
20 to discovery or otherwise affect the discovery of any communication,
21 document, material, or other record not created for the sole purpose
22 of preparing, drafting, or submitting the report.

23 (d) SHARING WITH NON-FEDERAL ENTITIES.—The Agency shall
24 anonymize the victim who reported the information when making informa-
25 tion provided in reports received under section 10763 of this title available to
26 critical infrastructure owners and operators and the general public.

27 (e) RELATIONSHIP TO CHAPTER 121 OF TITLE 18.—Nothing in this sub-
28 chapter shall be construed to permit or require disclosure by a provider of
29 a remote computing service or a provider of an electronic communication
30 service to the public of information not otherwise permitted or required to
31 be disclosed under chapter 121 of title 18.

32 **§ 10767. Cyber Incident Reporting Council**

33 (a) RESPONSIBILITY OF THE SECRETARY.—The Secretary shall lead an
34 intergovernmental Cyber Incident Reporting Council, in consultation with
35 the Director of the Office of Management and Budget, the Attorney Gen-
36 eral, the National Cyber Director, Sector Risk Management Agencies, and
37 other appropriate Federal agencies, to coordinate, deconflict, and harmonize
38 Federal incident reporting requirements, including those issued through reg-
39 ulations.

40 (b) RULE OF CONSTRUCTION.—Nothing in subsection (a) shall be con-
41 strued to provide any additional regulatory authority to any Federal entity.

1 **§ 10768. Federal sharing of incident reports**

2 (a) DEFINITIONS.—In this section:

3 (1) SECTION 10701 DEFINITIONS.—The terms “Agency”, “Direc-
4 tor”, “information system”, “ransomware attack”, and “security vul-
5 nerability” have the meanings given those terms in section 10701 of
6 this title.

7 (2) SECTION 10761 DEFINITIONS.—The terms “covered cyber inci-
8 dent”, “covered entity”, “cyber incident”, and “ransom payment” have
9 the meanings given those terms in section 10761 of this title.

10 (b) CYBER INCIDENT REPORTING SHARING

11 (1) IN GENERAL.—Notwithstanding any other provision of law or
12 regulation, any Federal agency, including any independent establish-
13 ment (as defined in section 104 of title 5), that receives a report from
14 an entity of a cyber incident, including a ransomware attack, shall pro-
15 vide the report to the Agency as soon as possible, but not later than
16 24 hours after receiving the report, unless a shorter period is required
17 by an agreement made between the Department (including the Agency)
18 and the recipient Federal agency. The Director shall share and coordi-
19 nate each report pursuant to section 10762(b) of this title.

20 (2) RULE OF CONSTRUCTION.—The requirements described in para-
21 graph (1) and section 10766(d) of this title may not be construed to
22 be a violation of any provision of law or policy that would otherwise
23 prohibit disclosure or provision of information within the executive
24 branch.

25 (3) PROTECTION OF INFORMATION.—The Director shall comply with
26 any obligations of the recipient Federal agency described in paragraph
27 (1) to protect information, including with respect to privacy, confiden-
28 tiality, or information security, if those obligations would impose great-
29 er protection requirements than this subchapter or the amendments
30 made by the Cyber Incident Reporting for Critical Infrastructure Act of
31 2022 (Public Law 117–103, div. Y, 136 Stat. 1038).

32 (4) EFFECTIVE DATE.—This subsection shall take effect on the ef-
33 fective date of the final rule issued pursuant to section 10763(b) of this
34 title.

35 (5) AGENCY AGREEMENTS.—

36 (A) IN GENERAL.—The Agency and any Federal agency, includ-
37 ing any independent establishment (as defined in section 104 of
38 title 5), that receives incident reports from entities, including due
39 to ransomware attacks, shall, as appropriate, enter into a docu-
40 mented agreement to establish policies, processes, procedures, and

1 mechanisms to ensure reports are shared with the Agency pursu-
2 ant to paragraph (1).

3 (B) AVAILABILITY.—To the maximum extent practicable, each
4 documented agreement required under subparagraph (A) shall be
5 made publicly available.

6 (C) REQUIREMENT.—The documented agreements required by
7 subparagraph (A) shall require reports be shared from Federal
8 agencies with the Agency in such time as to meet the overall
9 timeline for covered entity reporting of covered cyber incidents and
10 ransom payments established in section 10763 of this title.

11 (e) HARMONIZING REPORTING REQUIREMENTS.—The Secretary, acting
12 through the Director, shall, in consultation with the Cyber Incident Report-
13 ing Council described in section 10767 of this title, to the maximum extent
14 practicable—

15 (1) periodically review existing regulatory requirements, including the
16 information required in the reports, to report incidents and ensure that
17 any reporting requirements and procedures avoid conflicting, duplica-
18 tive, or burdensome requirements; and

19 (2) coordinate with appropriate Federal partners and regulatory au-
20 thorities that receive reports relating to incidents to identify opportuni-
21 ties to streamline reporting processes, and where feasible, facilitate
22 interagency agreements between the authorities to permit the sharing
23 of the reports, consistent with applicable law and policy, without im-
24 pacting the ability of the Agency to gain timely situational awareness
25 of a covered cyber incident or ransom payment.

26 **Subchapter V—Cybersecurity Information** 27 **Sharing**

28 **§ 10781. Definitions**

29 In this subchapter:

30 (1) AGENCY.—The term “agency” has the meaning given the term
31 in section 3502 of title 44.

32 (2) ANTITRUST LAWS.—The term “antitrust laws”—

33 (A) has the meaning given the term in the 1st section of the
34 Clayton Act (15 U.S.C. 12);

35 (B) includes section 5 of the Federal Trade Commission Act (15
36 U.S.C. 45) to the extent that section 5 of that Act applies to un-
37 fair competition; and

38 (C) includes any State antitrust law, but only to the extent that
39 the law is consistent with the law referred to in subparagraph (A)
40 or (B).

1 (3) APPROPRIATE FEDERAL ENTITIES.—The term “appropriate fed-
2 eral entities” means the following:

- 3 (A) The Department of Commerce.
4 (B) The Department of Defense.
5 (C) The Department of Energy.
6 (D) The Department of Homeland Security.
7 (E) The Department of Justice.
8 (F) The Department of the Treasury.

9 (4) CYBER THREAT INDICATOR.—The term “cyber threat indicator”
10 has the meaning given the term in section 10701 of this title.

11 (5) CYBERSECURITY PURPOSE.—The term “cybersecurity purpose”
12 has the meaning given the term in section 10701 of this title.

13 (6) CYBERSECURITY THREAT.—The term “cybersecurity threat” has
14 the meaning given the term in section 10701 of this title.

15 (7) DEFENSIVE MEASURE.—The term “defensive measure” has the
16 meaning given the term in section 10701 of this title.

17 (8) FEDERAL ENTITY.—The term “Federal entity” means a depart-
18 ment or agency of the United States or any component of the depart-
19 ment or agency.

20 (9) INFORMATION SYSTEM.—The term “information system” has the
21 meaning given the term in section 10701 of this title.

22 (10) LOCAL GOVERNMENT.—The term “local government” means
23 any borough, city, county, parish, town, township, village or other polit-
24 ical subdivision of a State.

25 (11) MALICIOUS CYBER COMMAND AND CONTROL.—The term “mali-
26 cious cyber command and control” has the meaning given the term in
27 section 10701 of this title.

28 (12) MALICIOUS RECONNAISSANCE.—The term “malicious reconnais-
29 sance” has the meaning given the term in section 10701 of this title.

30 (13) MONITOR.—The term “monitor” has the meaning given the
31 term in section 10701 of this title.

32 (14) NON-FEDERAL ENTITY.—

33 (A) IN GENERAL.—Except as provided in this paragraph, the
34 term “non-Federal entity” means any private entity, non-Federal
35 Government agency or department, or State, tribal, or local gov-
36 ernment (including a political subdivision, department, or compo-
37 nent of the government).

38 (B) INCLUSIONS.—The term “non-Federal entity” includes a
39 government agency or department of the District of Columbia,
40 Puerto Rico, the Virgin Islands, Guam, American Samoa, the

1 Northern Mariana Islands, and any other territory or possession
2 of the United States.

3 (C) EXCLUSIONS.—The term “non-Federal entity” does not in-
4 clude a foreign power as defined in section 101 of the Foreign In-
5 telligence Surveillance Act of 1978 (50 U.S.C. 1801).

6 (15) PRIVATE ENTITY.—

7 (A) IN GENERAL.—Except as provided in this paragraph, the
8 term “private entity” means any person or private group, organi-
9 zation, proprietorship, partnership, trust, cooperative organization,
10 or other commercial or nonprofit entity, including an officer, em-
11 ployee, or agent.

12 (B) INCLUSION.—The term “private entity” includes a State,
13 tribal, or local government performing utility services, such as
14 electric, natural gas, or water services.

15 (C) EXCLUSION.—The term “private entity” does not include a
16 foreign power as defined in section 101 of the Foreign Intelligence
17 Surveillance Act of 1978 (50 U.S.C. 1801).

18 (16) SECURITY CONTROL.—The term “security control” has the
19 meaning given the term in section 10701 of this title.

20 (17) SECURITY VULNERABILITY.—The term “security vulnerability”
21 has the meaning given the term in section 10701 of this title.

22 (18) TRIBAL.—The term “tribal” has the meaning given the term
23 “Indian tribe” in section 4 of the Indian Self-Determination and Edu-
24 cation Assistance Act (25 U.S.C. 5304).

25 **§ 10782. Procedures for sharing information by Federal Gov-**
26 **ernment**

27 (a) IN GENERAL.—Consistent with the protection of classified informa-
28 tion, intelligence sources and methods, and privacy and civil liberties, the
29 Director of National Intelligence, the Secretary, the Secretary of Defense,
30 and the Attorney General, in consultation with the heads of the appropriate
31 Federal entities, shall jointly develop and issue procedures to facilitate and
32 promote—

33 (1) timely sharing of classified cyber threat indicators and defensive
34 measures the Federal Government possesses with representatives of rel-
35 evant Federal entities and non-Federal entities that have appropriate
36 security clearances;

37 (2) timely sharing with relevant Federal entities and non-Federal en-
38 tities of cyber threat indicators, defensive measures, and information
39 relating to cybersecurity threats or authorized uses under this sub-
40 chapter, in the possession of the Federal Government, that may be de-
41 classified and shared at an unclassified level;

1 (3) timely sharing with relevant Federal entities and non-Federal en-
2 tities, or the public if appropriate, of unclassified, including controlled
3 unclassified, cyber threat indicators and defensive measures the Fed-
4 eral Government possesses;

5 (4) timely sharing with Federal entities and non-Federal entities, if
6 appropriate, of information relating to cybersecurity threats or author-
7 ized uses under this subchapter that the Federal Government possesses
8 about cybersecurity threats to those entities to prevent or mitigate ad-
9 verse effects from the threats; and

10 (5) periodic sharing, through publication and targeted outreach, of
11 cybersecurity best practices that are developed based on ongoing anal-
12 yses of cyber threat indicators, defensive measures, and information re-
13 lating to cybersecurity threats or authorized uses under this sub-
14 chapter, in the possession of the Federal Government with attention to
15 accessibility and implementation challenges faced by small business
16 concerns (as defined in section 3 of the Small Business Act (15 U.S.C.
17 632)).

18 (b) CONTENT.—The procedures developed under subsection (a) shall—

19 (1) ensure the Federal Government has and maintains the capability
20 to share cyber threat indicators and defensive measures in real time
21 consistent with the protection of classified information;

22 (2) incorporate to the greatest extent practicable existing processes
23 and existing roles and responsibilities of Federal entities and non-Fed-
24 eral entities for information sharing by the Federal Government, in-
25 cluding sector-specific information sharing and analysis centers;

26 (3) include procedures for notifying, in a timely manner, Federal en-
27 tities and non-Federal entities that have received a cyber threat indi-
28 cator or defensive measure from a Federal entity under this subchapter
29 that is known or determined to be in error or in contravention of the
30 requirements of this subchapter or another provision of Federal law or
31 policy of the error or contravention;

32 (4) include requirements for Federal entities sharing cyber threat in-
33 dicators or defensive measures to implement and utilize security con-
34 trols to protect against unauthorized access to, or acquisition of, the
35 indicators or measures;

36 (5) include procedures that require a Federal entity, prior to the
37 sharing of a cyber threat indicator—

38 (A) to—

39 (i) review the indicator to assess whether the indicator con-
40 tains any information not directly related to a cybersecurity
41 threat that the Federal entity knows at the time of sharing

1 to be personal information of a specific individual or informa-
2 tion that identifies a specific individual; and

3 (ii) remove the information; or

4 (B) to implement and utilize a technical capability configured to
5 remove information not directly related to a cybersecurity threat
6 that the Federal entity knows at the time of sharing to be per-
7 sonal information of a specific individual or information that iden-
8 tifies a specific individual; and

9 (6) include procedures for notifying, in a timely manner, any United
10 States person whose personal information is known or determined to
11 have been shared by a Federal entity in violation of this subchapter.

12 (e) CONSULTATION.—In developing the procedures required under this
13 section, the Director of National Intelligence, the Secretary, the Secretary
14 of Defense, and the Attorney General shall consult with appropriate Federal
15 entities, including the Small Business Administration and the National Lab-
16 oratories (as defined in section 2 of the Energy Policy Act of 2005 (42
17 U.S.C. 15801)), to ensure that effective protocols are implemented that will
18 facilitate and promote the sharing of cyber threat indicators by the Federal
19 Government in a timely manner.

20 (d) SUBMITTAL TO CONGRESS.—The Director of National Intelligence, in
21 consultation with the heads of the appropriate Federal entities, shall submit
22 to Congress a report on the procedures required by subsection (a).

23 **§ 10783. Authorization for preventing, detecting, analyzing,**
24 **and mitigating cybersecurity threats**

25 (a) AUTHORIZATION FOR MONITORING.—

26 (1) IN GENERAL.—Notwithstanding another law, a private entity
27 may, for cybersecurity purposes, monitor—

28 (A) an information system of the private entity;

29 (B) an information system of another non-Federal entity, on the
30 authorization and written consent of the other entity;

31 (C) an information system of a Federal entity, on the authoriza-
32 tion and written consent of an authorized representative of the
33 Federal entity; and

34 (D) information that is stored on, processed by, or transiting an
35 information system monitored by the private entity under this
36 paragraph.

37 (2) CONSTRUCTION.—Nothing in paragraph (1) shall be construed
38 to—

39 (A) authorize the monitoring of an information system, or the
40 use of information obtained through the monitoring, other than as
41 provided in this subchapter; or

1 (B) limit otherwise lawful activity.

2 (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

3 (1) IN GENERAL.—Notwithstanding another law, a private entity
4 may, for cybersecurity purposes, operate a defensive measure that is
5 applied to—

6 (A) an information system of the private entity to protect the
7 rights or property of the entity;

8 (B) an information system of another non-Federal entity, on
9 written consent of the other entity for operation of the defensive
10 measure to protect the rights or property of the entity;

11 (C) an information system of a Federal entity on written con-
12 sent of an authorized representative of the Federal entity for oper-
13 ation of the defensive measure to protect the rights or property
14 of the Federal Government.

15 (2) CONSTRUCTION.—Nothing in paragraph (1) shall be construed
16 to—

17 (A) authorize the use of a defensive measure other than as pro-
18 vided in paragraph (1); or

19 (B) limit otherwise lawful activity.

20 (c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDI-
21 CATORS OR DEFENSIVE MEASURES.—

22 (1) IN GENERAL.—Except as provided in paragraph (2) and notwith-
23 standing another law, a non-Federal entity may, for a cybersecurity
24 purpose and consistent with the protection of classified information,
25 share with, or receive, from, any other non-Federal entity or the Fed-
26 eral Government a cyber threat indicator or defensive measure.

27 (2) COMPLIANCE WITH LAWFUL RESTRICTION.—A non-Federal enti-
28 ty receiving a cyber threat indicator or defensive measure from another
29 non-Federal entity or a Federal entity shall comply with otherwise law-
30 ful restrictions placed on the sharing or use of the indicator or defen-
31 sive measure by the sharing non-Federal entity or Federal entity.

32 (3) CONSTRUCTION.—Nothing in paragraph (1) shall be construed
33 to—

34 (A) authorize the sharing or receiving of a cyber threat indi-
35 cator or defensive measure other than as provided in paragraph
36 (1); or

37 (B) limit otherwise lawful activity.

38 (d) PROTECTION AND USE OF INFORMATION.—

39 (1) SECURITY OF INFORMATION.—A non-Federal entity monitoring
40 an information system, operating a defensive measure, or providing or
41 receiving a cyber threat indicator or defensive measure under this sec-

1 tion shall implement and utilize a security control to protect against
2 unauthorized access to or acquisition of the cyber threat indicator or
3 defensive measure.

4 (2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—A non-Fed-
5 eral entity sharing a cyber threat indicator pursuant to this subchapter
6 shall, prior to sharing—

7 (A) review the cyber threat indicator to assess whether the indi-
8 cator contains any information not directly related to a cybersecu-
9 rity threat that the non-Federal entity knows at the time of shar-
10 ing to be personal information of a specific individual or informa-
11 tion that identifies a specific individual and remove the informa-
12 tion; or

13 (B) implement and utilize a technical capability configured to
14 remove any information not directly related to a cybersecurity
15 threat that the non-Federal entity knows at the time of sharing
16 to be personal information of a specific individual or information
17 that identifies a specific individual.

18 (3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES
19 BY NON-FEDERAL ENTITIES.—

20 (A) IN GENERAL.—Consistent with this subchapter, a cyber
21 threat indicator or defensive measure shared or received under this
22 section may, for cybersecurity purposes—

23 (i) be used by a non-Federal entity to monitor or operate
24 a defensive measure that is applied to—

25 (I) an information system of the non-Federal entity;

26 or

27 (II) an information system of another non-Federal en-
28 tity or a Federal entity on the written consent of the
29 other non-Federal entity or that Federal entity; and

30 (ii) be otherwise used, retained, and further shared by a
31 non-Federal entity subject to—

32 (I) an otherwise lawful restriction placed by the shar-
33 ing non-Federal entity or Federal entity on the cyber
34 threat indicator or defensive measure; or

35 (II) an otherwise applicable provision of law.

36 (B) CONSTRUCTION.—Nothing in subparagraph (A) shall be
37 construed to authorize the use of a cyber threat indicator or defen-
38 sive measure other than as provided in this section.

39 (4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR
40 LOCAL GOVERNMENT.—

1 (A) LAW ENFORCEMENT USE.—A State, tribal, or local govern-
2 ment that receives a cyber threat indicator or defensive measure
3 under this subchapter may use the cyber threat indicator or defen-
4 sive measure for the purposes described in section 10784(e)(5)(A)
5 of this title.

6 (B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator
7 or defensive measure shared by or with a State, tribal, or local
8 government, including a component of a State, tribal, or local gov-
9 ernment that is a private entity, under this section shall be—

10 (i) considered voluntarily shared information; and

11 (ii) exempt from disclosure under any provision of State,
12 tribal, or local freedom of information law, open government
13 law, open meetings law, open records law, sunshine law, or
14 similar law requiring disclosure of information or records.

15 (C) STATE, TRIBAL, AND LOCAL REGULATORY AUTHORITY.—

16 (i) IN GENERAL.—Except as provided in clause (ii), a cyber
17 threat indicator or defensive measure shared with a State,
18 tribal, or local government under this subchapter shall not be
19 used by any State, tribal, or local government to regulate, in-
20 cluding an enforcement action, the lawful activity of any non-
21 Federal entity or any activity taken by a non-Federal entity
22 pursuant to mandatory standards, including an activity relat-
23 ing to monitoring, operating a defensive measure, or sharing
24 a cyber threat indicator.

25 (ii) REGULATORY AUTHORITY SPECIFICALLY RELATING TO
26 PREVENTION OR MITIGATION OF CYBERSECURITY
27 THREATS.—A cyber threat indicator or defensive measure
28 shared as described in clause (i) may, consistent with a State,
29 tribal, or local government regulatory authority specifically re-
30 lating to the prevention or mitigation of cybersecurity threats
31 to information systems, inform the development or implemen-
32 tation of a regulation relating to the information systems.

33 (e) ANTITRUST EXEMPTION.—

34 (1) IN GENERAL.—Except as provided in section 10789(e) of this
35 title, it shall not be considered a violation of any provision of antitrust
36 laws for 2 or more private entities to exchange or provide a cyber
37 threat indicator or defensive measure, or assistance, relating to the pre-
38 vention, investigation, or mitigation of a cybersecurity threat, for cyber-
39 security purposes under this subchapter.

40 (2) APPLICABILITY.—Paragraph (1) shall apply only to information
41 that is exchanged or assistance provided to assist with—

1 (A) facilitating the prevention, investigation, or mitigation of a
2 cybersecurity threat to an information system or information that
3 is stored on, processed by, or transiting an information system; or

4 (B) communicating or disclosing a cyber threat indicator to help
5 prevent, investigate, or mitigate the effect of a cybersecurity threat
6 to an information system or information that is stored on, pro-
7 cessed by, or transiting an information system.

8 (f) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator or
9 defensive measure with a non-Federal entity under this subchapter shall not
10 create a right or benefit to similar information by the non-Federal entity
11 or any other non-Federal entity.

12 **§ 10784. Sharing of cyber threat indicators and defensive**
13 **measures with Federal Government**

14 (a) DEVELOPMENT OF POLICIES AND PROCEDURES.—The Attorney Gen-
15 eral and the Secretary shall, in consultation with the heads of the appro-
16 priate Federal entities, jointly issue and make publicly available policies and
17 procedures relating to the receipt of cyber threat indicators and defensive
18 measures by the Federal Government. Consistent with the guidelines re-
19 quired by subsection (c), the policies and procedures shall ensure—

20 (1) that cyber threat indicators shared with the Federal Government
21 by any non-Federal entity pursuant to section 10783(c) of this title
22 through the real-time process described in subsection (d)—

23 (A) are shared in an automated manner with all appropriate
24 Federal entities;

25 (B) are only subject to a delay, modification, or other action due
26 to controls established for the real-time process that could impede
27 real-time receipt by all appropriate Federal entities when the
28 delay, modification, or other action is due to controls—

29 (i) agreed on unanimously by all of the heads of the appro-
30 priate Federal entities;

31 (ii) carried out before any appropriate Federal entity re-
32 tains or uses the cyber threat indicators or defensive meas-
33 ures; and

34 (iii) uniformly applied so that each appropriate Federal en-
35 tity is subject to the same delay, modification, or other ac-
36 tion; and

37 (C) may be provided to other Federal entities;

38 (2) that cyber threat indicators shared with the Federal Government
39 by any non-Federal entity pursuant to section 10783 of this title in a
40 manner other than the real-time process described in subsection (d)—

1 (A) are shared as quickly as operationally practicable with all
2 appropriate Federal entities;

3 (B) are not subject to any unnecessary delay, interference, or
4 any other action that could impede receipt by all appropriate Fed-
5 eral entities; and

6 (C) may be provided to other Federal entities; and

7 (3) there are—

8 (A) audit capabilities; and

9 (B) appropriate sanctions in place for officers, employees, or
10 agents of a Federal entity who knowingly and willfully conduct ac-
11 tivities under this subchapter in an unauthorized manner.

12 (b) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS
13 WITH FEDERAL GOVERNMENT.—The Attorney General and the Secretary
14 jointly shall develop and make publicly available guidance to assist entities
15 and promote sharing of cyber threat indicators with Federal entities under
16 this subchapter. The guidelines shall include guidance on the following:

17 (1) Identification of types of information that would qualify as a
18 cyber threat indicator under this subchapter that would be unlikely to
19 include information that—

20 (A) is not directly related to a cybersecurity threat; and

21 (B) is personal information of a specific individual or informa-
22 tion that identifies a specific individual.

23 (2) Identification of types of information protected under otherwise
24 applicable privacy laws that are unlikely to be directly related to a cy-
25 bersecurity threat.

26 (3) Such other matters as the Attorney General and the Secretary
27 consider appropriate for entities sharing cyber threat indicators with
28 Federal entities under this subchapter.

29 (c) PRIVACY AND CIVIL LIBERTIES.—

30 (1) ISSUANCE AND AVAILABILITY OF GUIDELINES.—The Attorney
31 General and the Secretary shall, in coordination with the heads of the
32 appropriate Federal entities and in consultation with officers des-
33 ignated under section 1062 of the National Security Intelligence Re-
34 form Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with
35 industry expertise as the Attorney General and the Secretary consider
36 relevant, jointly issue and make publicly available final guidelines relat-
37 ing to privacy and civil liberties that shall govern the receipt, retention,
38 use, and dissemination of cyber threat indicators by a Federal entity
39 obtained in connection with activities authorized in this subchapter.

1 (2) CONTENT.—The guidelines shall, consistent with the need to pro-
2 tect information systems from cybersecurity threats and mitigate cyber-
3 security threats—

4 (A) limit the effect on privacy and civil liberties of activities by
5 the Federal Government under this subchapter;

6 (B) limit the receipt, retention, use, and dissemination of cyber
7 threat indicators containing personal information of specific indi-
8 viduals or information that identifies specific individuals, including
9 by establishing—

10 (i) a process for the timely destruction of the information
11 that is known not to be directly related to uses authorized
12 under this subchapter; and

13 (ii) specific limitations on the length of any period in which
14 a cyber threat indicator may be retained;

15 (C) include requirements to safeguard cyber threat indicators
16 containing personal information of specific individuals or informa-
17 tion that identifies specific individuals from unauthorized access or
18 acquisition, including appropriate sanctions for activities by offi-
19 cers, employees, or agents of the Federal Government in con-
20 travention of the guidelines;

21 (D) consistent with this subchapter, any other applicable provi-
22 sions of law, and the fair information practice principles set forth
23 in appendix A of the document entitled “National Strategy for
24 Trusted Identities in Cyberspace” and published by the President
25 in April 2011, govern the retention, use, and dissemination by the
26 Federal Government of cyber threat indicators shared with the
27 Federal Government under this subchapter, including the extent to
28 which the cyber threat indicators may be used by the Federal Gov-
29 ernment;

30 (E) include procedures for notifying entities and Federal enti-
31 ties if information received pursuant to this section is known or
32 determined by a Federal entity receiving the information not to
33 constitute a cyber threat indicator;

34 (F) protect the confidentiality of cyber threat indicators con-
35 taining personal information of specific individuals or information
36 that identifies specific individuals to the greatest extent practicable
37 and require recipients to be informed that the indicators may only
38 be used for purposes authorized under this subchapter; and

39 (G) include steps that may be needed so that dissemination of
40 cyber threat indicators is consistent with the protection of classi-
41 fied and other sensitive national security information.

1 (3) PERIODIC REVIEW.—The Attorney General and the Secretary
2 shall, in coordination with the heads of the appropriate Federal entities
3 and in consultation with officers and private entities described in para-
4 graph (1), periodically, but not less frequently than once every 2 years,
5 jointly review the guidelines issued under paragraph (1).

6 (d) CAPABILITY AND PROCESS IN THE DEPARTMENT.—

7 (1) IN GENERAL.—The Secretary, in coordination with the heads of
8 the appropriate Federal entities, shall develop and implement a capa-
9 bility and process in the Department that—

10 (A) shall accept from any non-Federal entity in real time cyber
11 threat indicators and defensive measures, pursuant to this section;

12 (B) on submittal of the certification under paragraph (2) that
13 the capability and process fully and effectively operates as de-
14 scribed in paragraph (2), shall be the process by which the Fed-
15 eral Government receives cyber threat indicators and defensive
16 measures under this subchapter that are shared by a non-Federal
17 entity with the Federal Government through electronic mail or
18 media, an interactive form on an Internet website, or a real time,
19 automated process between information systems, except—

20 (i) consistent with section 10733 of this title, communica-
21 tions between a Federal entity and a non-Federal entity re-
22 garding a previously shared cyber threat indicator to—

23 (I) describe the relevant cybersecurity threat; or

24 (II) develop a defensive measure based on the cyber
25 threat indicator; and

26 (ii) communications by a regulated non-Federal entity with
27 the entity's Federal regulatory authority regarding a cyberse-
28 curity threat;

29 (C) ensures that all of the appropriate Federal entities receive
30 in an automated manner cyber threat indicators and defensive
31 measures shared through the real-time process in the Department;

32 (D) is in compliance with the policies, procedures, and guide-
33 lines required by this section; and

34 (E) does not limit or prohibit otherwise lawful disclosures of
35 communications, records, or other information, including—

36 (i) the reporting of known or suspected criminal activity,
37 by a non-Federal entity to any other non-Federal entity or a
38 Federal entity, including cyber threat indicators or defensive
39 measures shared with a Federal entity in furtherance of open-
40 ing a Federal law enforcement investigation;

- 1 (ii) voluntary or legally compelled participation in a Fed-
- 2 eral investigation; and
- 3 (iii) the provision of cyber threat indicators or defensive
- 4 measures as part of a statutory or authorized contractual re-
- 5 quirement.

6 (2) CERTIFICATION AND DESIGNATION.—

7 (A) CERTIFICATION OF CAPABILITY AND PROCESS.—The Sec-

8 retary shall, in consultation with the heads of the appropriate Fed-

9 eral entities, submit to Congress a certification as to whether the

10 capability and process required by paragraph (1) fully and effec-

11 tively operates—

- 12 (i) as the process by which the Federal Government re-
- 13 ceives from any non-Federal entity a cyber threat indicator
- 14 or defensive measure under this subchapter; and
- 15 (ii) in accordance with the interim policies, procedures, and
- 16 guidelines developed under this subchapter.

17 (B) DESIGNATION.—

18 (i) IN GENERAL.—At any time after certification is sub-

19 mitted under subparagraph (A), the President may designate

20 an appropriate Federal entity, other than the Department of

21 Defense (including the National Security Agency), to develop

22 and implement a capability and process as described in para-

23 graph (1) in addition to the capability and process developed

24 under paragraph (1) by the Secretary, if, not fewer than 30

25 days before making the designation, the President submits to

26 Congress a certification and explanation that—

27 (I) the designation is necessary to ensure full, effec-

28 tive, and secure operation of a capability and process for

29 the Federal Government to receive from any non-Federal

30 entity cyber threat indicators or defensive measures

31 under this subchapter;

32 (II) the designated appropriate Federal entity will re-

33 ceive and share cyber threat indicators and defensive

34 measures in accordance with the policies, procedures,

35 and guidelines developed under this subchapter, includ-

36 ing subsection (a)(1); and

37 (III) the designation is consistent with the mission of

38 the appropriate Federal entity and improves the ability

39 of the Federal Government to receive, share, and use

40 cyber threat indicators and defensive measures as au-

41 thorized under this subchapter.

1 (ii) APPLICATION TO ADDITIONAL CAPABILITY AND PROC-
2 ESS.—If the President designates an appropriate Federal en-
3 tity to develop and implement a capability and process under
4 clause (i), this subchapter that apply to the capability and
5 process required by paragraph (1) apply to the capability and
6 process developed and implemented under clause (i).

7 (3) PUBLIC NOTICE AND ACCESS.—The Secretary shall ensure there
8 is public notice of, and access to, the capability and process developed
9 and implemented under paragraph (1) so that—

10 (A) any non-Federal entity may share cyber threat indicators
11 and defensive measures through the process with the Federal Gov-
12 ernment; and

13 (B) all of the appropriate Federal entities receive the cyber
14 threat indicators and defensive measures in real time with receipt
15 through the process in the Department consistent with the policies
16 and procedures issued under subsection (a).

17 (4) OTHER FEDERAL ENTITIES.—The process developed and imple-
18 mented under paragraph (1) shall ensure that other Federal entities re-
19 ceive in a timely manner any cyber threat indicators and defensive
20 measures shared with the Federal Government through the process.

21 (e) INFORMATION SHARED WITH OR PROVIDED TO FEDERAL GOVERN-
22 MENT.—

23 (1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of
24 cyber threat indicators and defensive measures to the Federal Govern-
25 ment under this subchapter shall not constitute a waiver of any appli-
26 cable privilege or protection provided by law, including trade secret pro-
27 tection.

28 (2) PROPRIETARY INFORMATION.—Consistent with section
29 10783(c)(2) of this title and any other applicable provision of law, a
30 cyber threat indicator or defensive measure provided by a non-Federal
31 entity to the Federal Government under this subchapter shall be con-
32 sidered the commercial, financial, and proprietary information of the
33 non-Federal entity when so designated by the originating non-Federal
34 entity or a third party acting in accordance with the written authoriza-
35 tion of the originating non-Federal entity.

36 (3) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator or de-
37 fensive measure shared with the Federal Government under this sub-
38 chapter shall be—

39 (A) deemed voluntarily shared information and exempt from dis-
40 closure under section 552 of title 5 and any State, tribal, or local
41 provision of law requiring disclosure of information or records; and

1 (B) withheld, without discretion, from the public under section
2 552(b)(3)(B) of title 5 and any State, tribal, or local provision of
3 law requiring disclosure of information or records.

4 (4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat
5 indicator or defensive measure to the Federal Government under this
6 subchapter shall not be subject to a rule of any Federal agency or de-
7 partment or any judicial doctrine regarding ex parte communications
8 with a decision-making official.

9 (5) DISCLOSURE, RETENTION, AND USE.—

10 (A) AUTHORIZED ACTIVITIES.—Cyber threat indicators and de-
11 fensive measures provided to the Federal Government under this
12 subchapter may, consistent with otherwise applicable provisions of
13 Federal law, be disclosed to, retained by, and used by any Federal
14 agency or department, component, officer, employee, or agent of
15 the Federal Government solely for—

16 (i) a cybersecurity purpose;

17 (ii) the purpose of identifying—

18 (I) a cybersecurity threat, including the source of the
19 cybersecurity threat; or

20 (II) a security vulnerability;

21 (iii) the purpose of responding to, or otherwise preventing
22 or mitigating, a specific threat of death, a specific threat of
23 serious bodily harm, or a specific threat of serious economic
24 harm, including a terrorist act or a use of a weapon of mass
25 destruction;

26 (iv) the purpose of responding to, investigating, pros-
27 ecuting, or otherwise preventing or mitigating, a serious
28 threat to a minor, including sexual exploitation and threats
29 to physical safety; or

30 (v) the purpose of preventing, investigating, disrupting, or
31 prosecuting an offense arising out of a threat described in
32 clause (iii) or any of the offenses listed in sections 1028
33 through 1030 and chapters 37 and 90 of title 18.

34 (B) PROHIBITED ACTIVITIES.—Cyber threat indicators and de-
35 fensive measures provided to the Federal Government under this
36 subchapter shall not be disclosed to, retained by, or used by any
37 Federal agency or department for any use not permitted under
38 subparagraph (A).

39 (C) PRIVACY AND CIVIL LIBERTIES.—Cyber threat indicators
40 and defensive measures provided to the Federal Government under

1 this subchapter shall be retained, used, and disseminated by the
2 Federal Government—

3 (i) in accordance with the policies, procedures, and guide-
4 lines required by subsections (a) through (c);

5 (ii) in a manner that protects from unauthorized use or
6 disclosure any cyber threat indicators that may contain—

7 (I) personal information of a specific individual; or

8 (II) information that identifies a specific individual;

9 and

10 (iii) in a manner that protects the confidentiality of cyber
11 threat indicators containing—

12 (I) personal information of a specific individual; or

13 (II) information that identifies a specific individual.

14 (D) FEDERAL REGULATORY AUTHORITY.—

15 (i) IN GENERAL.—Except as provided in clause (ii), cyber
16 threat indicators and defensive measures provided to the Fed-
17 eral Government under this subchapter shall not be used by
18 any Federal, State, tribal, or local government to regulate, in-
19 cluding an enforcement action, the lawful activities of any
20 non-Federal entity or any activities taken by a non-Federal
21 entity pursuant to mandatory standards, including activities
22 relating to monitoring, operating defensive measures, or shar-
23 ing cyber threat indicators.

24 (ii) EXCEPTIONS.—

25 (I) REGULATORY AUTHORITY SPECIFICALLY RELATING
26 TO PREVENTION OR MITIGATION OF CYBERSECURITY
27 THREATS.—Cyber threat indicators and defensive meas-
28 ures provided to the Federal Government under this sub-
29 chapter may, consistent with Federal or State regulatory
30 authority specifically relating to the prevention or miti-
31 gation of cybersecurity threats to information systems,
32 inform the development or implementation of regulations
33 relating to the information systems.

34 (II) PROCEDURES DEVELOPED AND IMPLEMENTED
35 UNDER THIS SUBCHAPTER.—Clause (i) shall not apply to
36 procedures developed and implemented under this sub-
37 chapter.

38 **§ 10785. Protection from liability**

39 (a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall
40 be brought in any court against any private entity, and the action shall be
41 promptly dismissed, for the monitoring of an information system and infor-

1 information under section 10783(a) of this title that is conducted in accordance
2 with this subchapter.

3 (b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of
4 action shall be brought in any court against any private entity, and the ac-
5 tion shall be promptly dismissed, for the sharing or receipt of a cyber threat
6 indicator or defensive measure under section 10783(e) of this title if—

7 (1) the sharing or receipt is conducted in accordance with this sub-
8 chapter; and

9 (2) in a case in which a cyber threat indicator or defensive measure
10 is shared with the Federal Government, the cyber threat indicator or
11 defensive measure is shared in a manner that is consistent with section
12 10784(d)(1)(B) of this title.

13 (c) CONSTRUCTION.—Nothing in this subchapter shall be construed—

14 (1) to create—

15 (A) a duty to share a cyber threat indicator or defensive meas-
16 ure; or

17 (B) a duty to warn or act based on the receipt of a cyber threat
18 indicator or defensive measure; or

19 (2) to undermine or limit the availability of otherwise applicable com-
20 mon law or statutory defenses.

21 **§ 10786. Oversight of Government activities**

22 (a) REPORT ON IMPLEMENTATION.—Not later than December 18, 2016,
23 the heads of the appropriate Federal entities shall jointly submit to Con-
24 gress a detailed report concerning the implementation of this subchapter.
25 The report may include such recommendations as the heads of the appro-
26 priate Federal entities may have for improvements or modifications to the
27 authorities, policies, procedures, and guidelines under this subchapter and
28 shall include the following:

29 (1) An evaluation of the effectiveness of real-time information shar-
30 ing through the capability and process developed under section
31 10784(d) of this title, including any impediments to real-time sharing.

32 (2) An assessment of whether cyber threat indicators or defensive
33 measures have been properly classified and an accounting of the num-
34 ber of security clearances authorized by the Federal Government for
35 sharing cyber threat indicators or defensive measures with the private
36 sector.

37 (3) The number of cyber threat indicators or defensive measures re-
38 ceived through the capability and process developed under section
39 10784(d) of this title.

40 (4) A list of Federal entities that have received cyber threat indica-
41 tors or defensive measures under this subchapter.

1 (b) BIENNIAL REPORT ON COMPLIANCE.—

2 (1) WHEN REPORT SHALL BE SUBMITTED.—Not later than Decem-
3 ber 18, 2017, and not less frequently than once every 2 years there-
4 after, the inspectors general of the appropriate Federal entities, in con-
5 sultation with the Inspector General of the Intelligence Community and
6 the Council of Inspectors General on Financial Oversight, shall jointly
7 submit to Congress an interagency report on the actions of the execu-
8 tive branch of the Federal Government to carry out this subchapter
9 during the most recent 2-year period.

10 (2) CONTENTS.—Each report shall include, for the period covered by
11 the report, the following:

12 (A) An assessment of the sufficiency of the policies, procedures,
13 and guidelines relating to the sharing of cyber threat indicators in
14 the Federal Government, including those policies, procedures, and
15 guidelines relating to the removal of information not directly re-
16 lated to a cybersecurity threat that is personal information of a
17 specific individual or information that identifies a specific indi-
18 vidual.

19 (B) An assessment of whether cyber threat indicators or defen-
20 sive measures have been properly classified and an accounting of
21 the number of security clearances authorized by the Federal Gov-
22 ernment for the purpose of sharing cyber threat indicators or de-
23 fensive measures with the private sector.

24 (C) A review of the actions taken by the Federal Government
25 based on cyber threat indicators or defensive measures shared with
26 the Federal Government under this subchapter, including a review
27 of the following:

28 (i) The appropriateness of subsequent uses and dissemina-
29 tions of cyber threat indicators or defensive measures.

30 (ii) Whether cyber threat indicators or defensive measures
31 were shared in a timely and adequate manner with appro-
32 priate entities, or, if appropriate, were made publicly avail-
33 able.

34 (D) An assessment of the cyber threat indicators or defensive
35 measures shared with the appropriate Federal entities under this
36 subchapter, including the following:

37 (i) The number of cyber threat indicators or defensive
38 measures shared through the capability and process developed
39 under section 10784(d) of this title.

40 (ii) An assessment of any information not directly related
41 to a cybersecurity threat that is personal information of a

1 specific individual or information identifying a specific indi-
2 vidual and was shared by a non-Federal government entity
3 with the Federal Government in contravention of this sub-
4 chapter, or was shared in the Federal Government in con-
5 travention of the guidelines required by this subchapter, in-
6 cluding a description of any significant violation of this sub-
7 chapter.

8 (iii) The number of times, according to the Attorney Gen-
9 eral, that information shared under this subchapter was used
10 by a Federal entity to prosecute an offense listed in section
11 10784(e)(5)(A) of this title.

12 (iv) A quantitative and qualitative assessment of the effect
13 of the sharing of cyber threat indicators or defensive meas-
14 ures with the Federal Government on the privacy and civil
15 liberties of specific individuals, including the number of no-
16 tices that were issued with respect to a failure to remove in-
17 formation not directly related to a cybersecurity threat that
18 was personal information of a specific individual or informa-
19 tion that identified a specific individual in accordance with
20 the procedures required by section 10784(c)(2)(E) of this
21 title.

22 (v) The adequacy of any steps taken by the Federal Gov-
23 ernment to reduce any adverse effect from activities carried
24 out under this subchapter on the privacy and civil liberties of
25 United States persons.

26 (E) An assessment of the sharing of cyber threat indicators or
27 defensive measures among Federal entities to identify inappro-
28 priate barriers to sharing information.

29 (3) RECOMMENDATIONS.—Each report may include such rec-
30 ommendations as the inspectors general may have for improvements or
31 modifications to the authorities and processes under this subchapter.

32 (c) INDEPENDENT REPORT ON REMOVAL OF PERSONAL INFORMATION.—
33 Not later than December 18, 2018, the Comptroller General shall submit
34 to Congress a report on the actions taken by the Federal Government to
35 remove personal information from cyber threat indicators or defensive meas-
36 ures pursuant to this subchapter. The report shall include an assessment
37 of the sufficiency of the policies, procedures, and guidelines established
38 under this subchapter in addressing concerns relating to privacy and civil
39 liberties.

40 (d) FORM OF REPORTS.—Each report required under this section shall
41 be submitted in an unclassified form, but may include a classified annex.

1 (e) PUBLIC AVAILABILITY OF REPORTS.—The unclassified portions of the
2 reports required under this section shall be made available to the public.

3 **§ 10787. Report on cybersecurity threats**

4 (a) DEFINITION OF INTELLIGENCE COMMUNITY.—In this section, the
5 term “intelligence community” has the meaning given that term in section
6 3 of the National Security Act of 1947 (50 U.S.C. 3003).

7 (b) WHEN REPORT SHALL BE SUBMITTED.—Not later than 180 days
8 after December 18, 2015, the Director of National Intelligence, in coordina-
9 tion with the heads of other appropriate elements of the intelligence commu-
10 nity, shall submit to the Select Committee on Intelligence of the Senate and
11 the Permanent Select Committee on Intelligence of the House of Represent-
12 atives a report on cybersecurity threats, including cyberattacks, theft, and
13 data breaches.

14 (c) CONTENTS.—The report shall include the following:

15 (1) An assessment of the current intelligence sharing and coopera-
16 tion relationships of the United States with other countries regarding
17 cybersecurity threats, including cyberattacks, theft, and data breaches,
18 directed against the United States that threaten the United States’ na-
19 tional security interests, economy, and intellectual property, specifically
20 identifying the relative utility of the relationships, which elements of
21 the intelligence community participate in the relationships, and whether
22 and how the relationships could be improved.

23 (2) A list and an assessment of the countries and nonstate actors
24 that are the primary threats to carry out a cybersecurity threat, includ-
25 ing a cyberattack, theft, or data breach, against the United States that
26 threatens the United States’ national security, economy, and intellec-
27 tual property.

28 (3) A description of the extent to which the capabilities of the United
29 States Government to respond to or prevent cybersecurity threats, in-
30 cluding cyberattacks, theft, or data breaches, directed against the
31 United States private sector are degraded by a delay in the prompt no-
32 tification by private entities of those threats or cyberattacks, theft, and
33 data breaches.

34 (4) An assessment of additional technologies or capabilities that
35 would enhance the ability of the United States to prevent and to re-
36 spond to cybersecurity threats, including cyberattacks, theft, and data
37 breaches.

38 (5) An assessment of any technologies or practices utilized by the
39 private sector that could be rapidly fielded to assist the intelligence
40 community in preventing and responding to cybersecurity threats.

1 (d) FORM OF REPORT.—The report required by subsection (b) shall be
2 made available in classified and unclassified forms.

3 **§ 10788. Exception to limitation on authority of Secretary of**
4 **Defense to disseminate information**

5 Notwithstanding section 393(c)(3) of title 10, the Secretary of Defense
6 may authorize the sharing of cyber threat indicators and defensive measures
7 pursuant to the policies, procedures, and guidelines developed or issued
8 under this subchapter.

9 **§ 10789. Construction and preemption**

10 (a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this subchapter
11 shall be construed—

12 (1) to limit or prohibit otherwise lawful disclosures of communica-
13 tions, records, or other information, including reporting of known or
14 suspected criminal activity, by a non-Federal entity to any other non-
15 Federal entity or the Federal Government under this subchapter; or

16 (2) to limit or prohibit otherwise lawful use of the disclosures by any
17 Federal entity, even when the otherwise lawful disclosures duplicate or
18 replicate disclosures made under this subchapter.

19 (b) WHISTLE BLOWER PROTECTIONS.—Nothing in this subchapter shall
20 be construed to prohibit or limit the disclosure of information protected
21 under section 2302(b)(8) or 7211 of title 5, section 1034 of title 10, section
22 1104 of the National Security Act of 1947 (50 U.S.C. 3234), or any similar
23 provision of Federal or State law.

24 (c) PROTECTION OF SOURCES AND METHODS.—Nothing in this sub-
25 chapter shall be construed—

26 (1) to create any immunity against, or otherwise affecting, any ac-
27 tion brought by the Federal Government, or any agency or department
28 of the Government, to enforce any law, executive order, or procedure
29 governing the appropriate handling, disclosure, or use of classified in-
30 formation;

31 (2) to affect the conduct of authorized law enforcement or intel-
32 ligence activities; or

33 (3) to modify the authority of a department or agency of the Federal
34 Government to protect classified information and sources and methods
35 and the national security of the United States.

36 (d) RELATIONSHIP TO OTHER LAWS.—Nothing in this subchapter shall
37 be construed to affect any requirement under any other provision of law for
38 a non-Federal entity to provide information to the Federal Government.

39 (e) PROHIBITED CONDUCT.—Nothing in this subchapter shall be con-
40 strued to permit price-fixing, allocating a market between competitors, mo-
41 nopolizing or attempting to monopolize a market, boycotting, or exchanging

1 price or cost information, customer lists, or information regarding future
2 competitive planning.

3 (f) INFORMATION SHARING RELATIONSHIPS.—Nothing in this subchapter
4 shall be construed—

5 (1) to limit or modify an existing information sharing relationship;

6 (2) to prohibit a new information sharing relationship;

7 (3) to require a new information sharing relationship between any
8 non-Federal entity and a Federal entity or another non-Federal entity;
9 or

10 (4) to require the use of the capability and process in the Depart-
11 ment developed under section 10784(d) of this title.

12 (g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—
13 Nothing in this subchapter shall be construed—

14 (1) to amend, repeal, or supersede any current or future contractual
15 agreement, terms of service agreement, or other contractual relation-
16 ship between non-Federal entities, or between a non-Federal entity and
17 a Federal entity; or

18 (2) to abrogate trade secret or intellectual property rights of a non-
19 Federal entity or Federal entity.

20 (h) ANTI-TASKING RESTRICTION.—Nothing in this subchapter shall be
21 construed to permit a Federal entity—

22 (1) to require a non-Federal entity to provide information to a Fed-
23 eral entity or another non-Federal entity;

24 (2) to condition the sharing of cyber threat indicators with a non-
25 Federal entity on the entity's provision of cyber threat indicators to a
26 Federal entity or another non-Federal entity; or

27 (3) to condition the award of a Federal grant, contract, or purchase
28 on the provision of a cyber threat indicator to a Federal entity or an-
29 other non-Federal entity.

30 (i) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this subchapter
31 shall be construed to subject any entity to liability for choosing not to en-
32 gage in the voluntary activities authorized in this subchapter.

33 (j) USE AND RETENTION OF INFORMATION.—Nothing in this subchapter
34 shall be construed to authorize, or to modify any existing authority of, a
35 department or agency of the Federal Government to retain or use any infor-
36 mation shared under this subchapter for any use other than permitted in
37 this subchapter.

38 (k) FEDERAL PREEMPTION.—

39 (1) IN GENERAL.—This subchapter supersedes any statute or other
40 provision of law of a State or political subdivision of a State that re-

1 stricts or otherwise expressly regulates an activity authorized under
2 this subchapter.

3 (2) STATE LAW ENFORCEMENT.—Nothing in this subchapter shall be
4 construed to supersede any statute or other provision of law of a State
5 or political subdivision of a State concerning the use of authorized law
6 enforcement practices and procedures.

7 (l) REGULATORY AUTHORITY.—Nothing in this subchapter shall be con-
8 strued—

9 (1) to authorize the prescribing of any regulations not specifically
10 authorized to be issued under this subchapter;

11 (2) to establish or limit any regulatory authority not specifically es-
12 tablished or limited under this subchapter; or

13 (3) to authorize regulatory actions that would duplicate or conflict
14 with regulatory requirements, mandatory standards, or related proc-
15 esses under another provision of Federal law.

16 (m) AUTHORITY OF SECRETARY OF DEFENSE TO RESPOND TO MALI-
17 CIOUS CYBER ACTIVITY CARRIED OUT BY FOREIGN POWERS.—Nothing in
18 this subchapter shall be construed to limit the authority of the Secretary
19 of Defense under section 394 of title 10.

20 (n) DISCLOSURE IN CRIMINAL PROSECUTION.—Nothing in this sub-
21 chapter shall be construed to prevent the disclosure of a cyber threat indi-
22 cator or defensive measure shared under this subchapter in a criminal pro-
23 secution when an applicable provision of Federal, State, tribal, or local law
24 requires disclosure in the case.

25 **§ 10790. Effective period**

26 (a) IN GENERAL.—Except as provided in subsection (b), this subchapter
27 and the amendments made by the Cybersecurity Information Sharing Act
28 of 2015 (Public Law 114–113, div. N, title I, 129 Stat. 2936) are effective
29 during the period ending on September 30, 2025.

30 (b) EXCEPTION.—With respect to any action authorized by this sub-
31 chapter or information obtained pursuant to an action authorized by this
32 subchapter that occurs before the date on which the provisions referred to
33 in subsection (a) cease to have effect, this subchapter shall continue in ef-
34 fect.

35 **Subchapter VI—Cybersecurity**
36 **Enhancement**
37 **Part A—Federal Cybersecurity**
38 **Enhancement**

39 **§ 10801. Definitions**

40 In this part:

1 (1) AGENCY.—The term “agency” has the meaning given the term
2 in section 3502 of title 44.

3 (2) AGENCY INFORMATION SYSTEM.—The term “agency information
4 system” has the meaning given the term in section 10707 of this title.

5 (3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
6 priate congressional committees” means—

7 (A) the Committee on Homeland Security and Governmental
8 Affairs of the Senate; and

9 (B) the Committee on Homeland Security of the House of Rep-
10 resentatives.

11 (4) CYBERSECURITY RISK.—The term “cybersecurity risk” has the
12 meaning given the term in section 10701 of this title.

13 (5) DIRECTOR.—The term “Director” means the Director of the Of-
14 fice of Management and Budget.

15 (6) INFORMATION SYSTEM.—The term “information system” has the
16 meaning given the term in section 10706 of this title.

17 (7) INTELLIGENCE COMMUNITY.—The term “intelligence commu-
18 nity” has the meaning given the term in section 3 of the National Se-
19 curity Act of 1947 (50 U.S.C. 3003).

20 (8) NATIONAL SECURITY SYSTEM.—The term “national security sys-
21 tem” has the meaning given the term in section 11103 of title 40.

22 § 10802. Advanced internal defenses

23 (a) ADVANCED NETWORK SECURITY TOOLS.—

24 (1) IN GENERAL.—The Secretary shall include, in the efforts of the
25 Department to continuously diagnose and mitigate cybersecurity risks,
26 advanced network security tools to improve visibility of network activ-
27 ity, including through the use of commercial and free or open source
28 tools, and to detect and mitigate intrusions and anomalous activity.

29 (2) DEVELOPMENT OF PLAN.—The Director shall develop, and the
30 Secretary shall implement, a plan to ensure that each agency utilizes
31 advanced network security tools, including those described in paragraph
32 (1), to detect and mitigate intrusions and anomalous activity.

33 (b) PRIORITIZING ADVANCED SECURITY TOOLS.—The Director and the
34 Secretary, in consultation with appropriate agencies, shall—

35 (1) review and update Government-wide policies and programs to en-
36 sure appropriate prioritization and use of network security monitoring
37 tools in agency networks; and

38 (2) brief appropriate congressional committees on the prioritization
39 and use.

40 (c) IMPROVED METRICS.—The Secretary, in collaboration with the Direc-
41 tor, shall review and update the metrics used to measure security under sec-

1 tion 3554 of title 44 to include measures of intrusion and incident detection
2 and response times.

3 (d) **TRANSPARENCY AND ACCOUNTABILITY.**—The Director, in consulta-
4 tion with the Secretary, shall increase transparency to the public on agency
5 cybersecurity posture, including by increasing the number of metrics avail-
6 able on Federal Government performance websites and, to the greatest ex-
7 tent practicable, by displaying metrics for department components, small
8 agencies, and micro-agencies.

9 (e) **EXCEPTION.**—The requirements under this section shall not apply to
10 the Department of Defense, a national security system, or an element of
11 the intelligence community.

12 **§ 10803. Federal cybersecurity requirements**

13 (a) **IMPLEMENTATION OF FEDERAL CYBERSECURITY STANDARDS.**—Con-
14 sistent with section 3553 of title 44, the Secretary, in consultation with the
15 Director, shall exercise the authority to issue binding operational directives
16 to assist the Director in ensuring timely agency adoption of, and compliance
17 with, policies and standards promulgated under section 11331 of title 40
18 for securing agency information systems.

19 (b) **CYBERSECURITY REQUIREMENTS AT AGENCIES.**—

20 (1) **IN GENERAL.**—Consistent with policies, standards, guidelines,
21 and directives on information security under subchapter II of chapter
22 35 of title 44 and the standards and guidelines promulgated under sec-
23 tion 11331 of title 40 and except as provided in paragraph (2), not
24 later than December 18, 2016, the head of each agency shall—

25 (A) identify sensitive and mission critical data stored by the
26 agency consistent with the inventory required under the first sub-
27 section (c) (relating to the inventory of major information sys-
28 tems) and the second subsection (c) (relating to the inventory of
29 information systems) of section 3505 of title 44;

30 (B) assess access controls to the data described in subparagraph
31 (A), the need for readily accessible storage of the data, and indi-
32 viduals' need to access the data;

33 (C) encrypt or otherwise render indecipherable to unauthorized
34 users the data described in subparagraph (A) that is stored on or
35 transiting agency information systems;

36 (D) implement a single sign-on trusted identity platform for in-
37 dividuals accessing each public website of the agency that requires
38 user authentication, as developed by the Administrator of General
39 Services in collaboration with the Secretary; and

1 (E) implement identity management consistent with section 504
2 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7464),
3 including multi-factor authentication, for—

4 (i) remote access to an agency information system; and
5 (ii) each user account with elevated privileges on an agency
6 information system.

7 (2) EXCEPTION.—The requirements under paragraph (1) shall not
8 apply to an agency information system for which—

9 (A) the head of the agency has personally certified to the Direc-
10 tor with particularity that—

11 (i) operational requirements articulated in the certification
12 and related to the agency information system would make it
13 excessively burdensome to implement the cybersecurity re-
14 quirement;

15 (ii) the cybersecurity requirement is not necessary to secure
16 the agency information system or agency information stored
17 on or transiting it; and

18 (iii) the agency has taken all necessary steps to secure the
19 agency information system and agency information stored on
20 or transiting it; and

21 (B) the head of the agency or the designee of the head of the
22 agency has submitted the certification described in subparagraph
23 (A) to the appropriate congressional committees and the agency's
24 authorizing committees.

25 (3) CONSTRUCTION.—

26 (A) AUTHORITY OF OFFICIALS NOT ALTERED.—Nothing in this
27 section shall be construed to alter the authority of the Secretary,
28 the Director, or the Director of the National Institute of Stand-
29 ards and Technology in implementing subchapter II of chapter 35
30 of title 44.

31 (B) DEVELOPMENT OF TECHNOLOGY, STANDARDS, POLICIES,
32 AND GUIDELINES NOT AFFECTED.—Nothing in this section shall
33 be construed to affect the National Institute of Standards and
34 Technology standards process or the requirement under section
35 3553(a)(4) of title 44 or to discourage continued improvements
36 and advancements in the technology, standards, policies, and
37 guidelines used to promote Federal information security.

38 (c) EXCEPTION.—The requirements under this section do not apply to the
39 Department of Defense, a national security system, or an element of the
40 intelligence community.

1 **§ 10804. Assessment; reports**

2 (a) DEFINITIONS.—In this section:

3 (1) AGENCY INFORMATION.—The term “agency information” has the
4 meaning given the term in section 10711 of this title.

5 (2) CYBER THREAT INDICATOR; DEFENSIVE MEASURE.—The terms
6 “cyber threat indicator” and “defensive measure” have the meanings
7 given the terms in section 10701 of this title.

8 (3) INTRUSION ASSESSMENTS.—The term “intrusion assessments”
9 means actions taken under the intrusion assessment plan to identify
10 and remove intruders in agency information systems.

11 (4) INTRUSION ASSESSMENT PLAN.—The term “intrusion assess-
12 ment plan” means the plan required under section 10707(b) of this
13 title.

14 (5) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—The
15 term “intrusion detection and prevention capabilities” means the capa-
16 bilities required under section 10711(b) of this title.

17 (b) THIRD PARTY ASSESSMENT.—Not later than December 18, 2018, the
18 Comptroller General shall conduct a study and publish a report on the effec-
19 tiveness of the approach and strategy of the Federal Government to secur-
20 ing agency information systems, including the intrusion detection and pre-
21 vention capabilities and the intrusion assessment plan.

22 (c) REPORTS TO CONGRESS.—

23 (1) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—

24 (A) SECRETARY.—The Secretary not later than June 18 each
25 year shall submit to the appropriate congressional committees a
26 report on the status of the implementation of the intrusion detec-
27 tion and prevention capabilities, including—

28 (i) a description of privacy controls;

29 (ii) a description of the technologies and capabilities uti-
30 lized to detect cybersecurity risks in network traffic, including
31 the extent to which those technologies and capabilities include
32 existing commercial and noncommercial technologies;

33 (iii) a description of the technologies and capabilities uti-
34 lized to prevent network traffic associated with cybersecurity
35 risks from transiting or traveling to or from agency informa-
36 tion systems, including the extent to which those technologies
37 and capabilities include existing commercial and noncomm-
38 ercial technologies;

39 (iv) a list of the types of indicators or other identifiers or
40 techniques used to detect cybersecurity risks in network traf-
41 fic transiting or traveling to or from agency information sys-

1 tems on each iteration of the intrusion detection and preven-
2 tion capabilities, and the number of each type of indicator,
3 identifier, and technique;

4 (v) the number of instances in which the intrusion detec-
5 tion and prevention capabilities detected a cybersecurity risk
6 in network traffic transiting or traveling to or from agency
7 information systems and the number of times the intrusion
8 detection and prevention capabilities blocked network traffic
9 associated with cybersecurity risk; and

10 (vi) a description of the pilot established under section
11 10711(e)(5) of this title, including the number of new tech-
12 nologies tested and the number of participating agencies.

13 (B) DIRECTOR.—Not later than June 18, 2017, and annually
14 thereafter, the Director shall submit to Congress, as part of the
15 report required under section 3553(c) of title 44, an analysis of
16 agency application of the intrusion detection and prevention capa-
17 bilities, including—

18 (i) a list of each agency and the degree to which each agen-
19 cy has applied the intrusion detection and prevention capabili-
20 ties to an agency information system; and

21 (ii) a list by agency of—

22 (I) the number of instances in which the intrusion de-
23 tection and prevention capabilities detected a cybersecuri-
24 ty risk in network traffic transiting or traveling to or
25 from an agency information system and the types of in-
26 dicators, identifiers, and techniques used to detect the
27 cybersecurity risks; and

28 (II) the number of instances in which the intrusion de-
29 tection and prevention capabilities prevented network
30 traffic associated with a cybersecurity risk from
31 transiting or traveling to or from an agency information
32 system and the types of indicators, identifiers, and tech-
33 niques used to detect the agency information systems.

34 (C) CHIEF INFORMATION OFFICER.—Not earlier than June 18,
35 2017, and not later than December 18, 2017, the Federal Chief
36 Information Officer shall review and submit to the appropriate
37 congressional committees a report assessing the intrusion detection
38 and intrusion prevention capabilities, including—

39 (i) the effectiveness of the system in detecting, disrupting,
40 and preventing cyber-threat actors, including advanced per-

1 sistent threats, from accessing agency information and agency
2 information systems;

3 (ii) whether the intrusion detection and prevention capabili-
4 ties, continuous diagnostics and mitigation, and other systems
5 deployed under subtitle C of title II of the Homeland Security
6 Act of 2002 (Public Law 107–296, 116 Stat. 2155) are effec-
7 tive in securing Federal information systems;

8 (iii) the costs and benefits of the intrusion detection and
9 prevention capabilities, including as compared to commercial
10 technologies and tools and including the value of classified
11 cyber threat indicators; and

12 (iv) the capability of agencies to protect sensitive cyber
13 threat indicators and defensive measures if they were shared
14 through unclassified mechanisms for use in commercial tech-
15 nologies and tools.

16 (2) DEVELOPMENT AND IMPLEMENTATION OF INTRUSION ASSESS-
17 MENT PLAN, ADVANCED INTERNAL DEFENSES, AND FEDERAL CYBER-
18 SECURITY REQUIREMENTS.—The Director—

19 (A) 30 days after any update to the intrusion assessment plan,
20 shall submit the intrusion assessment plan to the appropriate con-
21 gressional committees;

22 (B) not later than December 18, 2016, and annually thereafter,
23 shall submit to Congress, as part of the report required under sec-
24 tion 3553(c) of title 44—

25 (i) a description of the implementation of the intrusion as-
26 sessment plan;

27 (ii) the findings of the intrusion assessments conducted
28 pursuant to the intrusion assessment plan;

29 (iii) a description of the advanced network security tools in-
30 cluded in the efforts to continuously diagnose and mitigate
31 cybersecurity risks pursuant to section 10802(a)(1) of this
32 title; and

33 (iv) a list by agency of compliance with the requirements
34 of section 10803(b) of this title; and

35 (C) not later than December 18, 2016, shall submit to the ap-
36 propriate congressional committees—

37 (i) a copy of the plan developed pursuant to section
38 10802(a)(2) of this title; and

39 (ii) the improved metrics developed pursuant to section
40 10802(c) of this title.

1 (3) TERMINATION.—The requirements under this subsection termi-
2 nate on September 30, 2023.

3 (d) FORM.—Each report required under this section shall be submitted
4 in unclassified form, but may include a classified annex.

5 **§ 10805. Report of security vulnerabilities on appropriate in-**
6 **formation systems**

7 (a) DEFINITIONS.—In this section:

8 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
9 priate congressional committees” means—

10 (A) the Committee on Homeland Security, the Committee on
11 Armed Services, the Committee on Energy and Commerce, and
12 the Permanent Select Committee on Intelligence of the House of
13 Representatives; and

14 (B) the Committee on Homeland Security and Governmental
15 Affairs, the Committee on Armed Services, the Committee on
16 Commerce, Science, and Transportation, and the Select Committee
17 on Intelligence of the Senate.

18 (2) APPROPRIATE INFORMATION SYSTEM.—The term “ appropriate
19 information system” means an information system that the Secretary
20 selects for inclusion under the vulnerability disclosure policy required
21 by subsection (b).

22 (3) INFORMATION SYSTEM.—The term “information system” has the
23 meaning given the term by section 3502 of title 44.

24 (4) SECURITY VULNERABILITY.—The term “security vulnerability”
25 has the meaning given the term in section 10801 of this title.

26 (b) VULNERABILITY DISCLOSURE POLICY.—The Secretary shall establish
27 a policy applicable to individuals, organizations, and companies that report
28 security vulnerabilities on appropriate information systems of the Depart-
29 ment. The policy shall include the following:

30 (1) The appropriate information systems of the Department that in-
31 dividuals, organizations, and companies may use to discover and report
32 security vulnerabilities on appropriate information systems.

33 (2) The conditions and criteria under which individuals, organiza-
34 tions, and companies may operate to discover and report security
35 vulnerabilities.

36 (3) How individuals, organizations, and companies may disclose to
37 the Department security vulnerabilities discovered on appropriate infor-
38 mation systems of the Department.

39 (4) The ways in which the Department may communicate with indi-
40 viduals, organizations, and companies that report security
41 vulnerabilities.

1 (5) The process the Department shall use for public disclosure of re-
2 ported security vulnerabilities.

3 (c) MITIGATION OR REMEDIATION PROCESS.—The Secretary shall de-
4 velop a process for the Department to address the mitigation or remediation
5 of the security vulnerabilities reported through the policy developed in sub-
6 section (b).

7 (d) CONSULTATION.—

8 (1) IN GENERAL.—In developing the security vulnerability disclosure
9 policy under subsection (b), the Secretary shall consult with the fol-
10 lowing:

11 (A) The Attorney General regarding how to ensure that individ-
12 uals, organizations, and companies that comply with the require-
13 ments of the policy developed under subsection (b) are protected
14 from prosecution under section 1030 of title 18, civil lawsuits, and
15 similar provisions of law with respect to specific activities author-
16 ized under the policy.

17 (B) The Secretary of Defense and the Administrator of General
18 Services regarding lessons that may be applied from existing vul-
19 nerability disclosure policies.

20 (C) Non-governmental security researchers.

21 (2) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of
22 title 5 shall not apply to any consultation under this subsection.

23 (e) PUBLIC AVAILABILITY.—The Secretary shall make the policy devel-
24 oped under subsection (b) publicly available.

25 (f) SUBMISSION TO CONGRESS.—

26 (1) DISCLOSURE POLICY AND MITIGATION OR REMEDIATION PROC-
27 ESS.—Not later than 90 days after December 21, 2018, the Secretary
28 shall submit to the appropriate congressional committees a copy of the
29 policy required under subsection (b) and the process required under
30 subsection (c).

31 (2) REPORT AND BRIEFING.—

32 (A) REPORT.—Not later than 1 year after establishing the pol-
33 icy required under subsection (b), the Secretary shall submit to
34 the appropriate congressional committees a report on the policy
35 and the process required under subsection (c).

36 (B) ANNUAL BRIEFING.—One year after the date of the submis-
37 sion of the report under subparagraph (A) and annually thereafter
38 for each of the next 3 years, the Secretary shall provide to the ap-
39 propriate congressional committees a briefing on the policy re-
40 quired under subsection (b) and the process required under sub-
41 section (c).

1 (C) MATTERS FOR INCLUSION.—The report required under sub-
2 paragraph (A) and the briefings required under subparagraph (B)
3 shall include the following with respect to the policy required
4 under subsection (b) and the process required under subsection (c)
5 for the period covered:

6 (i) The number of unique vulnerabilities reported.

7 (ii) The number of previously unknown security
8 vulnerabilities mitigated or remediated.

9 (iii) The number of unique individuals, organizations, and
10 companies that reported security vulnerabilities.

11 (iv) The average length of time between the reporting of
12 security vulnerabilities and mitigation or remediation of the
13 vulnerabilities.

14 **§ 10806. Bug bounty pilot program**

15 (a) DEFINITIONS.—In this section:

16 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
17 priate congressional committees” means—

18 (A) the Committee on Homeland Security and Governmental
19 Affairs of the Senate.

20 (B) the Select Committee on Intelligence of the Senate.

21 (C) the Committee on Homeland Security of the House of Rep-
22 resentatives; and

23 (D) the Permanent Select Committee on Intelligence of the
24 House of Representatives.

25 (2) BUG BOUNTY PROGRAM.—The term “bug bounty program”
26 means a program under which—

27 (A) individuals, organizations, and companies are temporarily
28 authorized to identify and report vulnerabilities of appropriate in-
29 formation systems of the Department; and

30 (B) eligible individuals, organizations, and companies receive
31 compensation in exchange for the reports.

32 (3) ELIGIBLE INDIVIDUAL, ORGANIZATION, OR COMPANY.—The term
33 “eligible individual, organization, or company” means an individual, or-
34 ganization, or company that meets such criteria as the Secretary deter-
35 mines in order to receive compensation in compliance with Federal
36 laws.

37 (4) INFORMATION SYSTEM.—The term “information system” has the
38 meaning given the term in section 3502 of title 44.

39 (5) PILOT PROGRAM.—The term “pilot program” means the bug
40 bounty program required to be established under subsection (b).

41 (b) ESTABLISHMENT.—

1 (1) IN GENERAL.—Not later than 180 days after December 21,
2 2018, the Secretary shall establish, in the Office of the Chief Informa-
3 tion Officer, a bug bounty pilot program to minimize vulnerabilities of
4 appropriate information systems of the Department.

5 (2) AUTHORITY TO AWARD CONTRACT TO MANAGE PROGRAM.—In es-
6 tablishing the pilot program, the Secretary, subject to the availability
7 of appropriations, may award 1 or more competitive contracts to an en-
8 tity, as necessary, to manage the pilot program.

9 (c) RESPONSIBILITIES OF SECRETARY.—In establishing and conducting
10 the pilot program, the Secretary shall—

11 (1) designate appropriate information systems to be included in the
12 pilot program;

13 (2) provide compensation to eligible individuals, organizations, and
14 companies for reports of previously unidentified security vulnerabilities
15 in the information systems designated under paragraph (1);

16 (3) establish criteria for individuals, organizations, and companies to
17 be considered eligible for compensation under the pilot program in com-
18 pliance with Federal laws;

19 (4) consult with the Attorney General on how to ensure that ap-
20 proved individuals, organizations, and companies that comply with the
21 requirements of the pilot program are protected from prosecution under
22 section 1030 of title 18 and similar provisions of law, and from civil
23 lawsuits, for specific activities authorized under the pilot program;

24 (5) consult with the Secretary of Defense and the heads of other de-
25 partments and agencies that have implemented programs to provide
26 compensation for reports of previously undisclosed vulnerabilities in in-
27 formation systems, regarding lessons that may be applied from the pro-
28 grams;

29 (6) develop an expeditious process by which an individual, organiza-
30 tion, or company can register with the Department, submit to a back-
31 ground check as determined by the Department, and receive a deter-
32 mination as to eligibility; and

33 (7) engage, as constructive and to the extent practicable, qualified
34 interested persons, including non-government sector representatives,
35 about the structure of the pilot program.

36 (d) REPORT TO CONGRESS.—Not later than 180 days after the date on
37 which the pilot program is completed, the Secretary shall submit to the ap-
38 propriate congressional committees a report on the pilot program, which
39 shall include—

- 1 (1) the number of individuals, the number of organizations, and the
2 number of companies that participated in the pilot program, broken
3 down by the number of individuals, organizations, or companies that—
4 (A) registered;
5 (B) were determined eligible;
6 (C) submitted security vulnerabilities; and
7 (D) received compensation;
- 8 (2) the number and severity of vulnerabilities reported as part of the
9 pilot program;
- 10 (3) the number of previously unidentified security vulnerabilities re-
11 mediated as a result of the pilot program;
- 12 (4) the current number of outstanding previously unidentified
13 vulnerabilities and Department remediation plans;
- 14 (5) the average length of time between the reporting of security
15 vulnerabilities and remediation of the vulnerabilities;
- 16 (6) the type of compensation provided under the pilot program; and
17 (7) the lessons learned from the pilot program.

18 **§ 10807. Pilot program on public-private partnerships with**
19 **internet ecosystem companies to detect and dis-**
20 **rupt adversary cyber operations**

21 (a) DEFINITIONS.—In this section:

22 (1) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appropri-
23 ate committees of Congress” means—

24 (A) the Committee on Homeland Security and Governmental
25 Affairs and the Committee on Armed Services of the Senate; and

26 (B) the Committee on Homeland Security and the Committee
27 on Armed Services of the House of Representatives.

28 (2) INTERNET ECOSYSTEM COMPANY.—The term “internet ecosystem
29 company” means a business incorporated in the United States that
30 provides cybersecurity services, internet service, content delivery serv-
31 ices, Domain Name Service, cloud services, mobile telecommunications
32 services, email and messaging services, internet browser services, or
33 such other services as the Secretary determines appropriate for the
34 purposes of the pilot program under subsection (b).

35 (b) IN GENERAL.—Not later than December 27, 2022, the Secretary, act-
36 ing through the Director of the Cybersecurity and Infrastructure Security
37 Agency and in coordination with the Secretary of Defense and the National
38 Cyber Director, shall commence a pilot program to assess the feasibility and
39 advisability of entering into public-private partnerships with internet eco-
40 system companies to facilitate, within the bounds of applicable provisions of
41 law and those companies’ terms of service, policies, procedures, contracts,

1 and other agreements, actions by those companies to discover and disrupt
2 use by malicious cyber actors of the platforms, systems, services, and infra-
3 structure of those companies.

4 (c)PUBLIC-PRIVATE PARTNERSHIPS.—

5 (1)IN GENERAL.—In carrying out the pilot program under sub-
6 section (b), the Secretary shall seek to enter into one or more public-
7 private partnerships with internet ecosystem companies.

8 (2)VOLUNTARY PARTICIPATION.—

9 (A)IN GENERAL.—Participation by an internet ecosystem com-
10 pany in a public-private partnership under the pilot program, in-
11 cluding in any activity described in subsection (d), shall be vol-
12 untary.

13 (B)PROHIBITION.—No funds appropriated by any Act may be
14 used to direct, pressure, coerce, or otherwise require that any
15 internet ecosystem company take any action on their platforms,
16 systems, services, or infrastructure as part of the pilot program.

17 (d)Authorized Activities.—In carrying out the pilot program under sub-
18 section (b), the Secretary may—

19 (1) provide assistance to a participating internet ecosystem company
20 to develop effective know-your-customer processes and requirements;

21 (2) provide information, analytics, and technical assistance to im-
22 prove the ability of participating companies to detect and prevent illicit
23 or suspicious procurement, payment, and account creation on their own
24 platforms, systems, services, or infrastructure;

25 (3) develop and socialize best practices for the collection, retention,
26 and sharing of data by participating internet ecosystem companies to
27 support discovery of malicious cyber activity, investigations, and attri-
28 bution on the platforms, systems, services, or infrastructure of those
29 companies;

30 (4) provide to participating internet ecosystem companies actionable,
31 timely, and relevant information, such as information about ongoing
32 operations and infrastructure, threats, tactics, and procedures, and in-
33 dicators of compromise, to enable those companies to detect and dis-
34 rupt the use by malicious cyber actors of the platforms, systems, serv-
35 ices, or infrastructure of the companies;

36 (5) provide recommendations for (but not design, develop, install, op-
37 erate, or maintain) operational workflows, assessment and compliance
38 practices, and training that participating internet ecosystem companies
39 can implement to reliably detect and disrupt the use by malicious cyber
40 actors of the platforms, systems, services, or infrastructure of the com-
41 panies;

1 (6) provide recommendations for accelerating, to the greatest extent
2 practicable, the automation of existing or implemented operational
3 workflows to operate at line-rate to enable real-time mitigation without
4 the need for manual review or action;

5 (7) provide recommendations for (but not design, develop, install, op-
6 erate, or maintain) technical capabilities to enable participating inter-
7 net ecosystem companies to collect and analyze data on malicious ac-
8 tivities occurring on the platforms, systems, services, or infrastructure
9 of those companies to detect and disrupt operations of malicious cyber
10 actors; and

11 (8) provide recommendations regarding relevant mitigations for sus-
12 pected or discovered malicious cyber activity and thresholds for action.

13 (e)COMPETITION CONCERNS.—Consistent with section 1905 of title 18, the
14 Secretary shall ensure that any trade secret or proprietary information of
15 a participating internet ecosystem company made known to the Federal
16 Government pursuant to a public-private partnership under the pilot pro-
17 gram remains private and protected unless explicitly authorized by the com-
18 pany.

19 (f)IMPARTIALITY.—In carrying out the pilot program under subsection
20 (b), the Secretary may not take any action that is intended primarily to ad-
21 vance the particular business interests of an internet ecosystem company
22 but may take actions that advance the interests of the United States, not-
23 withstanding differential impact or benefit to a given company's or given
24 companies' business interests.

25 (g)RESPONSIBILITIES.—

26 (1)SECRETARY.—The Secretary shall exercise primary responsibility
27 for the pilot program under subsection (b), including organizing and
28 directing authorized activities with participating Federal Government
29 organizations and internet ecosystem companies to achieve the objec-
30 tives of the pilot program.

31 (2)NATIONAL CYBER DIRECTOR.—The National Cyber Director shall
32 support prioritization and cross-agency coordination for the pilot pro-
33 gram, including ensuring appropriate participation by participating
34 agencies and the identification and prioritization of key private sector
35 entities and initiatives for the pilot program.

36 (3)SECRETARY OF DEFENSE.—The Secretary of Defense shall pro-
37 vide support and resources to the pilot program, including the provision
38 of technical and operational expertise drawn from appropriate and rel-
39 evant officials and components of the Department of Defense, including
40 the National Security Agency, United States Cyber Command, the
41 Chief Information Officer, the Office of the Secretary of Defense, mili-

1 tary department Principal Cyber Advisors, and the Defense Advanced
2 Research Projects Agency.

3 (h)PARTICIPATION OF OTHER FEDERAL GOVERNMENT COMPONENTS.—
4 The Secretary may invite to participate in the pilot program required under
5 subsection (b) the heads of such departments or agencies as the Secretary
6 considers appropriate.

7 (i)Integration With Other Efforts.—THE SECRETARY SHALL ENSURE
8 THAT THE PILOT PROGRAM REQUIRED UNDER SUBSECTION (B) MAKES USE
9 OF, BUILDS ON, AND, AS APPROPRIATE, INTEGRATES WITH AND DOES NOT
10 DUPLICATE OTHER EFFORTS OF THE DEPARTMENT AND THE DEPARTMENT
11 OF DEFENSE RELATING TO CYBERSECURITY, INCLUDING THE FOLLOWING:

12 (1) The Joint Cyber Defense Collaborative of the Cybersecurity and
13 Infrastructure Security Agency.

14 (2) The Cybersecurity Collaboration Center and Enduring Security
15 Framework of the National Security Agency.

16 (j)RULES OF CONSTRUCTION.—

17 (1)LIMITATION ON GOVERNMENT ACCESS TO DATA.—Nothing in this
18 section authorizes sharing of information, including information relat-
19 ing to customers of internet ecosystem companies or private individ-
20 uals, from an internet ecosystem company to an agency, officer, or em-
21 ployee of the Federal Government unless otherwise authorized by an-
22 other provision of law.

23 (2)STORED COMMUNICATIONS ACT.—Nothing in this section may be
24 construed to permit or require disclosure by a provider of a remote
25 computing service or a provider of an electronic communication service
26 to the public of information not otherwise permitted or required to be
27 disclosed underchapter 121 of title 18(commonly known as the “Stored
28 Communications Act”).

29 (3)THIRD PARTY CUSTOMERS.—Nothing in this section may be con-
30 strued to require a third party, such as a customer or managed service
31 provider of an internet ecosystem company, to participate in the pilot
32 program under subsection (b).

33 (k)ANNUAL BRIEFINGS.—

34 (1) IN GENERAL.—Not later than two years after December 27,
35 2023 and annually thereafter for 3 years, the Secretary, in coordina-
36 tion with the Secretary of Defense and the National Cyber Director,
37 shall brief the appropriate committees of Congress on the progress of
38 the pilot program required under subsection (b).

39 (2)ELEMENTS.—Each briefing required under paragraph (1) shall
40 include the following:

1 (A) Recommendations for addressing relevant policy, budgetary, and
2 legislative gaps to increase the effectiveness of the pilot program.

3 (B) Recommendations, such as providing liability protection, for
4 increasing private sector participation in the pilot program.

5 (C) A description of the challenges encountered in carrying out
6 the pilot program, including any concerns expressed by internet
7 ecosystem companies regarding participation in the pilot program.

8 (D) The findings of the Secretary with respect to the feasibility
9 and advisability of extending or expanding the pilot program.

10 (E) Such other matters as the Secretary considers appropriate.

11 (l)TERMINATION.—The pilot program required under subsection (b) shall
12 terminate on December 27, 2026.

13 **§ 10808. CyberSentry program**

14 (a) Definition of Industrial Control System.—In this section, the term
15 “industrial control system” means an information system used to monitor
16 and control industrial processes such as manufacturing, product handling,
17 production, and distribution, including supervisory control and data acquisi-
18 tion (SCADA) systems used to monitor and control geographically dispersed
19 assets, distributed control systems (DCSs), Human-Machine Interfaces
20 (HMIs), and programmable logic controllers that control localized processes.

21 (b) ESTABLISHMENT.—There is in the Agency a program, to be known
22 as “CyberSentry”, to provide continuous monitoring and detection of cyber-
23 security risks to critical infrastructure entities that own or operate indus-
24 trial control systems that support national critical functions, on request and
25 subject to the consent of the owner or operator.

26 (c) ACTIVITIES.—The Director, through CyberSentry, shall—

27 (1) enter into strategic partnerships with critical infrastructure own-
28 ers and operators that, in the determination of the Director and subject
29 to the availability of resources, own or operate regionally or nationally
30 significant industrial control systems that support national critical
31 functions, in order to provide technical assistance in the form of contin-
32 uous monitoring of industrial control systems and the information sys-
33 tems that support the systems and detection of cybersecurity risks to
34 the industrial control systems and other cybersecurity services, as ap-
35 propriate, based on and subject to the agreement and consent of the
36 owner or operator;

37 (2) leverage sensitive or classified intelligence about cybersecurity
38 risks regarding particular sectors, particular adversaries, and trends in
39 tactics, techniques, and procedures to advise critical infrastructure
40 owners and operators regarding mitigation measures and share infor-
41 mation as appropriate;

1 (3) identify cybersecurity risks in the information technology and in-
2 formation systems that support industrial control systems that could be
3 exploited by adversaries attempting to gain access to the industrial con-
4 trol systems, and work with owners and operators to remediate the
5 vulnerabilities;

6 (4) produce aggregated, anonymized analytic products, based on
7 threat hunting and continuous monitoring and detection activities and
8 partnerships, with findings and recommendations that can be dissemi-
9 nated to critical infrastructure owners and operators; and

10 (5) support activities authorized in accordance with section 1501 of
11 the National Defense Authorization Act for Fiscal Year 2022 (Public
12 Law 117–81, 135 Stat. 2020).

13 (d) PRIVACY REVIEW.—Not later than 180 days after December 27,
14 2021, the Privacy Officer of the Agency undersection 10304(d) of this
15 title shall review the policies, guidelines, and activities of CyberSentry for
16 compliance with all applicable privacy laws, including the laws governing the
17 acquisition, interception, retention, use, and disclosure of communities.

18 (e) REPORTS TO CONGRESS.—

19 (1) COMPLIANCE WITH PRIVACY LAWS.—Not later than 180 days
20 after December 27, 2021, the Privacy Officer of the Agency undersec-
21 tion 10304(d) of this title shall submit to the Committee on Homeland
22 Security of the House of Representatives and the Committee on Home-
23 land Security and Governmental Affairs of the Senate a report certi-
24 fying compliance with all applicable privacy laws as referred to in para-
25 graph (1) or identifying any instances of noncompliance with those pri-
26 vacy laws.

27 (2) IMPLEMENTATION.—Not later than December 27, 2022, the Di-
28 rector shall provide to the Committee on Homeland Security of the
29 House of Representatives and the Committee on Homeland Security
30 and Governmental Affairs of the Senate a briefing and written report
31 on implementation of this section.

32 (f) RULE OF CONSTRUCTION.—Nothing in this section may be construed
33 to permit the Federal Government to gain access to information of a remote
34 computing service provider to the public or an electronic service provider to
35 the public, the disclosure of which is not permitted undersection 2702 of
36 title 18.

37 (g) TERMINATION.—The authority to carry out a program under this sec-
38 tion shall terminate on December 27, 2028.

39 **§ 10809. Inventory of cryptographic systems; migration to**
40 **post-quantum cryptography**

41 (a) DEFINITIONS.—In this section:

1 (1) AGENCY.—The term “agency”—

2 (A) means any executive department, military department, Gov-
3 ernment corporation, Government controlled corporation, or other
4 establishment in the executive branch of the Government (includ-
5 ing the Executive Office of the President), or any independent reg-
6 ulatory agency; and

7 (B) does not include—

8 (i) the Government Accountability Office; or

9 (ii) the governments of the District of Columbia and of the
10 territories (including possessions) of the United States, and
11 their various subdivisions.

12 (2) CLASSICAL COMPUTER.—The term “classical computer” means a
13 device that accepts digital data and manipulates the information based
14 on a program or sequence of instructions for how data is to be pro-
15 cessed and encodes information in binary bits that can either be 0s or
16 1s.

17 (3) DIRECTOR OF CISA.—The term “Director of CISA” means the Di-
18 rector of the Cybersecurity and Infrastructure Security Agency.

19 (4) DIRECTOR OF NIST.—The term “Director of NIST” means the
20 Director of the National Institute of Standards and Technology.

21 (5) DIRECTOR OF OMB.—The term “Director of OMB” means the
22 Director of the Office of Management and Budget.

23 (6) INFORMATION TECHNOLOGY.—The term “information tech-
24 nology” has the meaning given the term in section 3502 of title 44.

25 (7) NATIONAL SECURITY SYSTEM.—The term “national security sys-
26 tem” has the meaning given the term in section 3552 of title 44.

27 (8) POST-QUANTUM CRYPTOGRAPHY.—The term “post-quantum cryp-
28 tography” means those cryptographic algorithms or methods that are
29 assessed not to be specifically vulnerable to attack by either a quantum
30 computer or classical computer.

31 (9) QUANTUM COMPUTER.—The term “quantum computer” means a
32 computer that uses the collective properties of quantum states, such as
33 superposition, interference, and entanglement, to perform calculations.

34 (b) INVENTORY.—

35 (1) ESTABLISHMENT.—Not later than 180 days after December 21,
36 2022, the Director of OMB, in coordination with the National Cyber
37 Director and in consultation with the Director of CISA, shall issue
38 guidance on the migration of information technology to post-quantum
39 cryptography, which shall include at a minimum—

40 (A) a requirement for each agency to establish and maintain a
41 current inventory of information technology in use by the agency

1 that is vulnerable to decryption by quantum computers, prioritized
2 using the criteria described in subparagraph (B);

3 (B) criteria to allow agencies to prioritize their inventory ef-
4 forts; and

5 (C) a description of the information required to be reported pur-
6 suant to subsection (e).

7 (2) ADDITIONAL CONTENT IN GUIDANCE.—In the guidance estab-
8 lished by paragraph (1), the Director of OMB shall include, in addition
9 to the requirements described in that paragraph—

10 (A) a description of information technology to be prioritized for
11 migration to post-quantum cryptography; and

12 (B) a process for evaluating progress on migrating information
13 technology to post-quantum cryptography, which shall be auto-
14 mated to the greatest extent practicable.

15 (3) PERIODIC UPDATES.—The Director of OMB shall update the
16 guidance required under paragraph (1) as the Director of OMB deter-
17 mines necessary, in coordination with the National Cyber Director and
18 in consultation with the Director of CISA.

19 (e) AGENCY REPORTS.—Not later than December 21, 2023, and on an
20 ongoing basis thereafter, the head of each agency shall provide to the Direc-
21 tor of OMB, the Director of CISA, and the National Cyber Director—

22 (1) the inventory described in subsection (b)(1); and

23 (2) any other information required to be reported under subsection
24 (b)(1)(C).

25 (d) MIGRATION AND ASSESSMENT.—Not later than 1 year after the date
26 on which the Director of NIST has issued post-quantum cryptography
27 standards, the Director of OMB shall issue guidance requiring each agency
28 to—

29 (1) prioritize information technology described under subsection
30 (b)(2)(A) for migration to post-quantum cryptography; and

31 (2) develop a plan to migrate information technology of the agency
32 to post-quantum cryptography consistent with the prioritization under
33 paragraph (1).

34 (e) INTEROPERABILITY.—The Director of OMB shall ensure that the
35 prioritizations made under subsection (d)(1) are assessed and coordinated
36 to ensure interoperability.

37 (f) OFFICE OF MANAGEMENT AND BUDGET REPORTS.—

38 (1) Report on post-quantum cryptography.—Not later than 15
39 months after December 21, 2022, the Director of OMB, in coordina-
40 tion with the National Cyber Director and in consultation with the Di-
41 rector of CISA, shall submit to the Committee on Homeland Security

1 and Governmental Affairs of the Senate and the Committee on Over-
2 sight and Reform of the House of Representatives a report on the fol-
3 lowing:

4 (A) A strategy to address the risk posed by the vulnerabilities
5 of information technology of agencies to weakened encryption due
6 to the potential and possible capability of a quantum computer to
7 breach that encryption.

8 (B) An estimate of the amount of funding needed by agencies
9 to secure the information technology described in subsection
10 (b)(1)(A) from the risk posed by an adversary of the United
11 States using a quantum computer to breach the encryption of the
12 information technology.

13 (C) A description of Federal civilian executive branch coordina-
14 tion efforts led by the National Institute of Standards and Tech-
15 nology, including timelines, to develop standards for post-quantum
16 cryptography, including any Federal Information Processing
17 Standards developed underchapter 35 of title 44, as well as stand-
18 ards developed through voluntary, consensus standards bodies
19 such as the International Organization for Standardization.

20 (2) REPORT ON MIGRATION TO POST-QUANTUM CRYPTOGRAPHY IN
21 INFORMATION TECHNOLOGY.—Not later than 1 year after the date on
22 which the Director of OMB issues guidance under subsection (d)(2),
23 and thereafter until the date that is 5 years after the date on which
24 post-quantum cryptographic standards are issued, the Director of
25 OMB, in coordination with the National Cyber Director and in con-
26 sultation with the Director of CISA, shall submit to the Committee on
27 Homeland Security and Governmental Affairs of the Senate and the
28 Committee on Oversight and Reform of the House of Representatives,
29 with the report submitted pursuant tosection 3553(c) of title 44, a re-
30 port on the progress of agencies in adopting post-quantum cryptog-
31 raphy standards.

32 **§ 10810. Competition relating to cybersecurity**
33 **vulnerabilities**

34 The Under Secretary for Science and Technology of the Department, in
35 consultation with the Director, may establish an incentive-based program
36 that allows industry, individuals, academia, and others to compete in identi-
37 fying remediation solutions for cybersecurity vulnerabilities (as that term is
38 defined in section 10706 of this title) to information systems (as that term
39 is defined in section 10701 of this title) and industrial control systems, in-
40 cluding supervisory control and data acquisition systems.

1 **§ 10811. Ransomware threat mitigation activities**

2 (a) DEFINITIONS.—In this section:

3 (1) SECTION 10701 DEFINITIONS.—The terms “Director”, “informa-
4 tion system”, “ransomware attack”, and “security vulnerability” have
5 the meanings given those terms in section 10701 of this title.

6 (2) SECTION 10761 DEFINITIONS.—The terms “covered cyber inci-
7 dent”, “covered entity”, “cyber incident”, and “ransom payment” have
8 the meanings given those terms in section 10761 of this title.

9 (b) JOINT RANSOMWARE TASK FORCE.—

10 (1) ESTABLISHMENT.—The Director, in consultation with the Na-
11 tional Cyber Director, the Attorney General, and the Director of the
12 Federal Bureau of Investigation, shall establish and chair the Joint
13 Ransomware Task Force to coordinate an ongoing nationwide cam-
14 paign against ransomware attacks, and identify and pursue opportuni-
15 ties for international cooperation.

16 (2) COMPOSITION.—The Joint Ransomware Task Force shall consist
17 of participants from Federal agencies, as determined appropriate by
18 the National Cyber Director in consultation with the Secretary.

19 (3) RESPONSIBILITIES.— The Joint Ransomware Task Force, uti-
20 lizing only existing authorities of each participating Federal agency,
21 shall coordinate across the Federal Government the following activities:

22 (A) Prioritizing intelligence-driven operations to disrupt specific
23 ransomware actors.

24 (B) Consulting with relevant private sector, State, local, Tribal,
25 and territorial governments and international stakeholders to iden-
26 tify needs and establish mechanisms for providing input into the
27 Joint Ransomware Task Force.

28 (C) Identifying, in consultation with relevant entities, a list of
29 highest threat ransomware entities updated on an ongoing basis,
30 to facilitate—j

31 (i) prioritization for Federal action by appropriate Federal
32 agencies; and

33 (ii) identification of metrics for success of the actions.

34 (D) Disrupting ransomware criminal actors, associated infra-
35 structure, and their finances.

36 (E) Facilitating coordination and collaboration between Federal
37 entities and relevant entities, including the private sector, to im-
38 prove Federal actions against ransomware threats.

39 (F) Collecting, sharing, and analyzing ransomware trends to in-
40 form Federal actions.

1 (G) Creating after-action reports and other lessons learned from
2 Federal actions that identify successes and failures to improve
3 subsequent actions.

4 (H) Any other activities determined appropriate by the Joint
5 Ransomware Task Force to mitigate the threat of ransomware at-
6 tacks.

7 (4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be
8 construed to provide any additional authority to any Federal agency.

9 (c) RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM

10 (1) ESTABLISHMENT.—Not later than March 15, 2023, the Director
11 shall establish a ransomware vulnerability warning pilot program to le-
12 verage existing authorities and technology to specifically develop proce-
13 sses and procedures for, and to dedicate resources to, identifying in-
14 formation systems that contain security vulnerabilities associated with
15 common ransomware attacks, and to notify the owners of those vulner-
16 able systems of their security vulnerability.

17 (2) IDENTIFICATION OF VULNERABLE SYSTEMS.—The pilot program
18 established under paragraph (1) shall—

19 (A) identify the most common security vulnerabilities utilized in
20 ransomware attacks and mitigation techniques; and

21 (B) utilize existing authorities to identify information systems
22 that contain the security vulnerabilities identified in subparagraph
23 (A).

24 (3) ENTITY NOTIFICATION.—

25 (A) IDENTIFICATION.—If the Director is able to identify the en-
26 tity at risk that owns or operates a vulnerable information system
27 identified in paragraph (2), the Director may notify the owner of
28 the information system.

29 (B) NO IDENTIFICATION.—If the Director is not able to identify
30 the entity at risk that owns or operates a vulnerable information
31 system identified in paragraph (2), the Director may utilize the
32 subpoena authority pursuant to section 10706 of this title to iden-
33 tify and notify the entity at risk pursuant to the procedures under
34 that section.

35 (C) REQUIRED INFORMATION.—A notification made under sub-
36 paragraph (A) shall include information on the identified security
37 vulnerability and mitigation techniques.

38 (4) PRIORITIZATION OF NOTIFICATIONS.—To the extent practicable,
39 the Director shall prioritize covered entities for identification and noti-
40 fication activities under the pilot program established under this sub-
41 section.

1 (5)LIMITATION ON PROCEDURES.—No procedure, notification, or
2 other authorities utilized in the execution of the pilot program estab-
3 lished under paragraph (1) shall require an owner or operator of a vul-
4 nerable information system to take any action as a result of a notice
5 of a security vulnerability made pursuant to paragraph (3).

6 (6)Rule of construction.—Nothing in this subsection shall be con-
7 strued to provide additional authorities to the Director to identify
8 vulnerabilities or vulnerable systems.

9 (7)TERMINATION.—The pilot program established under paragraph
10 (1) shall terminate on March 15, 2026.

11 **§ 10812. National cybersecurity preparedness consortium**

12 (a) DEFINITIONS.—In this section:

13 (1) COMMUNITY COLLEGE.—The term “community college” has the
14 meaning given the term “junior or community college” in section 312
15 of the Higher Education Act of 1965 (20 U.S.C. 1058).

16 (2) CONSORTIUM.—The term “consortium” means a group primarily
17 composed of nonprofit entities, including academic institutions, that de-
18 velop, update, and deliver cybersecurity training and education in sup-
19 port of homeland security.

20 (3) CYBERSECURITY RISK.—The term “cybersecurity risk” has the
21 meaning given the term in section 10701 of this title.

22 (4) HISPANIC-SERVING INSTITUTION.—The term “Hispanic-serving
23 institution” has the meaning given the term in section 502 of the
24 Higher Education Act of 1965 (20 U.S.C. 1101a).

25 (5) HISTORICALLY BLACK COLLEGE AND UNIVERSITY.—The term
26 “historically Black college and university” has the meaning given the
27 term “part B institution” in section 322 of the Higher Education Act
28 of 1965 (20 U.S.C. 1061).

29 (6) INCIDENT.—The term “incident” has the meaning given the
30 term in section 10701 of this title.

31 (7) MINORITY-SERVING INSTITUTION.—The term “minority-serving
32 institution” means an institution of higher education described in sec-
33 tion 371(a) of the Higher Education Act of 1965 (20 U.S.C.
34 1067q(a)).

35 (8) STATE.—The term “State” means a State, the District of Co-
36 lumbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, the
37 Northern Mariana Islands, and any possession of the United States.

38 (9) TRIBAL COLLEGES AND UNIVERSITIES.—The term “Tribal Col-
39 leges and Universities” has the meaning given the term in section 316
40 of the Higher Education Act of 1965 (20 U.S.C. 1059e).

1 (10) TRIBAL ORGANIZATION.—The term “Tribal organization” has
2 the meaning given the term in section 4 of the Indian Self-Determina-
3 tion and Education Assistance Act (25 U.S.C. 5304).

4 (b) IN GENERAL.—The Secretary may work with one or more consortia
5 to support efforts to address cybersecurity risks and incidents.

6 (c) ASSISTANCE TO CARRY OUT SECRETARY’S RESPONSIBILITIES.—The
7 Secretary may work with one or more consortia to carry out the Secretary’s
8 responsibility pursuant to section 10702(b)(1)(P) of this title to—

9 (1) provide training and education to State, Tribal, and local first
10 responders and officials specifically for preparing for and responding to
11 cybersecurity risks and incidents, in accordance with applicable law;

12 (2) develop and update a curriculum utilizing existing training and
13 educational programs and models, in accordance with section 10706 of
14 this title for State, Tribal, and local first responders and officials, re-
15 lated to cybersecurity risks and incidents;

16 (3) provide technical assistance services, training, and educational
17 programs to build and sustain capabilities in support of preparedness
18 for and response to cybersecurity risks and incidents, including threats
19 of acts of terrorism, in accordance with section 10706 of this title;

20 (4) conduct cross-sector cybersecurity training, education, and sim-
21 ulation exercises for entities, including State and local governments and
22 Tribal organizations, critical infrastructure owners and operators, and
23 private industry, to encourage community-wide coordination in defend-
24 ing against and responding to cybersecurity risks and incidents, in ac-
25 cordance with section 10707(c) of this title;

26 (5) help States, Tribal organizations, and communities develop cy-
27 bersecurity information sharing programs, in accordance with section
28 10706 of this title, for the dissemination of homeland security informa-
29 tion related to cybersecurity risks and incidents;

30 (6) help incorporate cybersecurity risk and incident prevention and
31 response into existing State, Tribal, and local emergency plans, includ-
32 ing continuity of operations plans; and

33 (7) assist State governments and Tribal organizations in developing
34 cybersecurity plans.

35 (d) CONSIDERATIONS REGARDING SELECTION OF A CONSORTIUM.—In
36 selecting a consortium with which to work under this section, the Secretary
37 shall take into consideration the following:

38 (1) Prior experience conducting cybersecurity training, education,
39 and exercises for State and local entities.

40 (2) Geographic diversity of the members of the consortium so as to
41 maximize coverage of the different regions of the United States.

1 viders using the process described in section 2(e) of the National Insti-
2 tute of Standards and Technology Act (15 U.S.C. 272(e)).

3 (2) REPORT.—The Director of the National Institute of Standards
4 and Technology shall submit to Congress a report on the result of the
5 activities of the Director under paragraph (1), including any methods
6 developed by the Director under paragraph (1), and shall make the re-
7 port publicly available on the website of the National Institute of
8 Standards and Technology.

9 (d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed
10 to—

11 (1) require a State to report data under subsection (a); or

12 (2) require a non-Federal entity (as defined in section 10801 of this
13 title) to—

14 (A) adopt a recommended measure developed under subsection
15 (b); or

16 (B) follow the result of the activities carried out under sub-
17 section (c), including any methods developed under subsection (c).

18 **§ 10822. Improving cybersecurity in the health care industry**

19 (a) DEFINITIONS.—In this section:

20 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
21 priate congressional committees” means—

22 (A) the Committee on Health, Education, Labor, and Pensions,
23 the Committee on Homeland Security and Governmental Affairs,
24 and the Select Committee on Intelligence of the Senate; and

25 (B) the Committee on Energy and Commerce, the Committee
26 on Homeland Security, and the Permanent Select Committee on
27 Intelligence of the House of Representatives.

28 (2) BUSINESS ASSOCIATE.—The term “business associate” has the
29 meaning given the term in section 160.103 of title 45, Code of Federal
30 Regulations (as in effect on December 17, 2015).

31 (3) COVERED ENTITY.—The term “covered entity” has the meaning
32 given the term in section 160.103 of title 45, Code of Federal Regula-
33 tions (as in effect on December 17, 2015).

34 (4) CYBERSECURITY THREAT; CYBER THREAT INDICATOR; DEFEN-
35 SIVE MEASURE; FEDERAL ENTITY.—The terms “cybersecurity threat”,
36 “cyber threat indicator”, “defensive measure”, and “Federal entity”
37 have the meanings given the terms in section 10781 of this title.

38 (5) HEALTH CARE CLEARINGHOUSE; HEALTH CARE PROVIDER;
39 HEALTH PLAN.—The terms “health care clearinghouse”, “health care
40 provider”, and “health plan” have the meanings given the terms in sec-

1 tion 160.103 of title 45, Code of Federal Regulations (as in effect on
2 December 17, 2015).

3 (6) HEALTH CARE INDUSTRY STAKEHOLDER.—The term “health
4 care industry stakeholder” means any—

5 (A) health plan, health care clearinghouse, or health care pro-
6 vider;

7 (B) advocate for patients or consumers;

8 (C) pharmacist;

9 (D) developer or vendor of health information technology;

10 (E) laboratory;

11 (F) pharmaceutical or medical device manufacturer; or

12 (G) additional stakeholder the Secretary determines necessary
13 for purposes of subsection (b)(1), (c)(1), (c)(3), or (d)(1).

14 (7) NON-FEDERAL ENTITY; PRIVATE ENTITY.—The terms “non-Fed-
15 eral entity” and “private entity” have the meanings given the terms
16 in section 10781 of this title.

17 (b) REPORT.—

18 (1) IN GENERAL.—Not later than December 18, 2016, the Secretary
19 of Health and Human Services shall submit to the Committee on
20 Health, Education, Labor, and Pensions of the Senate and the Com-
21 mittee on Energy and Commerce of the House of Representatives a re-
22 port on the preparedness of the Department of Health and Human
23 Services and health care industry stakeholders in responding to cyber-
24 security threats.

25 (2) CONTENTS OF REPORT.—With respect to the internal response
26 of the Department of Health and Human Services to emerging cyberse-
27 curity threats, the report under paragraph (1) shall include—

28 (A) a clear statement of the official in the Department of
29 Health and Human Services to be responsible for leading and co-
30 ordinating efforts of the Department of Health and Human Serv-
31 ices regarding cybersecurity threats in the health care industry;
32 and

33 (B) a plan from each relevant operating division and subdivision
34 of the Department of Health and Human Services on how the di-
35 vision or subdivision will address cybersecurity threats in the
36 health care industry, including a clear delineation of how the divi-
37 sion or subdivision will divide responsibility among the personnel
38 of the division or subdivision and communicate with other divisions
39 and subdivisions regarding efforts to address the threats.

40 (c) HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE.—

1 (1) IN GENERAL.—The Secretary of Health and Human Services, in
2 consultation with the Director of the National Institute of Standards
3 and Technology and the Secretary of Homeland Security, shall convene
4 health care industry stakeholders, cybersecurity experts, and any Fed-
5 eral agencies or entities the Secretary of Health and Human Services
6 determines appropriate to establish a task force to—

7 (A) analyze how industries, other than the health care industry,
8 have implemented strategies and safeguards for addressing cyber-
9 security threats in their respective industries;

10 (B) analyze challenges and barriers private entities (excluding
11 any State, tribal, or local government) in the health care industry
12 face securing themselves against cyberattacks;

13 (C) review challenges that covered entities and business associ-
14 ates face in securing networked medical devices and other software
15 or systems that connect to an electronic health record;

16 (D) provide the Secretary of Health and Human Services with
17 information to disseminate to health care industry stakeholders of
18 all sizes for purposes of improving their preparedness for, and re-
19 sponse to, cybersecurity threats affecting the health care industry;

20 (E) establish a plan for implementing Subchapter IV of this
21 chapter, so that the Federal Government and health care industry
22 stakeholders may in real time, share actionable cyber threat indi-
23 cators and defensive measures; and

24 (F) report to the appropriate congressional committees on the
25 findings and recommendations of the task force regarding carrying
26 out subparagraphs (A) through (E).

27 (2) TERMINATION.—The task force established under this subsection
28 shall terminate 1 year after the date on which the task force is estab-
29 lished.

30 (3) DISSEMINATION.—Not later than 60 days after the termination
31 of the task force established under this subsection, the Secretary of
32 Health and Human Services shall disseminate the information de-
33 scribed in paragraph (1)(D) to health care industry stakeholders in ac-
34 cordance with paragraph (1)(D).

35 (d) ALIGNING HEALTH CARE INDUSTRY SECURITY APPROACHES.—

36 (1) IN GENERAL.—The Secretary of Health and Human Services
37 shall establish, through a collaborative process with the Secretary of
38 Homeland Security, health care industry stakeholders, the Director of
39 the National Institute of Standards and Technology, and any Federal
40 entity or non-Federal entity the Secretary of Health and Human Serv-
41 ices determines appropriate, a common set of voluntary, consensus-

1 based, and industry-led guidelines, best practices, methodologies, proce-
2 dures, and processes that—

3 (A) serve as a resource for cost-effectively reducing cybersecu-
4 rity risks for a range of health care organizations;

5 (B) support voluntary adoption and implementation efforts to
6 improve safeguards to address cybersecurity threats;

7 (C) are consistent with—

8 (i) the standards, guidelines, best practices, methodologies,
9 procedures, and processes developed under section 2(c)(15) of
10 the National Institute of Standards and Technology Act (15
11 U.S.C. 272(c)(15));

12 (ii) the security and privacy regulations promulgated under
13 section 264(e) of the Health Insurance Portability and Ac-
14 countability Act of 1996 (42 U.S.C. 1320d–2 note); and

15 (iii) the Health Information Technology for Economic and
16 Clinical Health Act (Public Law 111–5, div. A, title XIII, div.
17 B, title IV, 123 Stat. 226, 467), and the amendments made
18 by the Act; and

19 (D) are updated on a regular basis and are applicable to a
20 range of health care organizations.

21 (2) LIMITATION.—Nothing in this subsection shall be interpreted as
22 granting the Secretary of Health and Human Services authority to—

23 (A) provide for audits to ensure that health care organizations
24 are in compliance with this subsection; or

25 (B) mandate, direct, or condition the award of any Federal
26 grant, contract, or purchase on compliance with this subsection.

27 (3) NO LIABILITY FOR NONPARTICIPATION.—Nothing in this section
28 shall be construed to subject a health care industry stakeholder to li-
29 ability for choosing not to engage in the voluntary activities authorized,
30 or guidelines developed, under this subsection.

31 (e) INCORPORATING ONGOING ACTIVITIES.—In carrying out the activities
32 under this section, the Secretary of Health and Human Services may incor-
33 porate activities that are ongoing as of December 17, 2015, and that are
34 consistent with the objectives of this section.

35 (f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed
36 to limit the antitrust exemption under section 10783(e) of this title or the
37 protection from liability under section 10785 of this title.

38 § 10823. K–12 education cybersecurity initiative

39 (a) DEFINITIONS.—In this section

40 (1) CYBERSECURITY RISK.—The term “cybersecurity risk” has the
41 meaning given the term in section 10701 of this title.

1 (2)DIRECTOR.—The term “Director” means the Director of Cyberse-
2 curity and Infrastructure Security.

3 (3)INFORMATION SYSTEM.—The term “information system” has the
4 meaning given the term in section 3502 of title 44.

5 (4) K12EDUCATIONAL INSTITUTION.—The term “K–12 educational
6 institution” means an elementary school or a secondary school, as those
7 terms are defined in section 8101 of the Elementary and Secondary
8 Education Act of 1965 (20 U.S.C. 7801).

9 (b) CYBERSECURITY RECOMMENDATIONS.—Not later than 60 days after
10 the completion of the study required under section 3(b)(1) of the K–12 Cy-
11 bersecurity Act of 2021 (Public Law 117–47, 135 Stat. 397), the Director,
12 in accordance with subsection (f)(1), shall develop recommendations that in-
13 clude cybersecurity guidelines designed to assist K–12 educational institu-
14 tions in facing the cybersecurity risks described in section 3(b)(1) of that
15 Act, using the findings of the study.

16 (c) ONLINE TRAINING TOOLKIT.—Not later than 120 days after the com-
17 pletion of the development of the recommendations required under sub-
18 section (b), the Director shall develop an online training toolkit designed for
19 officials at K–12 educational institutions to—

20 (1) educate the officials about the cybersecurity recommendations de-
21 veloped under subsection (b); and

22 (2) provide strategies for the officials to implement the recommenda-
23 tions developed under subsection (b).

24 (d) PUBLIC AVAILABILITY.—The Director shall make available on the
25 website of the Department with other information relating to school safety
26 the following:

27 (1) The findings of the study conducted under section 3(b)(1) of the
28 K–12 Cybersecurity Act of 2021 (Public Law 117–47, 135 Stat. 397).

29 (2) The cybersecurity recommendations developed under subsection
30 (b).

31 (3) The online training toolkit developed under subsection (c).

32 (e) VOLUNTARY USE.—The use of the cybersecurity recommendations de-
33 veloped under subsection (b) by K–12 educational institutions shall be vol-
34 untary.

35 (f)CONSULTATION.—

36 (1)IN GENERAL.—In the course of the development of the rec-
37 ommendations required under subsection (b), the Director shall consult
38 with individuals and entities focused on cybersecurity and education, as
39 appropriate, including—

40 (A) teachers;

41 (B) school administrators;

- 1 (C) Federal agencies;
2 (D) non-Federal cybersecurity entities with experience in edu-
3 cation issues; and
4 (E) private sector organizations.

5 (2) INAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of
6 title 5 shall not apply to any consultation under paragraph (1).

7 **§ 10824. Federal Clearinghouse on School Safety Evidence-**
8 **Based Practices**

9 (a) ESTABLISHMENT.—

10 (1) IN GENERAL.—The Secretary, in coordination with the Secretary
11 of Education, the Attorney General, and the Secretary of Health and
12 Human Services, shall establish a Federal Clearinghouse on School
13 Safety Evidence-Based Practices (in this section referred to as the
14 “Clearinghouse”) in the Department.

15 (2) PURPOSE.—The Clearinghouse shall serve as a Federal resource
16 to identify and publish online through SchoolSafety.gov, or any suc-
17 cessor website, evidence-based practices and recommendations to im-
18 prove school safety for use by State and local educational agencies, in-
19 stitutions of higher education, State and local law enforcement agen-
20 cies, health professionals, and the general public.

21 (3) PERSONNEL.—

22 (A) ASSIGNMENTS.—The Clearinghouse shall be assigned such
23 personnel and resources as the Secretary considers appropriate to
24 carry out this section.

25 (B) DETAILEES.— The Secretary of Education, the Attorney
26 General, and the Secretary of Health and Human Services may
27 detail personnel to the Clearinghouse.

28 (4) EXEMPTIONS.—

29 (A) CHAPTER 35 OF TITLE 44.— Chapter 35 of title 44 shall
30 not apply to any rulemaking or information collection required
31 under this section.

32 (B) CHAPTER 10 OF TITLE 5.—The Federal Advisory Committee
33 Act (5 U.S.C. App.)Chapter 10 of title 5 shall not apply for the
34 purposes of carrying out this section.

35 (b) CLEARINGHOUSE CONTENTS.—

36 (1) CONSULTATION.— In identifying the evidence-based practices
37 and recommendations for the Clearinghouse, the Secretary shall—

38 (A) consult with appropriate Federal, State, local, Tribal, pri-
39 vate sector, and nongovernmental organizations, including civil
40 rights and disability rights organizations; and

1 (B) consult with the Secretary of Education to ensure that evi-
2 dence-based practices published by the Clearinghouse are aligned
3 with evidence-based practices to support a positive and safe learn-
4 ing environment for all students.

5 (2) CRITERIA FOR EVIDENCE-BASED PRACTICES AND RECOMMENDA-
6 TIONS.— The evidence-based practices and recommendations of the
7 Clearinghouse shall—

8 (A) include comprehensive evidence-based school safety meas-
9 ures;

10 (B) include the evidence or research rationale supporting the de-
11 termination of the Clearinghouse that the evidence-based practice
12 or recommendation under subparagraph (A) has been shown to
13 have a significant effect on improving the health, safety, and wel-
14 fare of persons in school settings, including—

15 (i) relevant research that is evidence-based, as defined
16 in section 9101 of the Elementary and Secondary Education
17 Act of 1965 (20 U.S.C. 7801), supporting the evidence-based
18 practice or recommendation;

19 (ii) findings and data from previous Federal or State com-
20 missions recommending improvements to the safety posture of
21 a school; or

22 (iii) other supportive evidence or findings relied on by the
23 Clearinghouse in determining evidence-based practices and
24 recommendations, as determined in consultation with the offi-
25 cers described in subsection (a)(3)(B);

26 (C) include information on Federal programs for which imple-
27 mentation of each evidence-based practice or recommendation is
28 an eligible use for the program;

29 (D) be consistent with Federal civil rights laws, including title
30 II of the Americans with Disabilities Act of 1990 (42 U.S.C.
31 12131 et seq.), the Rehabilitation Act of 1973 (29 U.S.C. 701 et
32 seq.), and title VI of the Civil Rights Act of 1964 (42 U.S.C.
33 2000d et seq.); and

34 (E) include options for developmentally appropriate rec-
35 ommendations for use in educational settings with respect to chil-
36 dren's ages and physical, social, sensory, and emotionally develop-
37 mental statuses.

38 (3) PAST RECOMMENDATIONS.—The Clearinghouse shall present, as
39 determined in consultation with the officers described in subsection
40 (a)(3)(B), Federal, State, local, Tribal, private sector, and nongovern-
41 mental organization issued best practices and recommendations and

1 identify any best practice or recommendation of the Clearinghouse that
2 was previously issued by any organization or commission.

3 (e) ASSISTANCE AND TRAINING.—The Secretary may produce and pub-
4 lish materials on the Clearinghouse to assist and train educational agencies
5 and law enforcement agencies on the implementation of the evidence-based
6 practices and recommendations.

7 (d) CONTINUOUS IMPROVEMENT.— The Secretary shall—

8 (1) collect for the purpose of continuous improvement of the Clear-
9 inghouse—

10 (A) Clearinghouse data analytics;

11 (B) user feedback on the implementation of resources, evidence-
12 based practices, and recommendations identified by the Clearing-
13 house; and

14 (C) any evaluations conducted on implementation of the evi-
15 dence-based practices and recommendations of the Clearinghouse;
16 and

17 (2) in coordination with the Secretary of Education, the Sec-
18 retary of Health and Human Services, and the Attorney General—

19 -

20 (A) regularly assess and identify Clearinghouse evidence-based
21 practices and recommendations for which there are no resources
22 available through Federal Government programs for implementa-
23 tion; and

24 (B) establish an external advisory board, which shall be com-
25 prised of appropriate State, local, Tribal, private sector, and non-
26 governmental organizations, including organizations representing
27 parents of elementary and secondary school students,
28 representatives from civil rights organizations, representatives of
29 disability rights organizations, representatives of educators, rep-
30 resentatives of law enforcement, and nonprofit school safety and
31 security organizations, to—

32 (i) provide feedback on the implementation of evidence-
33 based practices and recommendations of the Clearinghouse;
34 and

35 (ii) propose additional recommendations for evidence-based
36 practices for inclusion in the Clearinghouse that meet the re-
37 quirements described in subsection (b)(2)(B).

38 (e) PARENTAL ASSISTANCE.—The Clearinghouse shall produce materials
39 in accessible formats to assist parents and legal guardians of students in
40 identifying relevant Clearinghouse resources related to supporting the imple-
41 mentation of Clearinghouse evidence-based practices and recommendations.

1 (f) NOTIFICATION.—

2 (1) BY SECRETARY OF EDUCATION.— The Secretary of Education
3 shall provide written notification of the publication of the Clearing-
4 house to—

5 (A) every State and local educational agency; and

6 (B) other Department of Education partners in the implementa-
7 tion of the evidence-based practices and recommendations of the
8 Clearinghouse, as determined appropriate by the Secretary of
9 Education.

10 (2) By Secretary.—The Secretary shall provide written notification of
11 the publication of the Clearinghouse to—

12 (A) every State homeland security advisor;

13 (B) every State department of homeland security; and

14 (C) other Department partners in the implementation of the evi-
15 dence-based practices and recommendations of the Clearinghouse,
16 as determined appropriate by the Secretary.

17 (3) By secretary of health and human services.—The Secretary of
18 Health and Human Services shall provide written notification of the
19 publication of the Clearinghouse to—

20 (A) every State department of public health; and

21 (B) other Department of Health and Human Services partners
22 in the implementation of the evidence-based practices and rec-
23 ommendations of the Clearinghouse, as determined appropriate by
24 the Secretary of Health and Human Services.

25 (4) By Attorney General.—The Attorney General shall provide writ-
26 ten notification of the publication of the Clearinghouse to—

27 (A) every State department of justice; and

28 (B) other Department of Justice partners in the implementation
29 of the evidence-based practices and recommendations of the Clear-
30 inghouse, as determined appropriate by the Attorney General.

31 (g) GRANT PROGRAM REVIEW.—

32 (1) FEDERAL GRANTS AND RESOURCES.— Not later June 25, 2023,
33 the Clearinghouse or the external advisory board shall—

34 (A) review grant programs and identify any grant program that
35 may be used to implement evidence-based practices and rec-
36 ommendations of the Clearinghouse;

37 (B) identify any evidence-based practices and recommendations
38 of the Clearinghouse for which there is not a Federal grant pro-
39 gram that may be used for the purposes of implementing the evi-
40 dence-based practice or recommendation as applicable to the agen-
41 cy; and

1 (C) periodically report any findings under subparagraph (B) to
2 the appropriate committees of Congress.

3 (2) STATE GRANTS AND RESOURCES.—The Clearinghouse shall, to
4 the extent practicable, identify, for each State—

5 (A) each agency responsible for school safety in the State, or
6 any State that does not have an agency designated;

7 (B) any grant program that may be used for the purposes of
8 implementing evidence-based practices and recommendations of
9 the Clearinghouse; and

10 (C) any resources other than grant programs that may be used
11 to assist in implementation of evidence-based practices and rec-
12 ommendations of the Clearinghouse.

13 (h) RULES OF CONSTRUCTION.—

14 (1) WAIVER OF REQUIREMENTS.—Nothing in this section shall be
15 construed to create, satisfy, or waive any requirement under—

16 (A) title II of the Americans with Disabilities Act of 1990 (42
17 U.S.C. 12131 et seq.);

18 (B) the Rehabilitation Act of 1973 (29 U.S.C. 701 et seq.);

19 (C) title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d
20 et seq.);

21 (D) title IX of the Education Amendments of 1972 (20 U.S.C.
22 1681 et seq.); or

23 (E) the Age Discrimination Act of 1975 (42 U.S.C. 6101 et
24 seq.).

25 (2) PROHIBITION OF FEDERALLY DEVELOPED, MANDATED, OR EN-
26 DORSED CURRICULUM.—Nothing in this section shall be construed to
27 authorize any officer or employee of the Federal Government to engage
28 in an activity otherwise prohibited under section 103(b) of the Depart-
29 ment of Education Organization Act (20 U.S.C. 3403(b)).

30 **§ 10825. Report and briefing on school and daycare protec-**
31 **tion**

32 (a) DEFINITIONS.—In this section, the terms “early childhood education
33 program”, “elementary school”, and “secondary school” have the meanings
34 given those terms in section 8101 of the Elementary and Secondary Edu-
35 cation Act of 1965 (20 U.S.C. 7801).

36 (b) REPORTS TO CONGRESS.—Not later than 180 days after December
37 23, 2022, and annually thereafter, the Secretary shall submit to the Com-
38 mittee on Homeland Security of the House of Representatives and the Com-
39 mittee on Homeland Security and Governmental Affairs of the Senate a re-
40 port regarding the following:

1 (1) The Department’s activities, policies, and plans to enhance the
2 security of early childhood education programs, elementary schools, and
3 secondary schools during the preceding year that includes information
4 on the Department’s activities through the Federal School Safety
5 Clearinghouse.

6 (2) Information on all structures or efforts in the Department in-
7 tended to bolster coordination among departmental components and of-
8 fices involved in carrying out paragraph (1) and with respect to each
9 structure or effort specificity on which components or offices are in-
10 volved and which component or office leads the structure or effort.

11 (3) A detailed description of the measures used to ensure privacy
12 rights, civil rights, and civil liberties protections in carrying out these
13 activities.

14 (c) BRIEFINGS.—Not later than 30 days after the submission of each re-
15 port required under subsection (b), the Secretary shall submit to the Com-
16 mittee on Homeland Security of the House of Representatives and the Com-
17 mittee on Homeland Security and Governmental Affairs of the Senate a
18 briefing regarding the report and the status of efforts to carry out plans
19 included in the report for the preceding year.

20 **Subchapter VII—Secure Handling of** 21 **Ammonium Nitrate**

22 **§ 10841. Definitions**

23 In this subchapter:

24 (1) AMMONIUM NITRATE.—The term “ammonium nitrate” means—

25 (A) solid ammonium nitrate that is chiefly the ammonium salt
26 of nitric acid and contains not less than 33 percent nitrogen by
27 weight; and

28 (B) a mixture containing a percentage of ammonium nitrate
29 that is equal to or greater than the percentage determined by the
30 Secretary under section 10842(b) of this title.

31 (2) AMMONIUM NITRATE FACILITY.—The term “ammonium nitrate
32 facility” means an entity that produces, sells or otherwise transfers
33 ownership of, or provides application services for, ammonium nitrate.

34 (3) AMMONIUM NITRATE PURCHASER.—The term “ammonium ni-
35 trate purchaser” means a person who purchases ammonium nitrate
36 from an ammonium nitrate facility.

37 **§ 10842. Regulation of the sale and transfer of ammonium** 38 **nitrate**

39 (a) IN GENERAL.—The Secretary shall regulate the sale and transfer of
40 ammonium nitrate by an ammonium nitrate facility in accordance with this
41 subchapter to prevent the misappropriation or use of ammonium nitrate in

1 an act of terrorism. The regulations shall be carried out by the Cybersecu-
2 rity and Infrastructure Security Agency.

3 (b) AMMONIUM NITRATE MIXTURES.—The Secretary, in consultation
4 with the heads of appropriate Federal departments and agencies (including
5 the Secretary of Agriculture), shall, after notice and an opportunity for
6 comment, establish a threshold percentage for ammonium nitrate in a sub-
7 stance.

8 (c) REGISTRATION OF OWNERS OF AMMONIUM NITRATE FACILITIES.—

9 (1) PROCESS.—The Secretary shall establish a process by which a
10 person that—

11 (A) owns an ammonium nitrate facility is required to register
12 with the Department; and

13 (B) registers under subparagraph (A) is issued a registration
14 number for purposes of this subchapter.

15 (2) INFORMATION.—A person applying to register under paragraph
16 (1) shall submit to the Secretary—

17 (A) the name, address, and telephone number of each ammo-
18 nium nitrate facility owned by that person;

19 (B) the name of the person designated by that person as the
20 point of contact for each facility, for purposes of this subchapter;
21 and

22 (C) other information the Secretary determines is appropriate.

23 (d) REGISTRATION OF AMMONIUM NITRATE PURCHASERS.—

24 (1) PROCESS.—The Secretary shall establish a process by which a
25 person that—

26 (A) intends to be an ammonium nitrate purchaser is required
27 to register with the Department; and

28 (B) registers under subparagraph (A) is issued a registration
29 number for purposes of this subchapter.

30 (2) INFORMATION.—A person applying to register under paragraph
31 (1) as an ammonium nitrate purchaser shall submit to the Secretary—

32 (A) the name, address, and telephone number of the applicant;
33 and

34 (B) the intended use of ammonium nitrate to be purchased by
35 the applicant.

36 (e) RECORDS.—

37 (1) MAINTENANCE OF RECORDS.—The owner of an ammonium ni-
38 trate facility shall—

39 (A) maintain a record of each sale or transfer of ammonium ni-
40 trate during the 2-year period beginning on the date of that sale
41 or transfer; and

1 (B) include in the record the information described in para-
2 graph (2).

3 (2) SPECIFIC INFORMATION REQUIRED.—For each sale or transfer
4 of ammonium nitrate, the owner of an ammonium nitrate facility
5 shall—

6 (A) record the name, address, telephone number, and registra-
7 tion number issued under subsection (c) or (d) of each person that
8 purchases ammonium nitrate, in a manner prescribed by the Sec-
9 retary;

10 (B) if applicable, record the name, address, and telephone num-
11 ber of an agent acting on behalf of the person described in sub-
12 paragraph (A), at the point of sale;

13 (C) record the date and quantity of ammonium nitrate sold or
14 transferred; and

15 (D) verify the identity of the persons described in subpara-
16 graphs (A) and (B), as applicable, in accordance with a procedure
17 established by the Secretary.

18 (3) PROTECTION OF INFORMATION.—In maintaining records under
19 paragraph (1), the owner of an ammonium nitrate facility shall take
20 reasonable actions to ensure the protection of the information included
21 in the records.

22 (f) EXEMPTION FOR EXPLOSIVE PURPOSES.—The Secretary may exempt
23 from this subchapter a person producing, selling, or purchasing ammonium
24 nitrate exclusively for use in the production of an explosive under a license
25 or permit issued under chapter 40 of title 18.

26 (g) CONSULTATION.—In carrying out this section, the Secretary shall
27 consult with the Secretary of Agriculture, States, and appropriate private-
28 sector entities, to ensure that the access of agricultural producers to ammo-
29 nium nitrate is not unduly burdened.

30 (h) DATA CONFIDENTIALITY.—

31 (1) IN GENERAL.—Notwithstanding section 552 of title 5 or the
32 USA PATRIOT Act (Public Law 107–56, 115 Stat. 272), and except
33 as provided in paragraph (2), the Secretary may not disclose to any
34 person any information obtained under this subchapter.

35 (2) EXCEPTION.—The Secretary may disclose information obtained
36 by the Secretary under this subchapter to—

37 (A) an officer or employee of the United States, or a person
38 that has entered into a contract with the United States, that has
39 a need to know the information to perform the duties of the offi-
40 cer, employee, or person; or

1 (B) a State agency under section 10844 of this title, under ap-
2 propriate arrangements to ensure the protection of the informa-
3 tion.

4 (i) REGISTRATION PROCEDURES AND CHECK OF TERRORIST SCREENING
5 DATABASE.—

6 (1) REGISTRATION PROCEDURES.—

7 (A) IN GENERAL.—The Secretary shall establish procedures to
8 efficiently receive applications for registration numbers under this
9 subchapter, conduct the checks required under paragraph (2), and
10 promptly issue or deny a registration number.

11 (B) INITIAL 6-MONTH REGISTRATION PERIOD.—The Secretary
12 shall take steps to maximize the number of registration applica-
13 tions that are submitted and processed during the 6-month period
14 described in section 10846(e) of this title.

15 (2) CHECK OF TERRORIST SCREENING DATABASE.—

16 (A) CHECK REQUIRED.—The Secretary shall conduct a check of
17 appropriate identifying information of a person seeking to register
18 with the Department under subsection (c) or (d) against identi-
19 fying information that appears in the terrorist screening database
20 of the Department.

21 (B) AUTHORITY TO DENY REGISTRATION NUMBER.—If the
22 identifying information of a person seeking to register with the
23 Department under subsection (c) or (d) appears in the terrorist
24 screening database of the Department, the Secretary may deny
25 issuance of a registration number under this subchapter.

26 (3) EXPEDITED REVIEW OF APPLICATIONS.—

27 (A) IN GENERAL.—Following the 6-month period described in
28 section 10846(e) of this title, the Secretary shall, to the extent
29 practicable, issue or deny registration numbers under this sub-
30 chapter not later than 72 hours after the time the Secretary re-
31 ceives a complete registration application, unless the Secretary de-
32 termines, in the interest of national security, that additional time
33 is necessary to review an application.

34 (B) NOTICE OF APPLICATION STATUS.—In all cases, the Sec-
35 retary shall notify a person seeking to register with the Depart-
36 ment under subsection (c) or (d) of the status of the application
37 of that person not later than 72 hours after the time the Secretary
38 receives a complete registration application.

39 (4) EXPEDITED APPEALS PROCESS.—

40 (A) REQUIREMENT.—

1 (i) ESTABLISHMENT.—The Secretary shall establish an ex-
2 pedited appeals process for persons denied a registration
3 number under this subchapter.

4 (ii) TIME FOR RESOLVING APPEALS.—The Secretary shall,
5 to the extent practicable, resolve appeals not later than 72
6 hours after receiving a complete request for appeal unless the
7 Secretary determines, in the interest of national security, that
8 additional time is necessary to resolve an appeal.

9 (B) CONSULTATION.—The Secretary, in developing the appeals
10 process under subparagraph (A), shall consult with appropriate
11 stakeholders.

12 (C) GUIDANCE.—The Secretary shall provide guidance regard-
13 ing the procedures and information required for an appeal under
14 subparagraph (A) to any person denied a registration number
15 under this subchapter.

16 (5) RESTRICTIONS ON USE AND MAINTENANCE OF INFORMATION.—

17 (A) IN GENERAL.—Information constituting grounds for denial
18 of a registration number under this section shall be maintained
19 confidentially by the Secretary and may be used only for making
20 determinations under this section.

21 (B) SHARING OF INFORMATION.—Notwithstanding this sub-
22 chapter, the Secretary may share information with Federal, State,
23 local, and tribal law enforcement agencies, as appropriate.

24 (6) REGISTRATION INFORMATION.—

25 (A) AUTHORITY TO REQUIRE INFORMATION.—The Secretary
26 may require a person applying for a registration number under
27 this subchapter to submit information necessary to carry out the
28 requirements of this section.

29 (B) REQUIREMENT TO UPDATE INFORMATION.—The Secretary
30 may require persons issued a registration under this subchapter to
31 update registration information submitted to the Secretary under
32 this subchapter, as appropriate.

33 (7) RECHECKS AGAINST TERRORIST SCREENING DATABASE.—

34 (A) IN GENERAL.—The Secretary shall, as appropriate, recheck
35 persons provided a registration number pursuant to this sub-
36 chapter against the terrorist screening database of the Depart-
37 ment, and may revoke the registration number if the Secretary de-
38 termines the person may pose a threat to national security.

39 (B) NOTICE OF REVOCATION.—The Secretary shall, as appro-
40 priate, provide prior notice to a person whose registration number

1 is revoked under this section, and the person shall have an oppor-
2 tunity to appeal, as provided in paragraph (4).

3 **§ 10843. Inspection and auditing of records**

4 The Secretary shall establish a process for the periodic inspection and au-
5 diting of the records maintained by owners of ammonium nitrate facilities
6 for the purpose of monitoring compliance with this subchapter or for the
7 purpose of deterring or preventing the misappropriation or use of ammo-
8 nium nitrate in an act of terrorism.

9 **§ 10844. Administrative provisions**

10 (a) COOPERATIVE AGREEMENTS.—The Secretary—

11 (1) may enter into a cooperative agreement with the Secretary of Ag-
12 riculture, or the head of any State department of agriculture or its des-
13 ignee involved in agricultural regulation, in consultation with the State
14 agency responsible for homeland security, to carry out this subchapter;
15 and

16 (2) wherever possible, shall seek to cooperate with State agencies or
17 their designees that oversee ammonium nitrate facility operations when
18 seeking cooperative agreements to implement the registration and en-
19 forcement provisions of this subchapter.

20 (b) DELEGATION.—

21 (1) AUTHORITY.—The Secretary may delegate to a State the author-
22 ity to assist the Secretary in the administration and enforcement of
23 this subchapter.

24 (2) DELEGATION REQUIRED.—At the request of a Governor of a
25 State, the Secretary shall delegate to that State the authority to carry
26 out functions under sections 10842 and 10843 of this title, if the Sec-
27 retary determines that the State is capable of satisfactorily carrying
28 out the functions.

29 (3) FUNDING.—Subject to the availability of appropriations, if the
30 Secretary delegates functions to a State under this subsection, the Sec-
31 retary shall provide to that State sufficient funds to carry out the dele-
32 gated functions.

33 (c) PROVISION OF GUIDANCE AND NOTIFICATION MATERIALS TO AMMO-
34 NIUM NITRATE FACILITIES.—

35 (1) GUIDANCE.—The Secretary shall make available to each owner
36 of an ammonium nitrate facility registered under section 10842(c) of
37 this title guidance on—

38 (A) the identification of suspicious ammonium nitrate purchases
39 or transfers or attempted purchases or transfers;

1 (B) the appropriate course of action to be taken by the ammo-
2 nium nitrate facility owner with respect to such a purchase or
3 transfer or attempted purchase or transfer, including—

4 (i) exercising the right of the owner of the ammonium ni-
5 trate facility to decline sale of ammonium nitrate; and

6 (ii) notifying appropriate law enforcement entities; and

7 (C) additional subjects determined appropriate to prevent the
8 misappropriation or use of ammonium nitrate in an act of ter-
9 rorism.

10 (2) USE OF MATERIALS AND PROGRAMS.—In providing guidance
11 under this subsection, the Secretary shall, to the extent practicable, le-
12 verage relevant materials and programs.

13 (3) NOTIFICATION MATERIALS.—

14 (A) IN GENERAL.—The Secretary shall make available materials
15 suitable for posting at locations where ammonium nitrate is sold.

16 (B) DESIGN.—Materials made available under subparagraph
17 (A) shall be designed to notify prospective ammonium nitrate pur-
18 chasers of—

19 (i) the record-keeping requirements under section 10842 of
20 this title; and

21 (ii) the penalties for violating the requirements.

22 **§ 10845. Theft reporting requirement**

23 A person who is required to comply with section 10842(e) of this title
24 who has knowledge of the theft or unexplained loss of ammonium nitrate
25 shall report the theft or loss to the appropriate Federal law enforcement au-
26 thorities not later than 1 calendar day after the date on which the person
27 becomes aware of the theft or loss. On receipt of the report, the relevant
28 Federal authorities shall inform State, local, and tribal law enforcement en-
29 tities, as appropriate.

30 **§ 10846. Prohibitions and penalty**

31 (a) PROHIBITIONS.—

32 (1) TAKING POSSESSION.—A person may not purchase ammonium
33 nitrate from an ammonium nitrate facility unless the person is reg-
34 istered under subsection (c) or (d) of section 10842 of this title or is
35 an agent of a person registered under subsection (c) or (d) of section
36 10842.

37 (2) TRANSFERRING POSSESSION.—An owner of an ammonium ni-
38 trate facility shall not transfer possession of ammonium nitrate from
39 the ammonium nitrate facility to an ammonium nitrate purchaser who
40 is not registered under subsection (c) or (d) of section 10842 of this
41 title, or to an agent acting on behalf of an ammonium nitrate pur-

1 chaser when the purchaser is not registered under subsection (c) or (d)
2 of section 10842.

3 (3) OTHER PROHIBITIONS.—A person may not—

4 (A) purchase ammonium nitrate without a registration number
5 required under subsection (c) or (d) of section 10842 of this title;

6 (B) own or operate an ammonium nitrate facility without a reg-
7 istration number required under section 10842(c) of this title; or

8 (C) fail to comply with a requirement or violate another prohibi-
9 tion under this subchapter.

10 (b) CIVIL PENALTY.—A person that violates this subchapter may be as-
11 sessed a civil penalty by the Secretary of not more than \$50,000 per viola-
12 tion.

13 (c) PENALTY CONSIDERATIONS.—In determining the amount of a civil
14 penalty under this section, the Secretary shall consider—

15 (1) the nature and circumstances of the violation;

16 (2) with respect to the person who commits the violation, any history
17 of prior violations, the ability to pay the penalty, and any effect the
18 penalty is likely to have on the ability of the person to do business;
19 and

20 (3) any other matter that the Secretary determines that justice re-
21 quires.

22 (d) NOTICE AND OPPORTUNITY FOR A HEARING.—A civil penalty may
23 not be assessed under this subchapter unless the person liable for the pen-
24 alty has been given notice and an opportunity for a hearing on the violation
25 for which the penalty is to be assessed in the county, parish, or incorporated
26 city of residence of that person.

27 (e) DELAY IN APPLICATION OF PROHIBITION.—Paragraphs (1) and (2)
28 of subsection (a) shall apply on and after the date that is 6 months after
29 the date that the Secretary issues a final rule implementing this subchapter.

30 **§ 10847. Protection from civil liability**

31 (a) IN GENERAL.—Notwithstanding another law, an owner of an ammo-
32 nium nitrate facility that in good faith refuses to sell or transfer ammonium
33 nitrate to a person, or that in good faith discloses to the Department or
34 to appropriate law enforcement authorities an actual or attempted purchase
35 or transfer of ammonium nitrate, based upon a reasonable belief that the
36 person seeking purchase or transfer of ammonium nitrate may use the am-
37 monium nitrate to create an explosive device to be employed in an act of
38 terrorism (as defined in section 3077 of title 18), or to use ammonium ni-
39 trate for any other unlawful purpose, shall not be liable in any civil action
40 relating to that refusal to sell ammonium nitrate or that disclosure.

1 (b) REASONABLE BELIEF.—A reasonable belief that an individual may
2 use ammonium nitrate to create an explosive device to be employed in an
3 act of terrorism under subsection (a) may not solely be based on the individ-
4 ual’s race, sex, national origin, creed, religion, status as a veteran, or status
5 as a member of the armed forces of the United States.

6 **§ 10848. Preemption of other laws**

7 (a) OTHER FEDERAL REGULATIONS.—Except as provided in section
8 10847 of this title, nothing in this subchapter affects a regulation issued
9 by an agency other than an agency of the Department.

10 (b) STATE LAW.—Subject to section 10847 of this title, this subchapter
11 preempts the laws of a State to the extent that the laws are inconsistent
12 with this subchapter, except that this subchapter shall not preempt any
13 State law that provides additional protection against the acquisition of am-
14 monium nitrate by terrorists or the use of ammonium nitrate in explosives
15 in acts of terrorism or for other illicit purposes, as determined by the Sec-
16 retary.

17 **Subchapter VIII—Chemical Facilities**

18 **§ 10861. Definitions**

19 In this subchapter:

20 (1) CFATS REGULATION.—The term “CFATS regulation” means—

21 (A) an existing CFATS regulation; and

22 (B) any regulation or amendment to an existing CFATS regula-
23 tion issued pursuant to the authority under section 10867 of this
24 title.

25 (2) CHEMICAL FACILITY OF INTEREST.—The term “chemical facility
26 of interest” means a facility that—

27 (A) holds, or that the Secretary has a reasonable basis to be-
28 lieve holds, a chemical of interest, as designated under Appendix
29 A to part 27 of title 6, Code of Federal Regulations, or any suc-
30 cessor to the Appendix, at a threshold quantity set pursuant to
31 relevant risk-related security principles; and

32 (B) is not an excluded facility.

33 (3) COVERED CHEMICAL FACILITY.—The term “covered chemical fa-
34 cility” means a facility that—

35 (A) the Secretary—

36 (i) identifies as a chemical facility of interest; and

37 (ii) based on review of the facility’s Top-Screen, determines
38 meets the risk criteria developed under section
39 10862(e)(2)(B) of this title; and

40 (B) is not an excluded facility.

41 (4) EXCLUDED FACILITY.—The term “excluded facility” means—

1 (A) a facility regulated under the Maritime Transportation Se-
2 curity Act of 2002 (Public Law 107–295; 116 Stat. 2064);

3 (B) a public water system, as that term is defined in section
4 1401 of the Public Health Service Act (42 U.S.C. 300f);

5 (C) a treatment works, as that term is defined in section 212
6 of the Federal Water Pollution Control Act (33 U.S.C. 1292);

7 (D) a facility owned or operated by the Department of Defense
8 or the Department of Energy; or

9 (E) a facility subject to regulation by the Nuclear Regulatory
10 Commission, or by a State that has entered into an agreement
11 with the Nuclear Regulatory Commission under section 274(b)
12 of the Atomic Energy Act of 1954 (42 U.S.C. 2021(b)) to protect
13 against unauthorized access of any material, activity, or structure
14 licensed by the Nuclear Regulatory Commission.

15 (5) EXISTING CFATS REGULATION.—The term “existing CFATS reg-
16 ulation” means—

17 (A) a regulation promulgated under section 550 of the Depart-
18 ment of Homeland Security Appropriations Act, 2007 (Public Law
19 109–295) that was in effect on December 17, 2014; and

20 (B) a Federal Register notice or other published guidance relat-
21 ing to section 550 of the Department of Homeland Security Ap-
22 propriations Act, 2007 (Public Law 109–295) that was in effect
23 on December 17, 2014.

24 (6) EXPEDITED APPROVAL FACILITY.—The term “expedited approval
25 facility” means a covered chemical facility for which the owner or oper-
26 ator elects to submit a site security plan in accordance with section
27 10862(e)(4) of this title.

28 (7) FACIALLY DEFICIENT.—The term “facially deficient”, relating to
29 a site security plan, means a site security plan that does not support
30 a certification that the security measures in the plan address the secu-
31 rity vulnerability assessment and the risk-based performance standards
32 for security for a facility, based on a review of—

33 (A) the facility’s site security plan;

34 (B) the facility’s Top-Screen;

35 (C) the facility’s security vulnerability assessment; or

36 (D) any other information that—

37 (i) the facility submits to the Department; or

38 (ii) the Department obtains from a public source or other
39 source.

1 (8) GUIDANCE FOR EXPEDITED APPROVAL FACILITIES.—The term
2 “guidance for expedited approval facilities” means the guidance issued
3 under section 10862(e)(4)(B)(i) of this title.

4 (9) RISK ASSESSMENT.—The term “risk assessment” means the Sec-
5 retary’s application of relevant risk criteria identified in section
6 10862(e)(2)(B) of this title.

7 (10) TERRORIST SCREENING DATABASE.—The term “terrorist
8 screening database” means the terrorist screening database maintained
9 by the Federal Government Terrorist Screening Center or its successor.

10 (11) TIER.—The term “tier” has the meaning given the term in sec-
11 tion 27.105 of title 6, Code of Federal Regulations, or any successor
12 to section 27.105.

13 (12) TIERING; TIERING METHODOLOGY.—The terms “tiering” and
14 “tiering methodology” mean the procedure by which the Secretary as-
15 signs a tier to each covered chemical facility based on the risk assess-
16 ment for that covered chemical facility.

17 (13) TOP-SCREEN.—The term “Top-Screen” has the meaning given
18 the term in section 27.105 of title 6, Code of Federal Regulations, or
19 any successor to section 27.105.

20 (14) VULNERABILITY ASSESSMENT.—The term “vulnerability assess-
21 ment” means the identification of weaknesses in the security of a
22 chemical facility of interest.

23 **§ 10862. Chemical Facility Anti-Terrorism Standards Pro-**
24 **gram**

25 (a) DUTIES OF SECRETARY.—In carrying out the Chemical Facility Anti-
26 Terrorism Standards Program, the Secretary shall—

27 (1) identify—

28 (A) chemical facilities of interest; and

29 (B) covered chemical facilities;

30 (2) require each chemical facility of interest to submit a Top-Screen
31 and any other information the Secretary determines necessary to enable
32 the Department to assess the security risks associated with the facility;

33 (3) establish risk-based performance standards designed to address
34 high levels of security risk at covered chemical facilities; and

35 (4) require each covered chemical facility to—

36 (A) submit a security vulnerability assessment; and

37 (B) develop, submit, and implement a site security plan.

38 (b) SECURITY MEASURES.—

39 (1) IN GENERAL.—A facility, in developing a site security plan as
40 required under subsection (a), shall include security measures that, in
41 combination, appropriately address the security vulnerability assess-

1 ment and the risk-based performance standards for security for the fa-
2 cility.

3 (2) EMPLOYEE INPUT.—To the greatest extent practicable, a facili-
4 ty’s security vulnerability assessment and site security plan shall in-
5 clude input from at least 1 facility employee and, where applicable, 1
6 employee representative from the bargaining agent at that facility, each
7 of whom possesses, in the determination of the facility’s security offi-
8 cer, relevant knowledge, experience, training, or education as pertains
9 to matters of site security.

10 (c) APPROVAL OR DISAPPROVAL OF SITE SECURITY PLANS.—

11 (1) IN GENERAL.—

12 (A) REVIEW.—Except as provided in paragraph (4), the Sec-
13 retary shall review and approve or disapprove each site security
14 plan submitted pursuant to subsection (a).

15 (B) BASES FOR DISAPPROVAL.—The Secretary—

16 (i) may not disapprove a site security plan based on the
17 presence or absence of a particular security measure; and

18 (ii) shall disapprove a site security plan if the plan fails to
19 satisfy the risk-based performance standards established pur-
20 suant to subsection (a)(3).

21 (2) ALTERNATIVE SECURITY PROGRAMS.—

22 (A) AUTHORITY TO APPROVE.—

23 (i) IN GENERAL.—The Secretary may approve an alter-
24 native security program established by a private-sector entity
25 or a Federal, State, or local authority or under other applica-
26 ble laws if the Secretary determines that the requirements of
27 the program meet the requirements under this section.

28 (ii) ADDITIONAL SECURITY MEASURES.—If the require-
29 ments of an alternative security program do not meet the re-
30 quirements under this section, the Secretary may recommend
31 additional security measures to the program that will enable
32 the Secretary to approve the program.

33 (B) SATISFACTION OF SITE SECURITY PLAN REQUIREMENT.—

34 A covered chemical facility may satisfy the site security plan re-
35 quirement under subsection (a)(4) by adopting an alternative secu-
36 rity program that the Secretary has—

37 (i) reviewed and approved under subparagraph (A); and

38 (ii) determined to be appropriate for the operations and se-
39 curity concerns of the covered chemical facility.

40 (3) SITE SECURITY PLAN ASSESSMENTS.—

1 (A) RISK ASSESSMENT POLICIES AND PROCEDURES.—In ap-
2 proving or disapproving a site security plan under this subsection,
3 the Secretary shall employ the risk assessment policies and proce-
4 dures developed under this subchapter.

5 (B) PREVIOUSLY APPROVED PLANS.—In the case of a covered
6 chemical facility for which the Secretary approved a site security
7 plan before December 18, 2014, the Secretary may not require the
8 facility to resubmit the site security plan solely by reason of the
9 enactment of this subchapter.

10 (4) EXPEDITED APPROVAL PROGRAM.—

11 (A) IN GENERAL.—A covered chemical facility assigned to tier
12 3 or 4 may meet the requirement to develop and submit a site se-
13 curity plan under subsection (a)(4) by developing and submitting
14 to the Secretary—

15 (i) a site security plan and the certification described in
16 subparagraph (C); or

17 (ii) a site security plan in conformance with a template au-
18 thorized under subparagraph (H).

19 (B) GUIDANCE FOR EXPEDITED APPROVAL FACILITIES.—

20 (i) IN GENERAL.—The Secretary shall issue guidance for
21 expedited approval facilities that identifies specific security
22 measures that are sufficient to meet the risk-based perform-
23 ance standards.

24 (ii) MATERIAL DEVIATION FROM GUIDANCE.—If a security
25 measure in the site security plan of an expedited approval fa-
26 cility materially deviates from a security measure in the guid-
27 ance for expedited approval facilities, the site security plan
28 shall include an explanation of how the security measure
29 meets the risk-based performance standards.

30 (iii) APPLICABILITY OF OTHER LAWS TO DEVELOPMENT
31 AND ISSUANCE OF INITIAL GUIDANCE.—In developing and
32 issuing, or amending, the guidance for expedited approval fa-
33 cilities under this subparagraph and in collecting information
34 from expedited approval facilities, the Secretary shall not be
35 subject to—

36 (I) section 553 of title 5;

37 (II) subchapter I of chapter 35 of title 44; or

38 (III) section 10867(b) of this title.

39 (C) CERTIFICATION.—The owner or operator of an expedited
40 approval facility shall submit to the Secretary a certification,
41 signed under penalty of perjury, that—

1 (i) the owner or operator is familiar with the requirements
2 of this subchapter and part 27 of title 6, Code of Federal
3 Regulations, or any successor to this subchapter or part 27,
4 and the site security plan being submitted;

5 (ii) the site security plan includes the security measures re-
6 quired by subsection (a);

7 (iii)(I) the security measures in the site security plan do
8 not materially deviate from the guidance for expedited ap-
9 proval facilities except where indicated in the site security
10 plan;

11 (II) any deviations from the guidance for expedited ap-
12 proval facilities in the site security plan meet the risk-based
13 performance standards for the tier to which the facility is as-
14 signed; and

15 (III) the owner or operator has provided an explanation of
16 how the site security plan meets the risk-based performance
17 standards for any material deviation;

18 (iv) the owner or operator has visited, examined, docu-
19 mented, and verified that the expedited approval facility
20 meets the criteria set forth in the site security plan;

21 (v) the expedited approval facility has implemented all the
22 required performance measures outlined in the site security
23 plan or set out planned measures that will be implemented
24 within a reasonable time period stated in the site security
25 plan;

26 (vi) each individual responsible for implementing the site
27 security plan has been made aware of the requirements rel-
28 evant to the individual's responsibility contained in the site
29 security plan and has demonstrated competency to carry out
30 those requirements;

31 (vii) the owner or operator has committed, or, in the case
32 of planned measures, will commit, the necessary resources to
33 fully implement the site security plan; and

34 (viii) the planned measures include an adequate procedure
35 for addressing events beyond the control of the owner or oper-
36 ator in implementing any planned measures.

37 (D) DEADLINE.—

38 (i) DATE FOR SUBMISSION TO SECRETARY.—The owner or
39 operator of an expedited approval facility shall submit to the
40 Secretary the site security plan and the certification described
41 in subparagraph (C) not later than 120 days after—

1 (I) for an expedited approval facility that was assigned
2 to tier 3 or 4 under existing CFATS regulations before
3 December 18, 2014, the date that is 210 days after De-
4 cember 18, 2014; and

5 (II) for any expedited approval facility not described
6 in subclause (I), the later of—

7 (aa) the date on which the expedited approval fa-
8 cility is assigned to tier 3 or 4 under subsection
9 (e)(2)(A); or

10 (bb) the date that is 210 days after December 18,
11 2014.

12 (ii) NOTICE.—An owner or operator of an expedited ap-
13 proval facility shall notify the Secretary of the intent of the
14 owner or operator to certify the site security plan for the ex-
15 pedited approval facility not later than 30 days before the
16 date on which the owner or operator submits the site security
17 plan and certification described in subparagraph (C).

18 (E) COMPLIANCE.—

19 (i) IN GENERAL.—For an expedited approval facility sub-
20 mitting a site security plan and certification in accordance
21 with subparagraphs (A), (B), (C), and (D)—

22 (I) the expedited approval facility shall comply with all
23 of the requirements of its site security plan; and

24 (II) the Secretary—

25 (aa) except as provided in subparagraph (G), may
26 not disapprove the site security plan; and

27 (bb) may audit and inspect the expedited ap-
28 proval facility under subsection (d) to verify compli-
29 ance with its site security plan.

30 (ii) NONCOMPLIANCE.—If the Secretary determines an ex-
31 pedited approval facility is not in compliance with the require-
32 ments of the site security plan or is otherwise in violation of
33 this subchapter, the Secretary may enforce compliance in ac-
34 cordance with section 10864 of this title.

35 (F) AMENDMENTS TO SITE SECURITY PLAN.—

36 (i) REQUIREMENT.—

37 (I) IN GENERAL.—If the owner or operator of an ex-
38 pedited approval facility amends a site security plan sub-
39 mitted under subparagraph (A), the owner or operator
40 shall submit the amended site security plan and a certifi-

1 cation relating to the amended site security plan that
2 contains the information described in subparagraph (C).

3 (II) TECHNICAL AMENDMENTS.—For purposes of this
4 clause, an amendment to a site security plan includes
5 any technical amendment to the site security plan.

6 (ii) WHEN AMENDMENT REQUIRED.—The owner or oper-
7 ator of an expedited approval facility shall amend the site se-
8 curity plan if—

9 (I) there is a change in the design, construction, oper-
10 ation, or maintenance of the expedited approval facility
11 that affects the site security plan;

12 (II) the Secretary requires additional security meas-
13 ures or suspends a certification and recommends addi-
14 tional security measures under subparagraph (G); or

15 (III) the owner or operator receives notice from the
16 Secretary of a change in tiering under subsection (e)(3).

17 (iii) DEADLINE.—An amended site security plan and cer-
18 tification shall be submitted under clause (i)—

19 (I) in the case of a change in design, construction, op-
20 eration, or maintenance of the expedited approval facility
21 that affects the security plan, not later than 120 days
22 after the date on which the change in design, construc-
23 tion, operation, or maintenance occurred;

24 (II) in the case of the Secretary requiring additional
25 security measures or suspending a certification and rec-
26 ommending additional security measures under subpara-
27 graph (G), not later than 120 days after the date on
28 which the owner or operator receives notice of the re-
29 quirement for additional security measures or suspension
30 of the certification and recommendation of additional se-
31 curity measures; and

32 (III) in the case of a change in tiering under sub-
33 section (e)(3), not later than 120 days after the date on
34 which the owner or operator receives notice.

35 (G) FACIALLY DEFICIENT SITE SECURITY PLANS.—

36 (i) PROHIBITION.—Notwithstanding subparagraph (A) or
37 (E), the Secretary may suspend the authority of a covered
38 chemical facility to certify a site security plan if the Sec-
39 retary—

40 (I) determines the certified site security plan or an
41 amended site security plan is facially deficient; and

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40

(II) not later than 100 days after the date on which the Secretary receives the site security plan and certification, provides the covered chemical facility with written notification that the site security plan is facially deficient, including a clear explanation of each deficiency in the site security plan.

(ii) ADDITIONAL SECURITY MEASURES.—

(I) IN GENERAL.—If, during or after a compliance inspection of an expedited approval facility, the Secretary determines that planned or implemented security measures in the site security plan of the facility are insufficient to meet the risk-based performance standards based on misrepresentation, omission, or an inadequate description of the site, the Secretary may—

- (aa) require additional security measures; or
- (bb) suspend the certification of the facility.

(II) RECOMMENDATION OF ADDITIONAL SECURITY MEASURES.—If the Secretary suspends the certification of an expedited approval facility under subclause (I), the Secretary shall—

- (aa) recommend specific additional security measures that, if made part of the site security plan by the facility, would enable the Secretary to approve the site security plan; and
- (bb) provide the facility an opportunity to submit a new or modified site security plan and certification under subparagraph (A).

(III) SUBMISSION; REVIEW.—If an expedited approval facility determines to submit a new or modified site security plan and certification as authorized under subclause (II)(bb)—

- (aa) not later than 90 days after the date on which the facility receives recommendations under subclause (II)(aa), the facility shall submit the new or modified plan and certification; and
- (bb) not later than 45 days after the date on which the Secretary receives the new or modified plan under item (aa), the Secretary shall review the plan and determine whether the plan is facially deficient.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41

(IV) DETERMINATION NOT TO INCLUDE ADDITIONAL SECURITY MEASURES.—

(aa) REVOCATION OF CERTIFICATION.—If an expedited approval facility does not agree to include in its site security plan specific additional security measures recommended by the Secretary under subclause (II)(aa), or does not submit a new or modified site security plan in accordance with subclause (III), the Secretary may revoke the certification of the facility by issuing an order under section 10864(a)(1)(B) of this title.

(bb) EFFECT OF REVOCATION.—If the Secretary revokes the certification of an expedited approval facility under item (aa) by issuing an order under section 10864(a)(1)(B) of this title—

(AA) the order shall require the owner or operator of the facility to submit a site security plan or alternative security program for review by the Secretary under paragraph (1) or (2); and

(BB) the facility shall no longer be eligible to certify a site security plan under this paragraph.

(V) FACIAL DEFICIENCY.—If the Secretary determines that a new or modified site security plan submitted by an expedited approval facility under subclause (III) is facially deficient—

(aa) not later than 120 days after the date of the determination, the owner or operator of the facility shall submit a site security plan or alternative security program for review by the Secretary under paragraph (1) or (2); and

(bb) the facility shall no longer be eligible to certify a site security plan under this paragraph.

(H) TEMPLATES.—

(i) IN GENERAL.—The Secretary may develop prescriptive site security plan templates with specific security measures to meet the risk-based performance standards under subsection (a)(3) for adoption and certification by a covered chemical facility assigned to tier 3 or 4 in lieu of developing and certifying its own plan.

1 (ii) APPLICABILITY OF OTHER LAWS TO DEVELOPING AND
2 ISSUING INITIAL SITE SECURITY PLAN TEMPLATES AND RE-
3 LATED GUIDANCE AND TO COLLECTING INFORMATION.—Dur-
4 ing the period before the Secretary has met the deadline
5 under subparagraph (D)(i), in developing and issuing, or
6 amending, the site security plan templates under this sub-
7 paragraph, in issuing guidance for implementation of the
8 templates, and in collecting information from expedited ap-
9 proval facilities, the Secretary shall not be subject to—

10 (I) section 553 of title 5;

11 (II) subchapter I of chapter 35 of title 44; or

12 (III) section 10867(b) of this title.

13 (iii) RULE OF CONSTRUCTION.—Nothing in this subpara-
14 graph shall be construed to prevent a covered chemical facil-
15 ity from developing and certifying its own security plan in ac-
16 cordance with subparagraph (A).

17 (I) EVALUATION.—

18 (i) IN GENERAL.—The Secretary shall take any appropriate
19 action necessary for a full evaluation of the expedited ap-
20 proval program authorized under this paragraph, including
21 conducting an appropriate number of inspections, as author-
22 ized under subsection (d), of expedited approval facilities.

23 (ii) REPORT.—The Secretary shall submit to the Com-
24 mittee on Homeland Security and Governmental Affairs of
25 the Senate and the Committee on Homeland Security and the
26 Committee on Energy and Commerce of the House of Rep-
27 resentatives a report that contains—

28 (I)(aa) the number of eligible facilities using the expe-
29 dited approval program authorized under this paragraph;
30 and

31 (bb) the number of facilities that are eligible for the
32 expedited approval program but are using the standard
33 process for developing and submitting a site security
34 plan under subsection (a)(4);

35 (II) any costs and efficiencies associated with the ex-
36 pedited approval program;

37 (III) the impact of the expedited approval program on
38 the backlog for site security plan approval and authoriza-
39 tion inspections;

40 (IV) an assessment of the ability of expedited approval
41 facilities to submit facially sufficient site security plans;

- 1 (V) an assessment of any impact of the expedited ap-
2 proval program on the security of chemical facilities; and
3 (VI) a recommendation by the Secretary on the fre-
4 quency of compliance inspections that may be required
5 for expedited approval facilities.

6 (d) COMPLIANCE.—

7 (1) AUDITS AND INSPECTIONS.—

8 (A) DEFINITIONS.—In this paragraph:

9 (i) NONDEPARTMENTAL.—The term “nondepartmental”—

10 (I) with respect to personnel, means personnel who are
11 not employed by the Department; and

12 (II) with respect to an entity, means an entity that is
13 not a component or other authority of the Department.

14 (ii) NONGOVERNMENTAL.—The term “nongovernmental”—

15 (I) with respect to personnel, means personnel who are
16 not employed by the Federal Government; and

17 (II) with respect to an entity, means an entity that is
18 not an agency, department, or other authority of the
19 Federal Government.

20 (B) AUTHORITY TO CONDUCT AUDITS AND INSPECTIONS.—The
21 Secretary shall conduct audits or inspections under this sub-
22 chapter using—

23 (i) employees of the Department;

24 (ii) nondepartmental or nongovernmental personnel ap-
25 proved by the Secretary; or

26 (iii) a combination of individuals described in clauses (i)
27 and (ii).

28 (C) SUPPORT PERSONNEL.—The Secretary may use nongovern-
29 mental personnel to provide administrative and logistical services
30 in support of audits and inspections under this subchapter.

31 (D) REPORTING STRUCTURE.—

32 (i) NONDEPARTMENTAL AND NONGOVERNMENTAL AUDITS
33 AND INSPECTIONS.—Any audit or inspection conducted by an
34 individual employed by a nondepartmental or nongovern-
35 mental entity shall be assigned in coordination with a regional
36 supervisor with responsibility for supervising inspectors in the
37 Infrastructure Security Compliance Division of the Depart-
38 ment for the region in which the audit or inspection is to be
39 conducted.

40 (ii) REQUIREMENT TO REPORT.—While an individual em-
41 ployed by a nondepartmental or nongovernmental entity is in

1 the field conducting an audit or inspection under this sub-
2 section, the individual shall report to the regional supervisor
3 with responsibility for supervising inspectors in the Infra-
4 structure Security Compliance Division of the Department for
5 the region in which the individual is operating.

6 (iii) APPROVAL.—The authority to approve a site security
7 plan under subsection (c) or determine if a covered chemical
8 facility is in compliance with an approved site security plan
9 shall be exercised solely by the Secretary or a designee of the
10 Secretary in the Department.

11 (E) STANDARDS FOR AUDITORS AND INSPECTORS.—The Sec-
12 retary shall prescribe standards for the training and retraining of
13 each individual used by the Department as an auditor or inspec-
14 tor, including each individual employed by the Department and all
15 nondepartmental or nongovernmental personnel, including—

16 (i) minimum training requirements for new auditors and
17 inspectors;

18 (ii) retraining requirements;

19 (iii) minimum education and experience levels;

20 (iv) the submission of information as required by the Sec-
21 retary to enable determination of whether the auditor or in-
22 spector has a conflict of interest;

23 (v) the proper certification necessary to handle chemical-
24 terrorism vulnerability information (as defined in section
25 27.105 of title 6, Code of Federal Regulations, or any suc-
26 cessor to section 27.105);

27 (vi) the reporting of any issue of non-compliance with this
28 section to the Secretary within 24 hours; and

29 (vii) any additional qualifications for fitness of duty as the
30 Secretary may require.

31 (F) CONDITIONS FOR NONGOVERNMENTAL AUDITORS AND IN-
32 SPECTORS.—If the Secretary arranges for an audit or inspection
33 under subparagraph (B) to be carried out by a nongovernmental
34 entity, the Secretary shall—

35 (i) prescribe standards for the qualification of the individ-
36 uals who carry out the audits and inspections that are com-
37 mensurate with the standards for similar Government audi-
38 tors or inspectors; and

39 (ii) ensure that any duties carried out by a nongovern-
40 mental entity are not inherently governmental functions.

41 (2) PERSONNEL SURETY PROGRAM.—

1 (A) ESTABLISHMENT.—For purposes of this subchapter, the
2 Secretary shall establish and carry out a Personnel Surety Pro-
3 gram that—

4 (i) does not require an owner or operator of a covered
5 chemical facility that voluntarily participates in the program
6 to submit information about an individual more than 1 time;

7 (ii) provides a participating owner or operator of a covered
8 chemical facility with relevant information about an individual
9 based on vetting the individual against the terrorist screening
10 database, to the extent that the feedback is necessary for the
11 facility to be in compliance with regulations promulgated
12 under this subchapter; and

13 (iii) provides redress to an individual—

14 (I) whose information was vetted against the terrorist
15 screening database under the program; and

16 (II) who believes that the personally identifiable infor-
17 mation submitted to the Department for vetting by a
18 covered chemical facility, or its designated representa-
19 tive, was inaccurate.

20 (B) IMPLEMENTATION.—To the extent that a risk-based per-
21 formance standard established under subsection (b) requires iden-
22 tifying individuals with ties to terrorism—

23 (i) a covered chemical facility—

24 (I) may satisfy its obligation under the standard by
25 using any Federal screening program that periodically
26 vets individuals against the terrorist screening database,
27 or any successor program, including the Personnel Sur-
28 ety Program established under subparagraph (A); and

29 (II) shall—

30 (aa) accept a credential from a Federal screening
31 program described in subclause (I) if an individual
32 who is required to be screened presents the creden-
33 tial; and

34 (bb) address in its site security plan or alter-
35 native security program the measures it will take to
36 verify that a credential or documentation from a
37 Federal screening program described in subclause
38 (I) is current;

39 (ii) visual inspection shall be sufficient to meet the require-
40 ment under clause (i)(II)(bb), but the facility should consider
41 other means of verification, consistent with the facility's as-

1 assessment of the threat posed by acceptance of the credentials;
2 and

3 (iii) the Secretary may not require a covered chemical facil-
4 ity to submit any information about an individual unless the
5 individual—

6 (I) is to be vetted under the Personnel Surety Pro-
7 gram; or

8 (II) has been identified as presenting a terrorism secu-
9 rity risk.

10 (C) RIGHTS UNAFFECTED.—Nothing in this section shall super-
11 secede the ability—

12 (i) of a facility to maintain its own policies regarding the
13 access of individuals to restricted areas or critical assets; or

14 (ii) of an employing facility and a bargaining agent, where
15 applicable, to negotiate as to how the results of a background
16 check may be used by the facility with respect to employment
17 status.

18 (3) AVAILABILITY OF INFORMATION.—The Secretary shall share
19 with the owner or operator of a covered chemical facility any informa-
20 tion that the owner or operator needs to comply with this section.

21 (e) RESPONSIBILITIES OF THE SECRETARY.—

22 (1) IDENTIFICATION OF CHEMICAL FACILITIES OF INTEREST.—In
23 carrying out this subchapter, the Secretary shall consult with the heads
24 of other Federal agencies, States and political subdivisions thereof, rel-
25 evant business associations, and public and private labor organizations
26 to identify all chemical facilities of interest.

27 (2) RISK ASSESSMENT.—

28 (A) IN GENERAL.—For purposes of this subchapter, the Sec-
29 retary shall develop a security risk assessment approach and cor-
30 responding tiering methodology for covered chemical facilities that
31 incorporates the relevant elements of risk, including threat, vulner-
32 ability, and consequence.

33 (B) CRITERIA FOR DETERMINING SECURITY RISK.—The criteria
34 for determining the security risk of terrorism associated with a
35 covered chemical facility shall take into account—

36 (i) relevant threat information;

37 (ii) potential severe economic consequences and the poten-
38 tial loss of human life in the event of the facility's being sub-
39 ject to attack, compromise, infiltration, or exploitation by ter-
40 rorists; and

1 (iii) vulnerability of the facility to attack, compromise, infil-
2 tration, or exploitation by terrorists.

3 (3) CHANGES IN TIERING.—

4 (A) MAINTENANCE OF RECORDS.—The Secretary shall docu-
5 ment the basis for each instance in which—

- 6 (i) tiering for a covered chemical facility is changed; or
7 (ii) a covered chemical facility is determined to no longer
8 be subject to the requirements under this subchapter.

9 (B) REQUIRED INFORMATION.—The records maintained under
10 subparagraph (A) shall include information on whether and how
11 the Secretary confirmed the information that was the basis for the
12 change or determination described in subparagraph (A).

13 (4) SEMIANNUAL PERFORMANCE REPORTING.—Not later than 6
14 months after December 18, 2014, and not less frequently than once
15 every 6 months after that date, the Secretary shall submit to the Com-
16 mittee on Homeland Security and Governmental Affairs of the Senate
17 and the Committee on Homeland Security and the Committee on En-
18 ergy and Commerce of the House of Representatives a report that in-
19 cludes, for the period covered by the report—

20 (A) the number of covered chemical facilities in the United
21 States;

22 (B) information—

23 (i) describing—

24 (I) the number of instances in which the Secretary—

25 (aa) placed a covered chemical facility in a lower
26 risk tier; or

27 (bb) determined that a facility that had pre-
28 viously met the criteria for a covered chemical facil-
29 ity under section 10861(3) of this title no longer
30 met the criteria; and

31 (II) the basis, in summary form, for each action or de-
32 termination under subclause (I); and

33 (ii) that is provided in a sufficiently anonymized form to
34 ensure that the information does not identify any specific fa-
35 cility or company as the source of the information when
36 viewed alone or in combination with other public information;

37 (C) the average number of days spent reviewing site security or
38 an alternative security program for a covered chemical facility
39 prior to approval;

40 (D) the number of covered chemical facilities inspected;

1 (E) the average number of covered chemical facilities inspected
2 per inspector; and

3 (F) any other information that the Secretary determines will be
4 helpful to Congress in evaluating the performance of the Chemical
5 Facility Anti-Terrorism Standards Program.

6 **§ 10863. Protection and sharing of information**

7 (a) IN GENERAL.—Notwithstanding another law, information developed
8 under this subchapter, including vulnerability assessments, site security
9 plans, and other security related information, records, and documents shall
10 be given protections from public disclosure consistent with the protection of
11 similar information under section 70103(d) of title 46.

12 (b) SHARING OF INFORMATION WITH STATES AND LOCAL GOVERN-
13 MENTS.—Nothing in this section shall be construed to prohibit the sharing
14 of information developed under this subchapter, as the Secretary determines
15 appropriate, with State and local government officials possessing a need to
16 know and the necessary security clearances, including law enforcement offi-
17 cials and first responders, for the purpose of carrying out this subchapter,
18 provided that the information may not be disclosed pursuant to any State
19 or local law.

20 (c) SHARING OF INFORMATION WITH FIRST RESPONDERS.—

21 (1) REQUIREMENT.—The Secretary shall provide to State, local, and
22 regional fusion centers (as that term is defined in section 10512(a)(1)
23 of this title) and State and local government officials, as the Secretary
24 determines appropriate, such information as is necessary to help ensure
25 that first responders are properly prepared and provided with the situa-
26 tional awareness needed to respond to security incidents at covered
27 chemical facilities.

28 (2) DISSEMINATION.—The Secretary shall disseminate information
29 under paragraph (1) through a medium or system determined by the
30 Secretary to be appropriate to ensure the secure and expeditious dis-
31 semination of the information to necessary selected individuals.

32 (d) ENFORCEMENT PROCEEDINGS.—In any proceeding to enforce this
33 section, vulnerability assessments, site security plans, and other information
34 submitted to or obtained by the Secretary under this subchapter, and re-
35 lated vulnerability or security information, shall be treated as if the infor-
36 mation were classified information.

37 (e) AVAILABILITY OF INFORMATION.—Notwithstanding another law (in-
38 cluding section 552(b)(3) of title 5), section 552 of title 5 shall not apply
39 to information protected from public disclosure pursuant to subsection (a).

40 (f) SHARING OF INFORMATION WITH MEMBERS OF CONGRESS.—Nothing
41 in this section shall prohibit the Secretary from disclosing information devel-

1 oped under this subchapter to a Member of Congress in response to a re-
2 quest by a Member of Congress.

3 **§ 10864. Civil enforcement**

4 (a) NOTICE OF NONCOMPLIANCE.—

5 (1) IN GENERAL.—If the Secretary determines that a covered chem-
6 ical facility is not in compliance with this subchapter, the Secretary
7 shall—

8 (A) provide the owner or operator of the facility—

9 (i) not later than 14 days after the date on which the Sec-
10 retary makes the determination, a written notification of non-
11 compliance that includes a clear explanation of any deficiency
12 in the security vulnerability assessment or site security plan;
13 and

14 (ii) an opportunity for consultation with the Secretary or
15 the Secretary's designee; and

16 (B) issue to the owner or operator of the facility an order to
17 comply with this subchapter by a date specified by the Secretary
18 in the order, which date shall be not later than 180 days after the
19 date on which the Secretary issues the order.

20 (2) CONTINUED NONCOMPLIANCE.—If an owner or operator remains
21 noncompliant after the procedures outlined in paragraph (1) have been
22 executed, or demonstrates repeated violations of this subchapter, the
23 Secretary may enter an order in accordance with this section assessing
24 a civil penalty, an order to cease operations, or both.

25 (b) CIVIL PENALTIES.—

26 (1) VIOLATIONS OF ORDERS.—Any person who violates an order
27 issued under this subchapter shall be liable for a civil penalty under
28 section 70119(a) of title 46.

29 (2) NON-REPORTING CHEMICAL FACILITIES OF INTEREST.—Any
30 owner of a chemical facility of interest who fails to comply with, or
31 knowingly submits false information under, this subchapter or the
32 CFATS regulations shall be liable for a civil penalty under section
33 70119(a) of title 46.

34 (c) EMERGENCY ORDERS.—

35 (1) IN GENERAL.—Notwithstanding subsection (a) or any site secu-
36 rity plan or alternative security program approved under this sub-
37 chapter, if the Secretary determines that there is an imminent threat
38 of death, serious illness, or severe personal injury, due to a violation
39 of this subchapter or the risk of a terrorist incident that may affect
40 a chemical facility of interest, the Secretary—

1 (A) shall consult with the facility, if practicable, on steps to
2 mitigate the risk; and

3 (B) may order the facility, without notice or opportunity for a
4 hearing, effective immediately or as soon as practicable, to—

5 (i) implement appropriate emergency security measures; or

6 (ii) cease or reduce some or all operations, in accordance
7 with safe shutdown procedures, if the Secretary determines
8 that such a cessation or reduction of operations is the most
9 appropriate means to address the risk.

10 (2) LIMITATION ON DELEGATION.—The Secretary may not delegate
11 the authority under paragraph (1) to any official other than the Direc-
12 tor of the Cybersecurity and Infrastructure Security Agency.

13 (3) LIMITATION ON AUTHORITY.—The Secretary may exercise the
14 authority under this subsection only to the extent necessary to abate
15 the imminent threat determination under paragraph (1).

16 (4) DUE PROCESS FOR FACILITY OWNER OR OPERATOR.—

17 (A) WRITTEN ORDERS.—An order issued by the Secretary
18 under paragraph (1) shall be in the form of a written emergency
19 order that—

20 (i) describes the violation or risk that creates the imminent
21 threat;

22 (ii) states the security measures or order issued or im-
23 posed; and

24 (iii) describes the standards and procedures for obtaining
25 relief from the order.

26 (B) OPPORTUNITY FOR REVIEW.—After issuing an order under
27 paragraph (1) with respect to a chemical facility of interest, the
28 Secretary shall provide for review of the order under section 554
29 of title 5 if a petition for review is filed not later than 20 days
30 after the date on which the Secretary issues the order.

31 (C) EXPIRATION OF EFFECTIVENESS OF ORDER.—If a petition
32 for review of an order is filed under subparagraph (B) and the re-
33 view under subparagraph (B) is not completed by the last day of
34 the 30-day period beginning on the date on which the petition is
35 filed, the order shall vacate automatically at the end of that period
36 unless the Secretary determines, in writing, that the imminent
37 threat providing a basis for the order continues to exist.

38 (d) RIGHT OF ACTION.—Nothing in this subchapter confers upon any in-
39 dividual except the Secretary or his or her designee a right of action against
40 an owner or operator of a covered chemical facility to enforce any provision
41 of this subchapter.

1 **§ 10865. Whistleblower protections**

2 (a) PROCEDURE FOR REPORTING PROBLEMS.—

3 (1) ESTABLISHMENT.—The Secretary shall establish, and provide in-
4 formation to the public regarding, a procedure under which any em-
5 ployee or contractor of a chemical facility of interest may submit a re-
6 port to the Secretary regarding a violation of a requirement under this
7 subchapter.

8 (2) CONFIDENTIALITY.—The Secretary shall keep confidential the
9 identity of an individual who submits a report under paragraph (1),
10 and the report shall be treated as a record containing protected infor-
11 mation to the extent that the report does not consist of publicly avail-
12 able information.

13 (3) ACKNOWLEDGMENT OF RECEIPT.—If a report submitted under
14 paragraph (1) identifies the individual making the report, the Secretary
15 shall promptly respond to the individual directly and shall promptly ac-
16 knowledge receipt of the report.

17 (4) STEPS TO ADDRESS PROBLEMS.—The Secretary—

18 (A) shall review and consider the information provided in any
19 report submitted under paragraph (1); and

20 (B) may take action under section 10864 of this title if nec-
21 essary to address any substantiated violation of a requirement
22 under this subchapter identified in the report.

23 (5) DUE PROCESS FOR FACILITY OWNER OR OPERATOR.—

24 (A) IN GENERAL.—If, on the review described in paragraph (4),
25 the Secretary determines that a violation of a provision of this
26 subchapter, or a regulation prescribed under this subchapter, has
27 occurred, the Secretary may—

28 (i) institute a civil enforcement under section 10864(a) of
29 this title; or

30 (ii) if the Secretary makes the determination under section
31 10864(c) of this title, issue an emergency order.

32 (B) WRITTEN ORDERS.—The action of the Secretary under
33 paragraph (4) shall be in a written form that—

34 (i) describes the violation;

35 (ii) states the authority under which the Secretary is pro-
36 ceeding; and

37 (iii) describes the standards and procedures for obtaining
38 relief from the order.

39 (C) OPPORTUNITY FOR REVIEW.—After taking action under
40 paragraph (4), the Secretary shall provide for review of the action

1 if a petition for review is filed within 20 calendar days of the date
2 of issuance of the order for the action.

3 (D) EXPIRATION OF EFFECTIVENESS OF ORDER.—If a petition
4 for review of an action is filed under subparagraph (C) and the
5 review under that subparagraph is not completed by the end of the
6 30-day period beginning on the date the petition is filed, the ac-
7 tion shall cease to be effective at the end of that period unless the
8 Secretary determines, in writing, that the violation providing a
9 basis for the action continues to exist.

10 (6) RETALIATION PROHIBITED.—

11 (A) IN GENERAL.—An owner or operator of a chemical facility
12 of interest or agent thereof may not discharge an employee or oth-
13 erwise discriminate against an employee with respect to the com-
14 pensation provided to, or terms, conditions, or privileges of the
15 employment of, the employee because the employee (or an indi-
16 vidual acting pursuant to a request of the employee) submitted a
17 report under paragraph (1).

18 (B) EXCEPTION.—An employee shall not be entitled to the pro-
19 tections under this section if the employee—

20 (i) knowingly and willfully makes any false, fictitious, or
21 fraudulent statement or representation; or

22 (ii) uses any false writing or document knowing the writing
23 or document contains any false, fictitious, or fraudulent state-
24 ment or entry.

25 (b) PROTECTED DISCLOSURES.—Nothing in this subchapter shall be con-
26 strued to limit the right of an individual to make any disclosure—

27 (1) protected or authorized under section 2302(b)(8) or 7211 of title
28 5;

29 (2) protected under any other Federal or State law that shields the
30 disclosing individual against retaliation or discrimination for having
31 made the disclosure in the public interest; or

32 (3) to the Special Counsel of an agency, the inspector general of an
33 agency, or any other employee designated by the head of an agency to
34 receive disclosures similar to the disclosures described in paragraphs
35 (1) and (2).

36 (c) PUBLICATION OF RIGHTS.—The Secretary, in partnership with indus-
37 try associations and labor organizations, shall make publicly available both
38 physically and online the rights that an individual who discloses information,
39 including security-sensitive information, regarding problems, deficiencies, or
40 vulnerabilities at a covered chemical facility would have under Federal whis-
41 tleblower protection laws or this subchapter.

1 (d) PROTECTED INFORMATION.—All information contained in a report
2 made under subsection (a) shall be protected in accordance with section
3 10863 of this title.

4 **§ 10866. Relationship to other laws**

5 (a) OTHER FEDERAL LAWS.—Nothing in this subchapter shall be con-
6 strued to supersede, amend, alter, or affect any Federal law that—

7 (1) regulates (including by requiring information to be submitted or
8 made available) the manufacture, distribution in commerce, use, han-
9 dling, sale, other treatment, or disposal of chemical substances or mix-
10 tures; or

11 (2) authorizes or requires the disclosure of any record or information
12 obtained from a chemical facility under any law other than this sub-
13 chapter.

14 (b) STATES AND POLITICAL SUBDIVISIONS.—This subchapter shall not
15 preclude or deny any right of any State or political subdivision of a State
16 to adopt or enforce any regulation, requirement, or standard of performance
17 with respect to chemical facility security that is more stringent than a regu-
18 lation, requirement, or standard of performance issued under this sub-
19 chapter, or otherwise impair any right or jurisdiction of any State with re-
20 spect to chemical facilities within that State, unless there is an actual con-
21 flict between this section and the law of that State.

22 **§ 10867. CFATS regulations**

23 (a) GENERAL AUTHORITY.—The Secretary may, in accordance with chap-
24 ter 5 of title 5, promulgate regulations or amend CFATS regulations that
25 existed 30 days after December 18, 2014, to implement the provisions under
26 this subchapter.

27 (b) EXISTING CFATS REGULATIONS.—

28 (1) IN GENERAL.—Notwithstanding section 4(b) of the Protecting
29 and Securing Chemical Facilities from Terrorist Attacks Act of 2014
30 (Public Law 113–254, 128 Stat. 2919), each CFATS regulation that
31 existed on December 18, 2014, remains in effect unless the Secretary
32 amends, consolidates, or repeals the regulation.

33 (2) REPEAL.—Not later than 30 days after December 18, 2014, the
34 Secretary shall repeal any CFATS regulation that existed on that date
35 that the Secretary determines is duplicative of, or conflicts with, this
36 subchapter.

37 (c) AUTHORITY.—The Secretary shall exclusively rely upon authority pro-
38 vided under this subchapter in—

39 (1) determining compliance with this subchapter;

40 (2) identifying chemicals of interest; and

41 (3) determining security risk associated with a chemical facility.

1 **§ 10868. Small covered chemical facilities**

2 (a) DEFINITION OF SMALL COVERED CHEMICAL FACILITY.—In this sec-
3 tion, the term “small covered chemical facility” means a covered chemical
4 facility that—

5 (1) has fewer than 100 employees employed at the covered chemical
6 facility; and

7 (2) is owned and operated by a small business concern (as defined
8 in section 3 of the Small Business Act (15 U.S.C. 632)).

9 (b) ASSISTANCE TO FACILITIES.—The Secretary may provide guidance
10 and, as appropriate, tools, methodologies, or computer software, to assist
11 small covered chemical facilities in developing the physical security, cyberse-
12 curity, recordkeeping, and reporting procedures required under this sub-
13 chapter.

14 (c) REPORT.—The Secretary shall submit to the Committee on Homeland
15 Security and Governmental Affairs of the Senate and the Committee on
16 Homeland Security and the Committee on Energy and Commerce of the
17 House of Representatives a report on best practices that may assist small
18 covered chemical facilities in the development of physical security best prac-
19 tices.

20 **§ 10869. Outreach to chemical facilities of interest**

21 The Secretary shall establish an outreach implementation plan, in coordi-
22 nation with the heads of other appropriate Federal and State agencies, rel-
23 evant business associations, and public and private labor organizations, to—

24 (1) identify chemical facilities of interest; and

25 (2) make available compliance assistance materials and information
26 on education and training.

27 **§ 10870. Termination**

28 The authority provided under this subchapter terminates on July 27,
29 2023.

30 **Subchapter IX—Miscellaneous**

31 **§ 10881. Duties and authorities relating to .gov internet do-**
32 **main**

33 (a) PURPOSE.—The purpose of the .gov internet domain program is to—

34 (1) legitimize and enhance public trust in government entities and
35 their online services;

36 (2) facilitate trusted electronic communication and connections to
37 and from government entities;

38 (3) provide simple and secure registration of .gov internet domains;

39 (4) improve the security of the services hosted within these .gov
40 internet domains, and of the .gov namespace in general; and

1 (5) enable the discoverability of government services to the public
2 and to domain registrants.

3 (b) DEFINITIONS.—In this section:

4 (1) AGENCY.—The term “agency” has the meaning given the term
5 in section 3502 of title 44.

6 (2) DIRECTOR.—The term “Director” means the Director of the Cy-
7 bersecurity and Infrastructure Security Agency.

8 (3) ONLINE SERVICE.—The term “online service” means an internet-
9 facing service, including a website, email, a virtual private network, or
10 a custom application.

11 (4) STATE.—The term “State” means a State, the District of Co-
12 lumbia, Puerto Rico, Guam, American Samoa, the Virgin Islands,
13 Northern Mariana Islands, and a possession of the United States.

14 (c) TRANSITION.—The Director shall operationally administer the .gov
15 internet domain program formerly operated by the General Services Admin-
16 istration under title 41, Code of Federal Regulations, and shall publish on
17 a publicly available website the requirements for domain registrants as de-
18 scribed in subsection (d). The requirements in part 102–173 of title 41,
19 Code of Federal Regulations, are rescinded.

20 (d) AVAILABILITY OF .GOV INTERNET DOMAIN.—The Director shall
21 make .gov internet domain name registration services, as well as any sup-
22 porting services described in subsection (g), generally available—

23 (1) to any Federal, State, local, or territorial government entity, or
24 other publicly controlled entity, including any Tribal government recog-
25 nized by the Federal Government or a State government, that complies
26 with the requirements for registration developed by the Director as de-
27 scribed in subsection (e);

28 (2) without conditioning registration on the sharing of any informa-
29 tion with the Director or any other Federal entity, other than the infor-
30 mation required to meet the requirements described in subsection (e);
31 and

32 (3) without conditioning registration on participation in any separate
33 service offered by the Director or any other Federal entity.

34 (e) REQUIREMENTS.—The Director, with the approval of the Director of
35 the Office of Management and Budget for agency .gov internet domain re-
36 quirements and in consultation with the Director of the Office of Manage-
37 ment and Budget for .gov internet domain requirements for entities that are
38 not agencies, shall establish and publish on a publicly available website re-
39 quirements for the registration and operation of .gov internet domains suffi-
40 cient to—

1 (1) minimize the risk of .gov internet domains whose names could
2 mislead or confuse users;

3 (2) establish that .gov internet domains may not be used for com-
4 mercial or political campaign purposes;

5 (3) ensure that domains are registered and maintained only by au-
6 thorized individuals; and

7 (4) limit the sharing or use of any information obtained through the
8 administration of the .gov internet domain with any other Department
9 component or any other agency for a purpose other than the adminis-
10 tration of the .gov internet domain, the services described in subsection
11 (g), and the requirements for establishing a .gov inventory described
12 in subsection (k).

13 (f) EXECUTIVE BRANCH.—

14 (1) IN GENERAL.—The Director of the Office of Management and
15 Budget shall establish applicable processes and guidelines for the reg-
16 istration and acceptable use of .gov internet domains by agencies.

17 (2) APPROVAL REQUIRED.—The Director shall obtain the approval
18 of the Director of the Office of Management and Budget before reg-
19 istering a .gov internet domain name for an agency.

20 (3) COMPLIANCE.—Each agency shall ensure that any website or
21 digital service of the agency that uses a .gov internet domain is in com-
22 pliance with the 21st Century Integrated Digital Experience Act (44
23 U.S.C. 3501 note) and implementation guidance issued pursuant to
24 that Act.

25 (g) SUPPORTING SERVICES.—

26 (1) IN GENERAL.—The Director may provide services to the entities
27 described in subsection (d)(1) specifically intended to support the secu-
28 rity, privacy, reliability, accessibility, and speed of registered .gov inter-
29 net domains.

30 (2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be
31 construed to—

32 (A) limit other authorities of the Director to provide services or
33 technical assistance to an entity described in subsection (d)(1); or

34 (B) establish new authority for services other than those the
35 purpose of which expressly supports the operation of .gov internet
36 domains and the needs of .gov internet domain registrants.

37 (h) FEES.—

38 (1) IN GENERAL.—The Director may provide a service relating to
39 the availability of the .gov internet domain program, including .gov
40 internet domain name registration services described in subsection (d)
41 and supporting services described in subsection (g), to entities de-

1 scribed in subsection (d)(1) with or without reimbursement, including
2 variable pricing.

3 (2) PRICING.—The total fees collected for new .gov internet domain
4 registrants or annual renewals of .gov internet domains shall not ex-
5 ceed the direct operational expenses of improving, maintaining, and op-
6 erating the .gov internet domain, .gov internet domain services, and
7 .gov internet domain supporting services.

8 (3) ENTITIES NOT AGENCIES.—During the 5-year period beginning
9 on December 27, 2020, a fee charged to entities that are not agencies
10 for new .gov internet domain registrants or annual renewals of .gov
11 internet domains shall be not more than the amount of the fee charged
12 for the registration or renewal as of October 1, 2019.

13 (i) CONSULTATION.—The Director shall consult with the Director of the
14 Office of Management and Budget, the Administrator of General Services,
15 other civilian Federal agencies as appropriate, and entities representing
16 State, local, Tribal, or territorial governments in developing the strategic di-
17 rection of the .gov internet domain and in establishing requirements under
18 subsection (e), in particular on matters of privacy, accessibility, trans-
19 parency, and technology modernization.

20 (j) REFERENCE GUIDE.—Not later than 1 year after December 27, 2020,
21 the Director, in consultation with the Administrator of General Services and
22 entities representing State, local, Tribal, or territorial governments, shall de-
23 velop and publish on a publicly available website a reference guide for mi-
24 grating online services to the .gov internet domain, which shall include

25 (1) process and technical information on how to carry out a migra-
26 tion of common categories of online services, such as web and email
27 services;

28 (2) best practices for cybersecurity pertaining to registration and op-
29 eration of a .gov internet domain; and

30 (3) references to contract vehicles and other private-sector resources
31 vetted by the Director that may assist in performing the migration.

32 (k) .GOV INVENTORY.—

33 (1) IN GENERAL.—The Director shall, on a continuous basis—

34 (A) inventory all hostnames and services in active use within the
35 .gov internet domain; and

36 (B) provide the data described in subparagraph (A) to domain
37 registrants at no cost.

38 (2) REQUIREMENTS.—In carrying out paragraph (1)—

39 (A) the Director may collect the data through analysis of public
40 and non-public sources, including commercial data sets;

1 (B) the Director shall share with Federal and non-Federal do-
2 main registrants all unique hostnames and services discovered
3 within the zone of their registered domain;

4 (C) the Director shall share any data or information collected
5 or used in the management of the .gov internet domain name reg-
6 istration services relating to Federal executive branch registrants
7 with the Director of the Office of Management and Budget for the
8 purpose of fulfilling the duties of the Director of the Office of
9 Management and Budget under section 3553 of title 44;

10 (D) the Director shall publish on a publicly available website
11 discovered hostnames that describe publicly accessible agency
12 websites, to the extent consistent with the security of Federal in-
13 formation systems but with the presumption of disclosure;

14 (E) the Director may publish on a publicly available website any
15 analysis conducted and data collected relating to compliance with
16 Federal mandates and industry best practices, to the extent con-
17 sistent with the security of Federal information systems but with
18 the presumption of disclosure; and

19 (F) the Director shall—

20 (i) collect information on the use of non-.gov internet do-
21 main suffixes by agencies for their official online services;

22 (ii) collect information on the use of non-.gov internet do-
23 main suffixes by State, local, Tribal, and territorial govern-
24 ments; and

25 (iii) publish the information collected under clause (i) on a
26 publicly available website to the extent consistent with the se-
27 curity of the Federal information systems, but with the pre-
28 sumption of disclosure.

29 (3) NATIONAL SECURITY COORDINATION.—

30 (A) IN GENERAL.—In carrying out this subsection, the Director
31 shall inventory, collect, and publish hostnames and services in a
32 manner consistent with the protection of national security infor-
33 mation.

34 (B) LIMITATION.—The Director may not inventory, collect, or
35 publish hostnames or services under this subsection if the Direc-
36 tor, in coordination with other heads of agencies, as appropriate,
37 determines that the collection or publication would—

38 (i) disrupt a law enforcement investigation;

39 (ii) endanger national security or intelligence activities;

40 (iii) impede national defense activities or military oper-
41 ations; or

1 (iv) hamper security remediation actions.

2 (4) STRATEGY.—Not later than 180 days after December 27, 2020,
3 the Director shall develop and submit to the Committee on Homeland
4 Security and Governmental Affairs and the Committee on Rules and
5 Administration of the Senate and the Committee on Homeland Secu-
6 rity, the Committee on Oversight and Reform, and the Committee on
7 House Administration of the House of Representatives a strategy to
8 utilize the information collected under this subsection for countering
9 malicious cyber activity.

10 **§ 10882. Intelligence and cybersecurity diversity fellowship**
11 **program**

12 (a) DEFINITIONS.—In this section:

13 (1) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appro-
14 priate committees of Congress” means—

15 (A) the Committee on Homeland Security and Governmental
16 Affairs and the Select Committee on Intelligence of the Senate;
17 and

18 (B) the Committee on Homeland Security and the Permanent
19 Select Committee on Intelligence of the House of Representatives.

20 (2) EXCEPTED SERVICE.—The term “excepted service” has the
21 meaning given that term in section 2103 of title 5.

22 (3) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term
23 “historically Black college or university” has the meaning given the
24 term “part B institution” in section 322 of the Higher Education Act
25 of 1965 (20 U.S.C. 1061).

26 (4) INSTITUTION OF HIGHER LEARNING.—The term “institution of
27 higher learning” has the meaning given that term in section 101 of the
28 Higher Education Act of 1965 (20 U.S.C. 1001).

29 (5) MINORITY-SERVING INSTITUTION.—The term “minority-serving
30 institution” means an institution of higher education described in sec-
31 tion 371(a) of the Higher Education Act of 1965 (20 U.S.C.
32 1067q(a)).

33 (b) PROGRAM.—The Secretary shall carry out an intelligence and cyberse-
34 curity diversity fellowship program (in this section referred to as the “Pro-
35 gram”) under which an eligible individual may—

36 (1) participate in a paid internship at the Department that relates
37 to intelligence, cybersecurity, or some combination of intelligence and
38 cybersecurity;

39 (2) receive tuition assistance from the Secretary; and

40 (3) on graduation from an institution of higher education and suc-
41 cessful completion of the Program (as defined by the Secretary), re-

1 ceive an offer of employment to work in an intelligence or cybersecurity
2 position of the Department that is in the excepted service.

3 (c) ELIGIBILITY.—To be eligible to participate in the Program, an indi-
4 vidual shall—

5 (1) be a citizen of the United States; and

6 (2) as of the date of submitting the application to participate in the
7 Program—

8 (A) have a cumulative grade point average of at least 3.2 on
9 a 4.0 scale;

10 (B) be a socially disadvantaged individual (as that term is de-
11 fined in section 124.103 of title 13, Code of Federal Regulations,
12 or a successor regulation); and

13 (C) be a sophomore, junior, or senior at an institution of higher
14 education.

15 (d) DIRECT HIRE AUTHORITY.—If an individual who receives an offer of
16 employment under subsection (b)(3) accepts the offer, the Secretary shall
17 appoint, without regard to provisions of subchapter I of chapter 33 of title
18 5 (except for section 3328 of title 5) the individual to the position specified
19 in the offer.

20 (e) REPORTS.—Not later than 1 year after December 27, 2020, and on
21 an annual basis thereafter, the Secretary shall submit to the appropriate
22 committees of Congress a report on the Program. Each report shall include,
23 with respect to the most recent year, the following:

24 (1) A description of outreach efforts by the Secretary to raise aware-
25 ness of the Program among institutions of higher education in which
26 eligible individuals are enrolled.

27 (2) Information on specific recruiting efforts conducted by the Sec-
28 retary to increase participation in the Program.

29 (3) The number of individuals participating in the Program, listed
30 by the institution of higher education in which the individual is enrolled
31 at the time of participation, and information on the nature of the par-
32 ticipation, including on whether the duties of the individual under the
33 Program relate primarily to intelligence or to cybersecurity.

34 (4) The number of individuals who accepted an offer of employment
35 under the Program and an identification of the element in the Depart-
36 ment to which each individual was appointed.

37 **§ 10883. Cybersecurity State Coordinator**

38 (a) DEFINITIONS.—In this section:

39 (1) AGENCY.—The term “Agency” means the Cybersecurity and In-
40 frastructure Security Agency

1 (2) DIRECTOR.—The term “Director” means the Director of the Cy-
2 bersecurity and Infrastructure Security Agency.

3 (b) APPOINTMENT.—The Director shall appoint an employee of the Agen-
4 cy in each State, with the appropriate cybersecurity qualifications and ex-
5 pertise, who shall serve as the Cybersecurity State Coordinator.

6 (c) DUTIES.—The duties of a Cybersecurity State Coordinator appointed
7 under subsection (b) shall include—

8 (1) building strategic public- and, on a voluntary basis, private-sector
9 relationships, including by advising on establishing governance struc-
10 tures to facilitate the development and maintenance of secure and resil-
11 ient infrastructure;

12 (2) serving as the Federal cybersecurity risk advisor and supporting
13 preparation, response, and remediation efforts relating to cybersecurity
14 risks and incidents;

15 (3) facilitating the sharing of cyber threat information to improve
16 understanding of cybersecurity risks and situational awareness of cy-
17 bersecurity incidents;

18 (4) raising awareness of the financial, technical, and operational re-
19 sources available from the Federal Government to non-Federal entities
20 to increase resilience against cyber threats;

21 (5) supporting training, exercises, and planning for continuity of op-
22 erations to expedite recovery from cybersecurity incidents, including
23 ransomware;

24 (6) serving as a principal point of contact for non-Federal entities
25 to engage, on a voluntary basis, with the Federal Government on pre-
26 paring for, managing, and responding to cybersecurity incidents;

27 (7) assisting non-Federal entities in developing and coordinating vul-
28 nerability disclosure programs consistent with Federal and information
29 security industry standards;

30 (8) assisting State, local, Tribal, and territorial governments, on a
31 voluntary basis, in the development of State cybersecurity plans;

32 (9) coordinating with appropriate officials in the Agency; and

33 (10) performing such other duties as determined necessary by the
34 Director to achieve the goal of managing cybersecurity risks in the
35 United States and reducing the impact of cyber threats to non-Federal
36 entities.

37 (d) REPORTING STRUCTURE AND COORDINATION PROCESSES AND PRO-
38 CEDURES.—The Director shall establish and submit to the Committee on
39 Homeland Security and Governmental Affairs of the Senate and the Com-
40 mittee on Homeland Security of the House of Representatives a plan de-

1 scribing the reporting structure and coordination processes and procedures
2 of Cybersecurity State Coordinators in the Agency.

3 (e) FEEDBACK.—The Director shall consult with relevant State, local,
4 Tribal, and territorial officials regarding the appointment, and State, local,
5 Tribal, and territorial officials and other non-Federal entities regarding the
6 performance, of the Cybersecurity State Coordinator of a State.

7 (f) OVERSIGHT.—The Director shall establish and submit to the Com-
8 mittee on Homeland Security and Governmental Affairs of the Senate and
9 the Committee on Homeland Security of the House of Representatives a
10 briefing on the placement and efficacy of the Cybersecurity State Coordina-
11 tors appointed under subsection (b) and the coordination plan required
12 under subsection (d)—

13 (1) not later than 1 year after January 1, 2021; and

14 (2) not later than 2 years after providing the 1st briefing under this
15 subsection.

16 (g) RULE OF CONSTRUCTION.—Nothing in this section may be construed
17 to affect or otherwise modify the authority of Federal law enforcement agen-
18 cies with respect to investigations relating to cybersecurity incidents.

19 **§ 10884. Sector Risk Management Agencies**

20 (a) DEFINITIONS.—In this section:

21 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “approp-
22 riate congressional committees” means—

23 (A) the Committee on Homeland Security and the Committee
24 on Armed Services of the House of Representatives; and

25 (B) the Committee on Homeland Security and Governmental
26 Affairs and the Committee on Armed Services of the Senate.

27 (2) CRITICAL INFRASTRUCTURE.—The term “critical infrastructure”
28 has the meaning given that term in section 1016 of the Critical Infra-
29 structures Protection Act of 2001 (42 U.S.C. 5195c).

30 (3) DIRECTOR.—The term “Director” means the Director of the Cy-
31 bersecurity and Infrastructure Security Agency.

32 (4) SECTOR RISK MANAGEMENT AGENCY.—The term “sector risk
33 management agency” has the meaning given that term in section
34 10701 of this title.

35 (b) CRITICAL INFRASTRUCTURE SECTOR DESIGNATION.—

36 (1) INITIAL REVIEW.—Not later than 180 days after January 1,
37 2021, the Secretary, in consultation with the heads of Sector Risk
38 Management Agencies, shall—

39 (A) review the current framework for securing critical infra-
40 structure, as described in section 10702(a)(1)(D) of this title and
41 Presidential Policy Directive 21; and

1 (B) submit to the President and appropriate congressional com-
2 mittees a report that includes—

3 (i) information relating to—

4 (I) the analysis framework or methodology used to—

5 (aa) evaluate the current framework for securing
6 critical infrastructure referred to in subparagraph
7 (A); and

8 (bb) develop recommendations to—

9 (AA) revise the current list of critical infra-
10 structure sectors designated pursuant to Presi-
11 dential Policy Directive 21, a successor or re-
12 lated document, or a policy; or

13 (BB) identify and designate any subsectors
14 of those sectors; and

15 (II) the data, metrics, and other information used to
16 develop the recommendations required under clause (ii);
17 and

18 (ii) recommendations relating to—

19 (I) revising—

20 (aa) the current framework for securing critical
21 infrastructure referred to in subparagraph (A);

22 (bb) the current list of critical infrastructure sec-
23 tors designated pursuant to Presidential Policy Di-
24 rective 21, a successor or related document, or a
25 policy; or

26 (cc) the identification and designation of any sub-
27 sectors of those sectors; and

28 (II) any revisions to the list of designated Federal de-
29 partments or agencies that serve as the Sector Risk
30 Management Agency for a sector or subsector of that
31 sector, necessary to comply with paragraph (3)(B).

32 (2) PERIODIC EVALUATION BY SECRETARY.—At least once every 5
33 years, the Secretary, in consultation with the Director and the heads
34 of Sector Risk Management Agencies, shall—

35 (A) evaluate the current list of designated critical infrastructure
36 sectors and subsectors of those sectors and the appropriateness of
37 Sector Risk Management Agency designations, as set forth in
38 Presidential Policy Directive 21, a successor or related document,
39 or a policy; and

40 (B) recommend, as appropriate, to the President—

1 (i) revisions to the current list of designated critical infra-
2 structure sectors or subsectors of those sectors; and

3 (ii) revisions to the designation of a Federal department or
4 agency designated as the Sector Risk Management Agency for
5 a sector or subsector of that sector.

6 (3) REVIEW AND REVISION BY THE PRESIDENT.—Not later than 180
7 days after the Secretary submits a recommendation pursuant to para-
8 graph (1) or (2), the President shall—

9 (A) review the recommendation and revise, as appropriate, the
10 designation of a critical infrastructure sector or subsector or the
11 designation of a Sector Risk Management Agency; and

12 (B) submit to the appropriate congressional committees, the
13 Majority and Minority Leaders of the Senate, and the Speaker
14 and Minority Leader of the House of Representatives, a report
15 that includes—

16 (i) an explanation with respect to the basis for accepting
17 or rejecting the recommendations of the Secretary; and

18 (ii) information relating to the analysis framework, meth-
19 odology, metrics, and data used to—

20 (I) evaluate the current framework for securing crit-
21 ical infrastructure referred to in paragraph (1)(A); and

22 (II) develop—

23 (aa) recommendations to revise—

24 (AA) the list of critical infrastructure sectors
25 designated pursuant to Presidential Policy Di-
26 rective 21, a successor or related document, or
27 a policy; or

28 (BB) the designation of any subsectors of
29 those sectors; and

30 (bb) the recommendations of the Secretary.

31 (4) PUBLICATION.—Any designation of critical infrastructure sectors
32 shall be published in the Federal Register.

33 (c) DUTIES.—

34 (1) IN GENERAL.—Consistent with applicable law, Presidential direc-
35 tives, Federal regulations, and strategic guidance from the Secretary,
36 each Sector Risk Management Agency, in coordination with the Direc-
37 tor, shall—

38 (A) provide specialized sector-specific expertise to critical infra-
39 structure owners and operators in its designated critical infra-
40 structure sector or subsector of that sector; and

1 (B) support programs and associated activities of that sector or
2 subsector of that sector.

3 (2) IMPLEMENTATION.—In carrying out this subsection, Sector Risk
4 Management Agencies shall—

5 (A) coordinate with the Department and, as appropriate, other
6 relevant Federal departments and agencies;

7 (B) collaborate with critical infrastructure owners and operators
8 in the designated critical infrastructure sector or subsector of that
9 sector; and

10 (C) coordinate with independent regulatory agencies, and State,
11 local, Tribal, and territorial entities, as appropriate.

12 (3) RESPONSIBILITIES.—Consistent with applicable law, Presidential
13 directives, Federal regulations, and strategic guidance from the Sec-
14 retary, each Sector Risk Management Agency shall utilize its special-
15 ized expertise regarding its designated critical infrastructure sector or
16 subsector of that sector and authorities under applicable law—

17 (A) to support sector risk management, in coordination with the
18 Director, including—

19 (i) establishing and carrying out programs to assist critical
20 infrastructure owners and operators in the designated sector
21 or subsector of that sector in identifying, understanding, and
22 mitigating threats, vulnerabilities, and risks to their systems
23 or assets, or in a region, sector, or subsector of that sector;
24 and

25 (ii) recommending security measures to mitigate the con-
26 sequences of destruction, compromise, and disruption of sys-
27 tems and assets;

28 (B) to assess sector risk, in coordination with the Director, in-
29 cluding—

30 (i) identifying, assessing, and prioritizing risks in the des-
31 igned sector or subsector of that sector, considering phys-
32 ical security and cybersecurity threats, vulnerabilities, and
33 consequences; and

34 (ii) supporting national risk assessment efforts led by the
35 Department;

36 (C) to oversee sector coordination, including—

37 (i) serving as a day-to-day Federal interface for the
38 prioritization and coordination of sector-specific activities and
39 responsibilities under this title;

1 (ii) serving as the Federal Government coordinating council
2 chair for the designated sector or subsector of that sector;
3 and

4 (iii) participating in cross-sector coordinating councils, as
5 appropriate;

6 (D) to facilitate, in coordination with the Director, the sharing
7 with the Department and other appropriate Federal departments
8 of information regarding physical security and cybersecurity
9 threats in the designated sector or subsector of that sector, includ-
10 ing—

11 (i) facilitating, in coordination with the Director, access to,
12 and exchange of, information and intelligence necessary to
13 strengthen the security of critical infrastructure, including
14 through Information Sharing and Analysis Organizations and
15 the National Cybersecurity and Communications Integration
16 Center established pursuant to section 10706 of this title;

17 (ii) facilitating the identification of intelligence needs and
18 priorities of critical infrastructure owners and operators in
19 the designated sector or subsector of that sector, in coordina-
20 tion with the Director of National Intelligence and the heads
21 of other Federal departments and agencies, as appropriate;

22 (iii) providing the Director, and facilitating awareness in
23 the designated sector or subsector of that sector, of ongoing,
24 and where possible, real-time awareness of identified threats,
25 vulnerabilities, mitigations, and other actions related to the
26 security of the sector or subsector of that sector; and

27 (iv) supporting the reporting requirements of the Depart-
28 ment under applicable law by providing, on an annual basis,
29 sector-specific critical infrastructure information;

30 (E) to support incident management, including—

31 (i) supporting, in coordination with the Director, incident
32 management and restoration efforts during or following a se-
33 curity incident; and

34 (ii) supporting the Director, on request, in national cyber-
35 security asset response activities for critical infrastructure;
36 and

37 (F) to contribute to emergency preparedness efforts, includ-
38 ing—

39 (i) coordinating with critical infrastructure owners and op-
40 erators in the designated sector or subsector of that sector
41 and the Director in the development of planning documents

1 for coordinated action in the event of a natural disaster, act
2 of terrorism, or other man-made disaster or emergency;

3 (ii) participating in and, in coordination with the Director,
4 conducting or facilitating, exercises and simulations of poten-
5 tial natural disasters, acts of terrorism, or other man-made
6 disasters or emergencies in the designated sector or subsector
7 of that sector; and

8 (iii) supporting the Department and other Federal depart-
9 ments or agencies in developing planning documents or con-
10 ducting exercises or simulations when relevant to the des-
11 ignated sector or subsector of that sector.

12 (d) REPORT AND AUDITING.—Not later than 2 years after January 1,
13 2021 and every 4 years thereafter for 12 years, the Comptroller General
14 shall submit to the Committee on Homeland Security of the House of Rep-
15 resentatives and the Committee on Homeland Security and Governmental
16 Affairs of the Senate a report on the effectiveness of Sector Risk Manage-
17 ment Agencies in carrying out their responsibilities under subsection (c)(3).

18 (e) REFERENCES.—Any reference to a Sector Specific Agency (including
19 any permutation or conjugation of Sector Specific Agency) in a law, regula-
20 tion, map, document, record, or other paper of the United States shall be
21 deemed—

22 (1) to be a reference to the Sector Risk Management Agency of the
23 relevant critical infrastructure sector; and

24 (2) to have the meaning given the term “sector risk management
25 agency” in section 10701 of this title.

26 **§ 10885. National Cyber Director**

27 (a) DEFINITIONS.—In this section:

28 (1) CYBER ATTACK OR CYBER CAMPAIGN OF SIGNIFICANT CON-
29 SEQUENCE.—The term “cyber attack or cyber campaign of significant
30 consequence” means an incident or series of incidents that has the pur-
31 pose or effect of—

32 (A) causing a significant disruption to the confidentiality, integ-
33 rity, or availability of a Federal information system;

34 (B) harming, or otherwise significantly compromising the provi-
35 sion of service by, a computer or network of computers that sup-
36 port 1 or more entities in a critical infrastructure sector;

37 (C) significantly compromising the provision of services by 1 or
38 more entities in a critical infrastructure sector;

39 (D) causing a significant misappropriation of funds or economic
40 resources, trade secrets, personal identifiers, or financial informa-

- 1 (iii) efforts to understand and deter malicious cyber activ-
2 ity;
- 3 (iv) efforts to increase the security of information and com-
4 munications technology and services and to promote national
5 supply chain risk management and vendor security;
- 6 (v) diplomatic and other efforts to develop norms and inter-
7 national consensus around responsible state behavior in cyber-
8 space;
- 9 (vi) awareness and adoption of emerging technology that
10 may enhance, augment, or degrade the cybersecurity posture
11 of the United States; and
- 12 (vii) engaging in such other cybersecurity matters as the
13 President considers appropriate;
- 14 (B) offer advice and consultation to the National Security Coun-
15 cil and its staff, the Homeland Security Council and its staff, and
16 relevant Federal departments and agencies, for their consider-
17 ation, relating to the development and coordination of national
18 cyber policy and strategy, including the National Cyber Strategy;
- 19 (C) lead the coordination of implementation of national cyber
20 policy and strategy, including the National Cyber Strategy, by—
21 (i) in coordination with the heads of relevant Federal de-
22 partments or agencies, monitoring and assessing the effective-
23 ness, including cost-effectiveness, of the implementation of
24 the national cyber policy and strategy by Federal departments
25 and agencies;
- 26 (ii) making recommendations, relevant to changes in the
27 organization, personnel, and resource allocation and to poli-
28 cies of Federal departments and agencies, to the heads of rel-
29 evant Federal departments and agencies to implement the na-
30 tional cyber policy and strategy;
- 31 (iii) reviewing the annual budget proposals for relevant
32 Federal departments and agencies and advising the heads of
33 those departments and agencies whether the proposals are
34 consistent with the national cyber policy and strategy;
- 35 (iv) continuously assessing and making relevant rec-
36 ommendations to the President on the appropriate level of in-
37 tegration and interoperability across the Federal cyber cen-
38 ters;
- 39 (v) coordinating with the Attorney General, the Federal
40 Chief Information Officer, the Director of the Office of Man-
41 agement and Budget, the Director of National Intelligence,

1 and the Director of the Cybersecurity and Infrastructure Se-
2 curity Agency, on the streamlining of Federal policies and
3 guidelines, including with respect to implementation of sub-
4 chapter II of chapter 35 of title 44, and, as appropriate or
5 applicable, regulations relating to cybersecurity;

6 (vi) reporting annually to the President, the Assistant to
7 the President for National Security Affairs, and Congress on
8 the state of the cybersecurity posture of the United States,
9 the effectiveness of the national cyber policy and strategy,
10 and the status of the implementation of the national cyber
11 policy and strategy by Federal departments and agencies; and

12 (vii) engaging in such other activity as the President con-
13 sidered appropriate to further the national cyber policy and
14 strategy;

15 (D) lead the coordination of the development, and ensure imple-
16 mentation by the Federal Government, of integrated incident re-
17 sponse to a cyber attack or cyber campaign of significant con-
18 sequence, including—

19 (i) ensuring and facilitating coordination among relevant
20 Federal departments and agencies in the development of inte-
21 grated operational plans, processes, and playbooks, including
22 for incident response, that feature—

23 (I) clear lines of authority and lines of effort across
24 the Federal Government;

25 (II) authorities that have been delegated to an appro-
26 priate level to facilitate effective operational responses
27 across the Federal Government; and

28 (III) support for the integration of defensive cyber
29 plans and capabilities with offensive cyber plans and ca-
30 pabilities in a manner consistent with improving the cy-
31 bersecurity posture of the United States;

32 (ii) ensuring the exercising of defensive operational plans,
33 processes, and playbooks for incident response;

34 (iii) ensuring the updating of defensive operational plans,
35 processes, and playbooks for incident response as needed to
36 keep them updated; and

37 (iv) reviewing and ensuring that defensive operational
38 plans, processes, and playbooks improve coordination with rel-
39 evant private-sector entities, as appropriate;

40 (E) prepare the response by the Federal Government to a cyber
41 attack or cyber campaign of significant consequence across Fed-

1 eral departments and agencies with responsibilities pertaining to
2 cybersecurity and with the relevant private-sector entities, includ-
3 ing—

4 (i) developing for the approval of the President, in coordi-
5 nation with the Assistant to the President for National Secu-
6 rity Affairs and the heads of relevant Federal departments
7 and agencies, operational priorities, requirements, and plans;

8 (ii) ensuring incident response is executed consistent with
9 the plans described in clause (i); and

10 (iii) ensuring relevant Federal department and agency con-
11 sultation with relevant private-sector entities in incident re-
12 sponse;

13 (F) coordinate and consult with private-sector leaders on cyber-
14 security and emerging technology issues in support of, and in co-
15 ordination with, the Director of the Cybersecurity and Infrastruc-
16 ture Security Agency, the Director of National Intelligence, and
17 the heads of other Federal departments and agencies, as appro-
18 priate;

19 (G) annually report to Congress on cybersecurity threats and
20 issues facing the United States, including any new or emerging
21 technologies that may affect national security, economic pros-
22 perity, or enforcing the rule of law; and

23 (H) be responsible for such other functions as the President
24 may direct.

25 (2) ADDITIONAL DUTIES.—

26 (A) IN GENERAL.—The Director may—

27 (i) serve as the senior representative to any organization
28 that the President may establish for the purpose of providing
29 the President advice on cybersecurity; and

30 (ii) subject to subparagraph (B), be included as a partici-
31 pant in preparations for and, when appropriate, the execution
32 of domestic and international summits and other inter-
33 national meetings at which cybersecurity is a major topic.

34 (B) COORDINATION WITH SECRETARY OF STATE.—In acting
35 under subparagraph (A)(ii) in the case of a summit or a meeting
36 with an international partner, the Director shall act in coordina-
37 tion with the Secretary of State.

38 (3) DELEGATION OF AUTHORITY.—The Director may—

39 (A) delegate any of the Director's functions, powers, and duties
40 to such officers and employees of the Office as the Director con-
41 siders appropriate; and

1 (B) authorize such successive redelegations of the functions,
2 powers, and duties to such officers and employees of the Office as
3 the Director considers appropriate.

4 (e) POWERS.—

5 (1) IN GENERAL.—The Director may, for the purposes of carrying
6 out the functions of the Director under this section—

7 (A) subject to the civil service and classification laws, select, ap-
8 point, employ, and fix the compensation of such officers and em-
9 ployees as are necessary and prescribe their duties, except that not
10 more than 75 individuals may be employed without regard to any
11 provision of law regulating the employment or compensation at
12 rates not to exceed the basic rate of basic pay payable for level
13 IV of the Executive Schedule under section 5315 of title 5;

14 (B) employ experts and consultants in accordance with section
15 3109 of title 5, and compensate individuals so employed for each
16 day (including travel time) at rates not in excess of the maximum
17 rate of basic pay for grade GS-15 as provided in section 5332 of
18 title 5, and while those experts and consultants are so serving
19 away from their homes or regular place of business, pay those em-
20 ployees travel expenses and per diem in lieu of subsistence at rates
21 authorized by section 5703 of title 5 for individuals in Federal
22 Government service employed intermittently;

23 (C) accept officers or employees of the United States or mem-
24 bers of the Armed Forces on a detail from an element of the intel-
25 ligence community (as that term is defined in section 3 of the Na-
26 tional Security Act of 1947 (50 U.S.C. 3003) or from another ele-
27 ment of the Federal Government on a nonreimbursable basis, as
28 jointly agreed to by the heads of the receiving and detailing ele-
29 ments, for a period not to exceed 3 years;

30 (D) promulgate such rules and regulations as may be necessary
31 to carry out the functions, powers, and duties vested in the Direc-
32 tor;

33 (E) utilize, with their consent, the services, personnel, and facili-
34 ties of other Federal agencies;

35 (F) enter into and perform such contracts, leases, cooperative
36 agreements, or other transactions as may be necessary in the con-
37 duct of the work of the Office and on such terms as the Director
38 may determine appropriate, with a Federal agency, or with a pub-
39 lic or private person or entity;

40 (G) accept voluntary and uncompensated services, notwith-
41 standing the provisions of section 1342 of title 31;

1 (H) adopt an official seal, which shall be judicially noticed; and

2 (I) provide, where authorized by law, copies of documents to
3 persons at cost, except that any funds so received shall be credited
4 to, and be available for use from, the account from which expendi-
5 tures relating to copying documents were made.

6 (2) RULES OF CONSTRUCTION REGARDING DETAILS.— Nothing in
7 paragraph (1)(C) may be construed as imposing any limitation on any
8 other authority for reimbursable or nonreimbursable details. A nonre-
9 reimbursable detail made pursuant to paragraph (1)(C) shall not be con-
10 sidered an augmentation of the appropriations of the receiving element
11 of the Office of the National Cyber Director.

12 (f) RULES OF CONSTRUCTION.—Nothing in this section may be construed
13 as—

14 (1) modifying any authority or responsibility, including any oper-
15 ational authority or responsibility of any head of a Federal department
16 or agency;

17 (2) authorizing the Director or an individual acting under the au-
18 thority of the Director to interfere with or to direct a criminal or na-
19 tional security investigation, arrest, search, seizure, or disruption oper-
20 ation;

21 (3) amending a legal restriction that was in effect on December 31,
22 2020, that requires a law enforcement agency to keep confidential in-
23 formation learned in the course of a criminal or national security inves-
24 tigation;

25 (4) authorizing the Director or an individual acting under the au-
26 thority of the Director to interfere with or to direct a military oper-
27 ation;

28 (5) authorizing the Director or an individual acting under the au-
29 thority of the Director to interfere with or to direct a diplomatic or
30 consular activity;

31 (6) authorizing the Director or an individual acting under the au-
32 thority of the Director to interfere with or to direct an intelligence ac-
33 tivity, resource, or operation; or

34 (7) authorizing the Director or an individual acting under the au-
35 thority of the Director to modify the classification of intelligence infor-
36 mation.

37 **§ 10886. Apprehension and prosecution of international**
38 **cyber criminals**

39 (a) DEFINITION OF INTERNATIONAL CYBER CRIMINAL.—In this section,
40 the term “international cyber criminal” means an individual—

1 (1) who is believed to have committed a cybercrime or intellectual
2 property crime against the interests of the United States or the citizens
3 of the United States; and

4 (2) for whom—

5 (A) an arrest warrant has been issued by a judge in the United
6 States; or

7 (B) an international wanted notice (commonly referred to as a
8 “Red Notice”) has been circulated by Interpol.

9 (b) CONSULTATIONS FOR NONCOOPERATION.—The Secretary of State
10 shall consult with the appropriate government official of each country from
11 which extradition is not likely due to the lack of an extradition treaty with
12 the United States or other reasons, in which 1 or more international cyber
13 criminals are physically present, to determine what actions the government
14 of the country has taken—

15 (1) to apprehend and prosecute the criminals; and

16 (2) to prevent the criminals from carrying out cybercrimes or intel-
17 lectual property crimes against the interests of the United States or its
18 citizens.

19 (c) ANNUAL REPORT.—

20 (1) DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEES.—
21 For purposes of this subsection, the term “appropriate congressional
22 committees” means—

23 (A) the Committee on Foreign Relations, the Committee on Ap-
24 propriations, the Committee on Homeland Security and Govern-
25 mental Affairs, the Committee on Banking, Housing, and Urban
26 Affairs, the Select Committee on Intelligence, and the Committee
27 on the Judiciary of the Senate; and

28 (B) the Committee on Foreign Affairs, the Committee on Ap-
29 propriations, the Committee on Homeland Security, the Com-
30 mittee on Financial Services, the Permanent Select Committee on
31 Intelligence, and the Committee on the Judiciary of the House of
32 Representatives.

33 (2) CONTENTS.—The Secretary of State shall submit to the appro-
34 priate congressional committees an annual report that includes—

35 (A) the number of international cyber criminals located in other
36 countries, disaggregated by country, and indicating from which
37 countries extradition is not likely due to the lack of an extradition
38 treaty with the United States or other reasons;

39 (B) the nature and number of significant discussions by an offi-
40 cial of the Department of State on ways to thwart or prosecute

1 international cyber criminals with an official of another country,
2 including the name of each country; and

3 (C) for each international cyber criminal who was extradited to
4 the United States during the most recently completed calendar
5 year—

- 6 (i) his or her name;
- 7 (ii) the crimes for which he or she was charged;
- 8 (iii) his or her previous country of residence; and
- 9 (iv) the country from which he or she was extradited to the
10 United States.

11 (3) FORM.—The report shall be in unclassified form to the maximum
12 extent possible, but may include a classified annex.

13 **§ 10887. President’s Cup Cybersecurity Competition**

14 (a) IN GENERAL.—The Director of the Cybersecurity and Infrastructure
15 Security Agency (in this section referred to as the “Director”) may hold an
16 annual cybersecurity competition to be known as the “Department of Home-
17 land Security Cybersecurity and Infrastructure Security Agency’s Presi-
18 dent’s Cup Cybersecurity Competition” (in this section referred to as the
19 “competition”) for the purpose of identifying challenging and comparatively
20 awarding prizes, including cash prizes, to the United States Government’s
21 best cybersecurity practitioners and teams across offensive and defensive cy-
22 bersecurity disciplines.

23 (b) ELIGIBILITY.—To be eligible to participate in the competition, an in-
24 dividual shall be a Federal Civilian employee or member of the uniformed
25 services (as the term is defined in section 2101 of title 5) and shall comply
26 with any rules promulgated by the Director regarding the competition.

27 (c) ADMINISTRATION.—The Director may enter into a grant, contract, co-
28 operative agreement, or other agreement with a private sector for-profit or
29 nonprofit entity or State or local government agency to administer the com-
30 petition.

31 (d) PARAMETERS.—Each competition shall incorporate the following ele-
32 ments:

33 (1) Cybersecurity skills outlined in the National Institute for Cyber-
34 security Education Framework or any successor framework.

35 (2) Individual and team events.

36 (3) Categories demonstrating offensive and defensive cyber oper-
37 ations, such as software reverse engineering and software exploitation,
38 network operations, forensics, big data analysis, cyber analysis, cyber
39 defense, cyber exploitation, secure programming, obfuscated coding, or
40 cyber-physical systems.

1 (4) Any other elements related to paragraph (1), (2), or (3) as deter-
2 mined necessary by the Director.

3 (e) USE OF FUNDS.—To further the goals and objectives of the competi-
4 tion, the Director may use amounts made available to the Director for the
5 competition for reasonable expenses for the following:

6 (1) Advertising, marketing, and promoting the competition.

7 (2) Meals for participants and organizers of the competition if at-
8 tendance the meal during the competition is necessary to maintain the
9 integrity of the competition.

10 (3) Promotional items, including merchandise and apparel.

11 (4) Consistent with section 4503 of title 5, necessary expenses for
12 the honorary recognition of competition participants, including mem-
13 bers of the uniformed services.

14 (5) Monetary and nonmonetary awards for competition participants,
15 including members of the uniformed services, subject to subsection (f).

16 (f) PRIZE LIMITATION.—

17 (1) AWARDS BY THE DIRECTOR.—The Director may make 1 or more
18 awards per competition, except that the amount or value of each shall
19 not exceed \$10,000.

20 (2) AWARDS BY THE SECRETARY.—The Secretary may make 1 or
21 more awards per competition, except that the amount or value of each
22 shall not exceed \$25,000.

23 (3) ADDITION TO REGULAR PAY.—A monetary award under this sec-
24 tion shall be in addition to the regular pay of the recipient.

25 (4) OVERALL YEARLY AWARD LIMIT.—The total amount or
26 value of awards made under this section during a fiscal year may
27 not exceed \$100,000.

28 (g) REPORTING REQUIREMENTS.—The Director shall annually provide to
29 the Committee on Homeland Security of the House of Representatives and
30 the Committee on Homeland Security and Governmental Affairs of the Sen-
31 ate a report that includes the following with respect to each competition
32 conducted in the preceding year:

33 (1) A description of available amounts.

34 (2) A description of authorized expenditures.

35 (3) Information relating to participation.

36 (4) Information relating to lessons learned and how those lessons
37 may be applied to improve cybersecurity operations and recruitment of
38 the Cybersecurity and Infrastructure Security Agency.

1 **§ 10888. Incentive pay for positions requiring significant**
 2 **cyber skills**

3 Subject to the availability of appropriations, and in accordance with the
 4 comparable level of the General Schedule, the Attorney General and the Sec-
 5 retary shall provide incentive pay, in an amount that is not more than 25
 6 percent of the basic pay of the individual, to an individual appointed to a
 7 position in the Department of Justice (including the Federal Bureau of In-
 8 vestigation) or the Department (including positions in Homeland Security
 9 Investigations), respectively, requiring significant cyber skills, including to
 10 aid in—

- 11 (1) the protection of trafficking victims;
 12 (2) the prevention of trafficking in individuals; or
 13 (3) the prosecution of technology-facilitated crimes against children
 14 by buyers or traffickers in individuals.

15 **Chapter 109—Science and Technology in**
 16 **Support of Homeland Security**

Subchapter I—General

Sec.

10901. Responsibilities and authorities of Under Secretary for Science and Technology.
 10902. Functions transferred.
 10903. Conduct of certain public health-related activities.
 10904. Federally funded research and development centers.
 10905. Miscellaneous provisions.
 10906. Homeland Security Advanced Research Projects Agency.
 10907. Conduct of research, development, demonstration, testing, and evaluation.
 10908. Utilization of Department of Energy national laboratories and sites in support of
 homeland security activities.
 10909. Transfers from and to the Department of Agriculture.
 10910. Homeland Security Science and Technology Advisory Committee.
 10911. Technology clearinghouse to encourage and support innovative solutions to enhance
 homeland security.
 10912. Enhancement of public safety communications interoperability.
 10913. Office for Interoperability and Compatibility.
 10914. Emergency communications interoperability research and development.
 10915. National Biosurveillance Integration Center.
 10916. Promoting anti-terrorism through international cooperation program.
 10917. Transparency in research and development.
 10918. EMP and GMD mitigation research and development and threat assessment, re-
 sponse, and recovery.
 10919. National Urban Security Technology Laboratory.
 10920. Chemical Security Analysis Center.

**Subchapter II—Supporting Anti-Terrorism by Protecting Effective Tech-
 nologies**

10931. Definitions.
 10932. Administration.
 10933. Litigation management.
 10934. Risk management.

Subchapter III—Biodefense

10941. National biodefense strategy and implementation plan.
 10942. Update of national biodefense implementation plan.
 10943. Biodefense analysis and budget submission.

Subchapter I—General

§ 10901. Responsibilities and authorities of Under Secretary for Science and Technology

The Secretary, acting through the Under Secretary for Science and Technology, is responsible for—

(1) advising the Secretary regarding research and development efforts and priorities in support of the Department’s missions;

(2) developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for identifying priorities, goals, objectives, and policies for, and coordinating the Federal Government’s civilian efforts to identify and develop, countermeasures to chemical, biological, and other emerging terrorist threats, including the development of—

(A) comprehensive, research-based definable goals for the efforts; and

(B) annual measurable objectives and specific targets to accomplish and evaluate the goals for the efforts;

(3) supporting the Under Secretary for Intelligence and Analysis and the Director of the Cybersecurity and Infrastructure Security Agency, by assessing and testing homeland security vulnerabilities and possible threats;

(4) conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, except that the responsibility does not extend to human health-related research and development activities;

(5) establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of, technology and systems for—

(A) preventing the importation of chemical, biological, and related weapons and material; and

(B) detecting, preventing, protecting against, and responding to terrorist attacks;

(6) establishing a system for transferring homeland security developments or technologies to Federal, State, local government, and private-sector entities;

(7) entering into work agreements, joint sponsorships, contracts, or other agreements with the Department of Energy regarding the use of the national laboratories or sites, and the support of the science and technology base at those facilities;

1 (8) collaborating with the Secretary of Agriculture and the Attorney
2 General as provided in section 212 of the Agricultural Bioterrorism
3 Protection Act of 2002 (7 U.S.C. 8401);

4 (9) collaborating with the Secretary of Health and Human Services
5 and the Attorney General in determining any new biological agents and
6 toxins that shall be listed as “select agents” in Appendix A of part 72
7 of title 42, Code of Federal Regulations, pursuant to section 351A of
8 the Public Health Service Act (42 U.S.C. 262a);

9 (10) supporting United States leadership in science and technology;

10 (11) establishing and administering the primary research and devel-
11 opment activities of the Department, including the long-term research
12 and development needs and capabilities for all elements of the Depart-
13 ment;

14 (12) coordinating and integrating all research, development, dem-
15 onstration, testing, and evaluation activities of the Department;

16 (13) coordinating with other appropriate executive agencies in devel-
17 oping and carrying out the science and technology agenda of the De-
18 partment to reduce duplication and identify unmet needs; and

19 (14) developing and overseeing the administration of guidelines for
20 merit review of research and development projects throughout the De-
21 partment, and for the dissemination of research conducted or sponsored
22 by the Department.

23 **§ 10902. Functions transferred**

24 The Secretary succeeds to the functions, personnel, assets, and liabilities
25 of the following entities:

26 (1) The following programs and activities of the Department of En-
27 ergy, including the functions of the Secretary of Energy relating there-
28 to (but not including programs and activities relating to the strategic
29 nuclear defense posture of the United States):

30 (A) The chemical and biological national security and sup-
31 porting programs and activities of the nonproliferation and
32 verification research and development program.

33 (B) The nuclear smuggling programs and activities within the
34 proliferation detection program of the nonproliferation and
35 verification research and development program. The programs and
36 activities described in this subparagraph may be designated by the
37 President either for transfer to the Department or for joint oper-
38 ation by the Secretary and the Secretary of Energy.

39 (C) The nuclear assessment program and activities of the as-
40 sessment, detection, and cooperation program of the international
41 materials protection and cooperation program.

1 (D) Life sciences activities of the biological and environmental
2 research program related to microbial pathogens designated by the
3 President for transfer to the Department.

4 (E) The Environmental Measurements Laboratory.

5 (F) The advanced scientific computing research program and
6 activities at Lawrence Livermore National Laboratory.

7 (2) The National Bio-Weapons Defense Analysis Center of the De-
8 partment of Defense, including the functions of the Secretary of De-
9 fense related thereto.

10 **§ 10903. Conduct of certain public health-related activities**

11 (a) IN GENERAL.—With respect to civilian human health-related research
12 and development activities relating to countermeasures for chemical, biologi-
13 cal, radiological, and nuclear and other emerging terrorist threats carried
14 out by the Department of Health and Human Services (including the Public
15 Health Service), the Secretary of Health and Human Services shall set pri-
16 orities, goals, objectives, and policies and develop a coordinated strategy for
17 the activities in collaboration with the Secretary of Homeland Security to
18 ensure consistency with the national policy and strategic plan developed
19 under section 10901 of this title.

20 (b) EVALUATION OF PROGRESS.—In carrying out subsection (a), the Sec-
21 retary of Health and Human Services shall collaborate with the Secretary
22 in developing specific benchmarks and outcome measurements for evaluating
23 progress toward achieving the priorities and goals described in that sub-
24 section.

25 **§ 10904. Federally funded research and development centers**

26 The Secretary, acting through the Under Secretary for Science and Tech-
27 nology, shall have the authority to establish or contract with one or more
28 federally funded research and development centers to provide independent
29 analysis of homeland security issues, or to carry out other responsibilities
30 under this subtitle, including coordinating and integrating both the extra-
31 mural and intramural programs described in section 10907 of this title.

32 **§ 10905. Miscellaneous provisions**

33 (a) CLASSIFICATION.—To the greatest extent practicable, research con-
34 ducted or supported by the Department shall be unclassified.

35 (b) CONSTRUCTION.—Nothing in this chapter shall be construed to pre-
36 clude any Under Secretary of the Department from carrying out research,
37 development, demonstration, or deployment activities, as long as the activi-
38 ties are coordinated through the Under Secretary for Science and Tech-
39 nology.

40 (c) REGULATIONS.—The Secretary, acting through the Under Secretary
41 for Science and Technology, may issue necessary regulations with respect

1 to research, development, demonstration, testing, and evaluation activities of
2 the Department, including the conducting, funding, and reviewing of the ac-
3 tivities.

4 **§ 10906. Homeland Security Advanced Research Projects**
5 **Agency**

6 (a) DEFINITIONS.—In this section:

7 (1) FUND.—The term “Fund” means the Acceleration Fund for Re-
8 search and Development of Homeland Security Technologies estab-
9 lished in subsection (c).

10 (2) HOMELAND SECURITY RESEARCH.—The term “homeland secu-
11 rity research” means research relevant to the detection of, prevention
12 of, protection against, response to, attribution of, and recovery from
13 homeland security threats, particularly acts of terrorism.

14 (3) HSARPA.—The term “HSARPA” means the Homeland Secu-
15 rity Advanced Research Projects Agency established in subsection (b).

16 (4) UNDER SECRETARY.—The term “Under Secretary” means the
17 Under Secretary for Science and Technology.

18 (b) HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY.—

19 (1) ESTABLISHMENT.—There is in the Department the Homeland
20 Security Advanced Research Projects Agency (HSARPA).

21 (2) DIRECTOR.—The Director is the head of HSARPA. The Director
22 is appointed by the Secretary. The Director reports to the Under Sec-
23 retary.

24 (3) RESPONSIBILITIES.—The Director shall administer the Fund to
25 award competitive, merit-reviewed grants, cooperative agreements, or
26 contracts to public or private entities, including businesses, federally
27 funded research and development centers, and universities. The Direc-
28 tor shall administer the Fund to—

29 (A) support basic and applied homeland security research to
30 promote revolutionary changes in technologies that would promote
31 homeland security;

32 (B) advance the development, testing and evaluation, and de-
33 ployment of critical homeland security technologies;

34 (C) accelerate the prototyping and deployment of technologies
35 that would address homeland security vulnerabilities; and

36 (D) conduct research and development for the purpose of ad-
37 vancing technology for the investigation of child exploitation
38 crimes, including child victim identification, trafficking in individ-
39 uals, and child pornography, and for advanced forensics.

40 (4) TARGETED COMPETITIONS.—The Director may solicit proposals
41 to address specific vulnerabilities identified by the Director.

1 (5) COORDINATION.—The Director shall ensure that the activities of
2 HSARPA are coordinated with those of other relevant research agen-
3 cies, and may run projects jointly with other agencies.

4 (6) PERSONNEL.—In hiring personnel for HSARPA, the Secretary
5 has the hiring and management authorities described in section 1101
6 of the Strom Thurmond National Defense Authorization Act for Fiscal
7 Year 1999 (Public Law 105–261, 5 U.S.C. 3104 note). The term of
8 appointments for employees under subsection (c)(1) of that section may
9 not exceed 5 years before the granting of an extension under subsection
10 (c)(2) of that section.

11 (7) DEMONSTRATIONS.—The Director shall periodically hold home-
12 land security technology demonstrations to improve contact among
13 technology developers, vendors and acquisition personnel.

14 (c) ACCELERATION FUND.—There is in the Department the Acceleration
15 Fund for Research and Development of Homeland Security Technologies (in
16 this subsection referred to as the “Acceleration Fund”). The Director ad-
17 ministers the Acceleration Fund.

18 **§ 10907. Conduct of research, development, demonstration,**
19 **testing, and evaluation**

20 (a) IN GENERAL.—The Secretary, acting through the Under Secretary
21 for Science and Technology, shall carry out the responsibilities under section
22 10901(4) of this title through both extramural and intramural programs.

23 (b) EXTRAMURAL PROGRAMS.—

24 (1) IN GENERAL.—The Secretary, acting through the Under Sec-
25 retary for Science and Technology, shall operate extramural research,
26 development, demonstration, testing, and evaluation programs so as
27 to—

28 (A) ensure that colleges, universities, private research institutes,
29 and companies (and consortia thereof) from as many areas of the
30 United States as practicable participate;

31 (B) ensure that the research funded is of high quality, as deter-
32 mined through merit review processes developed under section
33 10901(14) of this title; and

34 (C) distribute funds through grants, cooperative agreements,
35 and contracts.

36 (2) UNIVERSITY-BASED CENTERS FOR HOMELAND SECURITY.—

37 (A) DESIGNATION.—The Secretary, acting through the Under
38 Secretary for Science and Technology, shall designate a university-
39 based center or several university-based centers for homeland secu-
40 rity. The purpose of the center or these centers shall be to estab-

1 lish a coordinated, university-based system to enhance the Na-
2 tion's homeland security.

3 (B) CRITERIA FOR DESIGNATION.—Criteria for the designation
4 of colleges or universities as a center or as centers for homeland
5 security shall include demonstrated expertise in—

- 6 (i) the training of first responders;
- 7 (ii) the response to incidents involving weapons of mass de-
8 struction and biological warfare;
- 9 (iii) emergency and diagnostic medical services;
- 10 (iv) chemical, biological, radiological, and nuclear counter-
11 measures or detection;
- 12 (v) animal and plant health and diagnostics;
- 13 (vi) food safety;
- 14 (vii) water and wastewater operations;
- 15 (viii) port and waterway security;
- 16 (ix) multi-modal transportation;
- 17 (x) information security and information engineering;
- 18 (xi) engineering;
- 19 (xii) educational outreach and technical assistance;
- 20 (xiii) border transportation and security; and
- 21 (xiv) the public policy implications and public dissemination
22 of homeland security related research and development;

23 (C) DISCRETION OF SECRETARY.—To the extent that exercising
24 discretion is in the interest of homeland security, and with respect
25 to the designation of any given university-based center for home-
26 land security, the Secretary may except certain criteria as speci-
27 fied in subparagraph (B) and consider additional criteria beyond
28 those specified in subparagraph (B). On designation of a univer-
29 sity-based center for homeland security, the Secretary shall that
30 day publish in the Federal Register the criteria that were excepted
31 or added in the selection process and the justification for the set
32 of criteria that were used for that designation.

33 (D) REPORT TO CONGRESS.—The Secretary shall report annu-
34 ally to Congress concerning the implementation of this section.
35 The report shall indicate which center or centers have been des-
36 ignated and how the designation or designations enhance home-
37 land security, as well as list any decisions to revoke or modify the
38 designations.

39 (e) INTRAMURAL PROGRAMS.—

40 (1) CONSULTATION.—In carrying out the duties under section 10901
41 of this title, the Secretary, acting through the Under Secretary for

1 Science and Technology, may draw upon the expertise of any labora-
2 tory of the Federal Government, whether operated by a contractor or
3 the Government.

4 (2) LABORATORIES.—The Secretary, acting through the Under Sec-
5 retary for Science and Technology, may establish a headquarters lab-
6 oratory for the Department at any laboratory or site and may establish
7 additional laboratory units at other laboratories or sites.

8 (3) CRITERIA FOR HEADQUARTERS LABORATORY.—If the Secretary
9 chooses to establish a headquarters laboratory under paragraph (2), the
10 Secretary shall do the following:

11 (A) Establish criteria for the selection of the headquarters lab-
12 oratory in consultation with the National Academy of Sciences, ap-
13 propriate Federal agencies, and other experts.

14 (B) Publish the criteria in the Federal Register.

15 (C) Evaluate all appropriate laboratories or sites against the
16 criteria.

17 (D) Select a laboratory or site on the basis of the criteria.

18 (E) Report to the appropriate congressional committees on
19 which laboratory was selected, how the selected laboratory meets
20 the published criteria, and what duties the headquarters labora-
21 tory shall perform.

22 (4) LIMITATION ON OPERATION OF LABORATORIES.—A laboratory
23 may not begin operating as the headquarters laboratory of the Depart-
24 ment until at least 30 days after the transmittal of the report required
25 by paragraph (3)(E).

26 (d) PREFERENCE FOR UNITED STATES INDUSTRY.—

27 (1) DEFINITIONS.—In this subsection

28 (A) COUNTRY OF CONCERN.—The term “country of concern”
29 means a country that—

30 (i) is a covered nation, as the term is defined in section
31 4872(d) of title 10; or

32 (ii) the Secretary determines is engaged in conduct that is
33 detrimental to the national security of the United States.

34 (B) DOMESTIC END PRODUCT.—The term “domestic end prod-
35 uct” has the meaning given the term in section 25.003 of title 48,
36 Code of Federal Regulations, or any successor regulation.

37 (C) MANUFACTURED SUBSTANTIALLY IN THE UNITED
38 STATES.—The term “manufactured substantially in the United
39 States” means an item is a domestic end product.

40 (D) NONPROFIT ORGANIZATION; SMALL BUSINESS FIRM; SUB-
41 JECT INVENTION.—The terms “nonprofit organization”, “small

1 business firm, and “subject invention” have the meanings given
2 those terms in section 201 of title 35.

3 (2) WAIVERS.—

4 (A) IN GENERAL.—Subject to subparagraph (B), in individual
5 cases, the Secretary may waive the requirements of section 204 of
6 title 35 on a showing by the small business firm, nonprofit organi-
7 zation, or assignee that reasonable but unsuccessful efforts have
8 been made to grant licenses on similar terms to potential licensees
9 that would be likely to manufacture substantially in the United
10 States or that under the circumstances domestic manufacture is
11 not commercially feasible.

12 (B) CONDITIONS.—

13 (i) BEFORE GRANT OF WAIVER.—Before granting a waiver
14 under subparagraph (A), the Secretary shall comply with the
15 procedures developed and implemented by the Department
16 pursuant to section 70923(b)(2) of the Build America, Buy
17 America Act (Public Law 117–58, div. G, title IX, subtitle A,
18 135 Stat. 1306).

19 (ii) PROHIBITION ON GRANTING CERTAIN WAIVERS.—The
20 Secretary may not grant a waiver under subparagraph (A) if,
21 as a result of the waiver, products embodying the applicable
22 subject invention, or produced through the use of the applica-
23 ble subject invention, would be manufactured substantially in
24 a country of concern.

25 **§ 10908. Utilization of Department of Energy national lab-**
26 **oratories and sites in support of homeland secu-**
27 **urity activities**

28 (a) AUTHORITY TO UTILIZE NATIONAL LABORATORIES AND SITES.—

29 (1) IN GENERAL.—In carrying out the missions of the Department,
30 the Secretary may utilize the Department of Energy national labora-
31 tories and sites through one or more of the following methods, as the
32 Secretary considers appropriate:

33 (A) A joint sponsorship arrangement referred to in subsection
34 (b).

35 (B) A direct contract between the Department and the applica-
36 ble Department of Energy laboratory or site, subject to subsection
37 (c).

38 (C) A “work for others” basis made available by that laboratory
39 or site.

40 (D) Any other method provided by law.

1 (2) ACCEPTANCE AND PERFORMANCE BY LABS AND SITES.—Not-
2 withstanding another law governing the administration, mission, use, or
3 operations of Department of Energy national laboratories and sites, the
4 laboratories and sites may accept and perform work for the Secretary,
5 consistent with resources provided, and perform work on an equal basis
6 to other missions at the laboratory and not on a noninterference basis
7 with other missions of the laboratory or site.

8 (b) JOINT SPONSORSHIP ARRANGEMENTS.—

9 (1) LABORATORIES.—The Department may be a joint sponsor, under
10 a multiple agency sponsorship arrangement with the Department of
11 Energy, of one or more Department of Energy national laboratories in
12 the performance of work.

13 (2) SITES.—The Department may be a joint sponsor of a Depart-
14 ment of Energy site in the performance of work as if the site were a
15 federally funded research and development center and the work were
16 performed under a multiple agency sponsorship arrangement with the
17 Department.

18 (3) PRIMARY SPONSOR.—The Department of Energy shall be the pri-
19 mary sponsor under a multiple agency sponsorship arrangement re-
20 ferred to in paragraph (1) or (2).

21 (4) LEAD AGENT.—The Secretary of Energy shall act as the lead
22 agent in coordinating the formation and performance of a joint spon-
23 sorship arrangement under this subsection between the Department
24 and a Department of Energy national laboratory or site.

25 (5) COMPLIANCE WITH FEDERAL ACQUISITION REGULATION.—Work
26 performed by a Department of Energy national laboratory or site under
27 a joint sponsorship arrangement under this subsection shall comply
28 with the policy on the use of federally funded research and development
29 centers under the Federal Acquisition Regulation.

30 (6) FUNDING.—The Department shall provide funds for work at the
31 Department of Energy national laboratories or sites, as the case may
32 be, under a joint sponsorship arrangement under this subsection under
33 the same terms and conditions as apply to the primary sponsor of a
34 national laboratory under section 3303(a)(1)(C) of title 41 or of a site
35 to the extent that section applies to the site as a federally funded re-
36 search and development center by reason of this subsection.

37 (c) SEPARATE CONTRACTING.—To the extent that programs or activities
38 transferred by the Homeland Security Act of 2002 (Public Law 107–296,
39 116 Stat. 2135) from the Department of Energy to the Department are
40 being carried out through direct contracts with the operator of a national
41 laboratory or site of the Department of Energy, the Secretary and the Sec-

1 retary of Energy shall ensure that direct contracts for the programs and
2 activities between the Department and the operator are separate from the
3 direct contracts of the Department of Energy with the operator.

4 (d) AUTHORITY WITH RESPECT TO COOPERATIVE RESEARCH AND DE-
5 VELOPMENT AGREEMENTS AND LICENSING AGREEMENTS.—In connection
6 with utilization of Department of Energy national laboratories and sites
7 under this section, the Secretary may permit the director of a national lab-
8 oratory or site to enter into cooperative research and development agree-
9 ments or to negotiate licensing agreements with any person, any agency or
10 instrumentality of the United States, any unit of State or local government,
11 and any other entity under the authority granted by section 12 of the Ste-
12 venson-Wylder Technology Innovation Act of 1980 (15 U.S.C. 3710a).
13 Technology may be transferred to a non-Federal party to an agreement con-
14 sistent with sections 11 and 12 of that Act (15 U.S.C. 3710, 3710a).

15 (e) REIMBURSEMENT OF COSTS.—In the case of an activity carried out
16 by the operator of a Department of Energy national laboratory or site in
17 connection with the utilization of the laboratory or site under this section,
18 the Department shall reimburse the Department of Energy for costs of the
19 activity through a method under which the Secretary of Energy waives any
20 requirement for the Department to pay administrative charges or personnel
21 costs of the Department of Energy or its contractors in excess of the
22 amount that the Secretary of Energy pays for an activity carried out by the
23 contractor and paid for by the Department of Energy.

24 (f) LABORATORY-DIRECTED RESEARCH AND DEVELOPMENT BY THE DE-
25 PARTMENT OF ENERGY.—No funds authorized to be appropriated or other-
26 wise made available to the Department in a fiscal year may be obligated
27 or expended for laboratory directed research and development activities car-
28 ried out by the Department of Energy unless the activities support the mis-
29 sions of the Department.

30 (g) OFFICE FOR NATIONAL LABORATORIES.—There is in the Directorate
31 of Science and Technology the Office for National Laboratories. The Office
32 is responsible for the coordination and utilization of the Department of En-
33 ergy national laboratories and sites under this section in a manner to create
34 a networked laboratory system for the purpose of supporting the missions
35 of the Department.

36 (h) DEPARTMENT OF ENERGY COORDINATION ON HOMELAND SECURITY-
37 RELATED RESEARCH.—The Secretary of Energy shall ensure that research,
38 development, test, and evaluation activities conducted in the Department of
39 Energy that are directly or indirectly related to homeland security are fully
40 coordinated with the Secretary to minimize duplication of effort and maxi-
41 mize the effective application of Federal budget resources.

1 **§ 10909. Transfers from and to the Department of Agri-**
2 **culture**

3 (a) PLUM ISLAND ANIMAL DISEASE CENTER.—

4 (1) IN GENERAL.—The Secretary succeeds the Secretary of Agri-
5 culture as head of the Plum Island Animal Disease Center of the De-
6 partment of Agriculture (in this section referred to as the “Center”),
7 including the assets and liabilities of the Center.

8 (2) CONTINUED DEPARTMENT OF AGRICULTURE ACCESS.—The Sec-
9 retary and the Secretary of Agriculture shall enter into an agreement
10 to ensure that the Department of Agriculture is able to carry out re-
11 search, diagnostic, and other activities of the Department of Agri-
12 culture at the Center.

13 (3) DIRECTION OF ACTIVITIES.—The Secretary of Agriculture shall
14 continue to direct the research, diagnostic, and other activities of the
15 Department of Agriculture at the Center.

16 (4) NOTIFICATION.—At least 180 days before a change in the bio-
17 safety level at the Center, the President shall notify Congress of the
18 change and describe the reasons for the change.

19 (5) DISPOSITION OF PLUM ISLAND PROPERTY AND TRANSPOR-
20 TATION ASSETS.—The Administrator of General Services shall ensure
21 that—

22 (A) Federal property known as Plum Island, New York, includ-
23 ing the Orient Point facility, all real and personal property, and
24 transportation assets that support Plum Island operations and ac-
25 cess to Plum Island, be disposed of as a single consolidated asset;
26 and

27 (B) the disposal is subject to conditions as may be necessary to
28 protect Government interests and meet program requirements.

29 (b) NATIONAL BIO AND AGRO-DEFENSE FACILITY.—The Secretary shall
30 transfer to the Secretary of Agriculture the operation of and all property
31 required to operate the National Bio- and Agro-Defense Facility in Manhat-
32 tan, Kansas. The transfer of function shall include the transfer of up to 40
33 full time equivalent positions, to be completed within 120 days of the effec-
34 tive date of the transfer of function, as jointly determined by the Secre-
35 taries.

36 **§ 10910. Homeland Security Science and Technology Advi-**
37 **sory Committee**

38 (a) ESTABLISHMENT.—There is in the Department a Homeland Security
39 Science and Technology Advisory Committee (in this section referred to as
40 the “Advisory Committee”). The Advisory Committee shall make rec-
41 ommendations with respect to the activities of the Under Secretary for

1 Science and Technology, including identifying research areas of potential
2 importance to the security of the Nation.

3 (b) MEMBERSHIP.—

4 (1) APPOINTMENT.—The Advisory Committee consists of 20 mem-
5 bers appointed by the Under Secretary for Science and Technology, in-
6 cluding emergency first-responders or representatives of organizations
7 or associations of emergency first-responders. The Advisory Committee
8 also shall include representatives of citizen groups, including economi-
9 cally disadvantaged communities. The individuals appointed as mem-
10 bers of the Advisory Committee—

11 (A) shall be eminent in fields such as emergency response, re-
12 search, engineering, new product development, business, and man-
13 agement consulting;

14 (B) shall be selected solely on the basis of established records
15 of distinguished service;

16 (C) shall not be employees of the Federal Government; and

17 (D) shall be selected to provide representation of a cross-section
18 of the research, development, demonstration, and deployment ac-
19 tivities supported by the Under Secretary for Science and Tech-
20 nology.

21 (2) NATIONAL RESEARCH COUNCIL.—The Under Secretary for
22 Science and Technology may enter into an arrangement for the Na-
23 tional Research Council to select members of the Advisory Committee,
24 but only if the panel used by the National Research Council reflects
25 the representation described in paragraph (1).

26 (c) TERMS OF OFFICE.—

27 (1) IN GENERAL.—Except as otherwise provided in this subsection,
28 the term of office of each member of the Advisory Committee shall be
29 3 years.

30 (2) VACANCIES.—A member appointed to fill a vacancy occurring be-
31 fore the expiration of the term for which the member's predecessor was
32 appointed shall be appointed for the remainder of the term.

33 (d) ELIGIBILITY.—A person who has completed 2 consecutive full terms
34 of service on the Advisory Committee is ineligible for appointment during
35 the 1-year period following the expiration of the 2d term.

36 (e) MEETINGS.—The Advisory Committee shall meet at least quarterly at
37 the call of the Chair or whenever one-third of the members request a meet-
38 ing in writing. Each member shall be given appropriate notice of the call
39 of each meeting, whenever possible not less than 15 days before the meet-
40 ing.

1 (f) QUORUM.—A majority of the members of the Advisory Committee not
2 having a conflict of interest in the matter being considered by the Advisory
3 Committee constitutes a quorum.

4 (g) CONFLICT OF INTEREST RULES.—The Advisory Committee shall es-
5 tablish rules for determining when 1 of its members has a conflict of inter-
6 est in a matter being considered by the Advisory Committee.

7 (h) REPORTS.—

8 (1) ANNUAL REPORT.—The Advisory Committee shall submit an an-
9 nual report to the Under Secretary for Science and Technology for
10 transmittal to Congress on or before January 31 each year. The report
11 shall describe the activities and recommendations of the Advisory Com-
12 mittee during the previous year.

13 (2) ADDITIONAL REPORTS.—The Advisory Committee may submit to
14 the Under Secretary for transmittal to Congress additional reports on
15 specific policy matters it considers appropriate.

16 (i) EXEMPTION FROM SECTION 1013 OF TITLE 5.—Section 1013 of title
17 5 shall not apply to the Advisory Committee.

18 **§ 10911. Technology clearinghouse to encourage and sup-**
19 **port innovative solutions to enhance homeland se-**
20 **curity**

21 (a) ESTABLISHMENT OF PROGRAM.—The Secretary, acting through the
22 Under Secretary for Science and Technology, shall establish and promote
23 a program to encourage technological innovation in facilitating the mission
24 of the Department (as described in section 10301 of this title).

25 (b) ELEMENTS OF PROGRAM.—The program described in subsection (a)
26 shall include the following components:

27 (1) The establishment of a centralized Federal clearinghouse for in-
28 formation relating to technologies that would further the mission of the
29 Department for dissemination, as appropriate, to Federal, State, and
30 local government and private-sector entities for additional review, pur-
31 chase, or use.

32 (2) The issuance of announcements seeking unique and innovative
33 technologies to advance the mission of the Department.

34 (3) The establishment of a technical assistance team to assist in
35 screening, as appropriate, proposals submitted to the Secretary (except
36 as provided in subsection (c)(2)) to assess the feasibility, scientific and
37 technical merits, and estimated cost of the proposals, as appropriate.

38 (4) The provision of guidance, recommendations, and technical as-
39 sistance, as appropriate, to assist Federal, State, and local government
40 and private-sector efforts to evaluate and implement the use of tech-
41 nologies described in paragraphs (1) and (2).

1 (5) The provision of information for persons seeking guidance on
2 how to pursue proposals to develop or deploy technologies that would
3 enhance homeland security, including information relating to Federal
4 funding, regulation, or acquisition.

5 (c) MISCELLANEOUS PROVISIONS.—

6 (1) IN GENERAL.—Nothing in this section shall be construed as au-
7 thORIZING the Secretary or the technical assistance team established
8 under subsection (b)(3) to set standards for technology to be used by
9 the Department, another executive agency, a State or local government
10 entity, or a private-sector entity.

11 (2) CERTAIN PROPOSALS.—The technical assistance team established
12 under subsection (b)(3) shall not consider or evaluate proposals sub-
13 mitted in response to a solicitation for offers for a pending procure-
14 ment or for a specific agency requirement.

15 (3) COORDINATION.—In carrying out this section, the Secretary shall
16 coordinate with the Technical Support Working Group (organized
17 under the April 1982 National Security Decision Directive Numbered
18 30).

19 **§ 10912. Enhancement of public safety communications**
20 **interoperability**

21 (a) DEFINITION OF INTEROPERABLE COMMUNICATIONS.—In this section,
22 the term “interoperable communications” means the ability of emergency
23 response providers and relevant Federal, State, and local government agen-
24 cies to communicate with each other as necessary, through a dedicated pub-
25 lic safety network utilizing information technology systems and radio com-
26 munications systems, and to exchange voice, data, and video with one an-
27 other on demand, in real time, as necessary.

28 (b) COORDINATION OF PUBLIC SAFETY INTEROPERABLE COMMUNICA-
29 TIONS PROGRAMS.—

30 (1) PROGRAM.—The Secretary, in consultation with the Secretary of
31 Commerce and the Chairman of the Federal Communications Commis-
32 sion, shall establish a program to enhance public safety interoperable
33 communications at all levels of government. The program shall—

34 (A) establish a comprehensive national approach to achieving
35 public safety interoperable communications;

36 (B) coordinate with other Federal agencies in carrying out sub-
37 paragraph (A);

38 (C) develop, in consultation with other appropriate Federal
39 agencies and State and local authorities, appropriate minimum ca-
40 pabilities for communications interoperability for Federal, State,
41 and local public safety agencies;

1 (D) accelerate, in consultation with other Federal agencies, in-
2 cluding the National Institute of Standards and Technology, the
3 private sector, and nationally recognized standards organizations
4 as appropriate, the development of national voluntary consensus
5 standards for public safety interoperable communications, recog-
6 nizing—

7 (i) the value, life cycle, and technical capabilities of existing
8 communications infrastructure;

9 (ii) the need for cross-border interoperability between
10 States and nations;

11 (iii) the unique needs of small, rural communities; and

12 (iv) the interoperability needs for daily operations and cata-
13 strophic events;

14 (E) encourage the development and implementation of flexible
15 and open architectures incorporating, where possible, technologies
16 that currently are commercially available, with appropriate levels
17 of security, for short-term and long-term solutions to public safety
18 communications interoperability;

19 (F) assist other Federal agencies in identifying priorities for re-
20 search, development, testing, and evaluation with regard to public
21 safety interoperable communications;

22 (G) identify priorities in the Department for research, develop-
23 ment, and testing and evaluation with regard to public safety
24 interoperable communications;

25 (H) establish coordinated guidance for Federal grant programs
26 for public safety interoperable communications;

27 (I) provide technical assistance to State and local public safety
28 agencies regarding planning, acquisition strategies, interoperability
29 architectures, training, and other functions necessary to achieve
30 public safety communications interoperability;

31 (J) develop and disseminate best practices to improve public
32 safety communications interoperability; and

33 (K) develop appropriate performance measures and milestones
34 to systematically measure the Nation's progress toward achieving
35 public safety communications interoperability, including the devel-
36 opment of national voluntary consensus standards.

37 (2) OFFICE FOR INTEROPERABILITY AND COMPATIBILITY.—

38 (A) ESTABLISHMENT.—The Secretary may establish an Office
39 for Interoperability and Compatibility in the Directorate of Science
40 and Technology to carry out this subsection.

1 (B) FUNCTIONS.—If the Secretary establishes an office, the
2 Secretary shall, through the office, carry out Department respon-
3 sibilities and authorities relating to the SAFECOM Program.

4 (c) INTERNATIONAL INTEROPERABILITY.—The President shall establish a
5 mechanism for coordinating cross-border interoperability issues between—

6 (1) the United States and Canada; and

7 (2) the United States and Mexico.

8 (d) MULTIYEAR INTEROPERABILITY GRANTS.—

9 (1) MULTIYEAR COMMITMENTS.—In awarding grants to a State, re-
10 gion, local government, or Indian tribe for the purposes of enhancing
11 interoperable communications capabilities for emergency response pro-
12 viders, the Secretary may commit to obligate Federal assistance beyond
13 the current fiscal year, subject to the limitations and restrictions in this
14 subsection.

15 (2) RESTRICTIONS.—

16 (A) TIME LIMIT.—No multiyear interoperability commitment
17 may exceed 3 years in duration.

18 (B) AMOUNT OF COMMITTED FUNDS.—The total amount of as-
19 sistance the Secretary has committed to obligate for a future fiscal
20 year under paragraph (1) may not exceed \$150,000,000.

21 (3) LETTERS OF INTENT.—

22 (A) ISSUANCE.—Under paragraph (1), the Secretary may issue
23 a letter of intent to an applicant committing to obligate from fu-
24 ture budget authority an amount, not more than the Federal Gov-
25 ernment's share of the project's cost, for an interoperability com-
26 munications project (including interest costs and costs of formu-
27 lating the project).

28 (B) SCHEDULE.—A letter of intent under this paragraph shall
29 establish a schedule under which the Secretary will reimburse the
30 applicant for the Federal Government's share of the project's
31 costs, as amounts become available, if the applicant, after the Sec-
32 retary issues the letter, carries out the project before receiving
33 amounts under a grant issued by the Secretary.

34 (C) NOTICE TO SECRETARY.—An applicant that is issued a let-
35 ter of intent under this subsection shall notify the Secretary of the
36 applicant's intent to carry out a project pursuant to the letter be-
37 fore the project begins.

38 (D) NOTICE TO CONGRESS.—The Secretary shall transmit a
39 written notification to Congress no later than 3 days before the
40 issuance of a letter of intent under this section.

1 (E) LIMITATIONS.—A letter of intent issued under this section
2 is not an obligation of the Government under section 1501 of title
3 31, and is not deemed to be an administrative commitment for fi-
4 nancing. An obligation or administrative commitment may be
5 made only as amounts are provided in authorization and appro-
6 priations laws.

7 (F) STATUTORY CONSTRUCTION.—Nothing in this subsection
8 shall be construed—

9 (i) to prohibit the obligation of amounts pursuant to a let-
10 ter of intent under this subsection in the same fiscal year as
11 the letter of intent is issued; or

12 (ii) to apply to, or replace, Federal assistance intended for
13 interoperable communications that is not provided pursuant
14 to a commitment under this subsection.

15 (e) INTEROPERABLE COMMUNICATIONS PLANS.—An applicant requesting
16 funding assistance from the Secretary for interoperable communications for
17 emergency response providers shall submit an Interoperable Communica-
18 tions Plan to the Secretary for approval. A plan shall—

19 (1) describe the current state of communications interoperability in
20 the applicable jurisdictions among Federal, State, and local emergency
21 response providers and other relevant private resources;

22 (2) describe the available and planned use of the public safety fre-
23 quency spectrum and of resources for interoperable communications
24 within the jurisdictions;

25 (3) describe how the planned use of the spectrum and the resources
26 for interoperable communications is compatible with surrounding capa-
27 bilities and interoperable communications plans of Federal, State, and
28 local governmental entities, military installations, foreign governments,
29 critical infrastructure, and other relevant entities;

30 (4) include a 5-year plan for the dedication of Federal, State, and
31 local government and private resources to achieve a consistent, secure,
32 and effective interoperable communications system, including planning,
33 system design and engineering, testing and technology development,
34 procurement and installation, training, and operations and mainte-
35 nance;

36 (5) describe how the 5-year plan meets or exceeds applicable stand-
37 ards and grant requirements established by the Secretary;

38 (6) include information on the governance structure used to develop
39 the plan, including this information about all agencies and organiza-
40 tions that participated in developing the plan and the scope and time
41 frame of the plan; and

1 (7) describe the method by which multijurisdictional, multidisci-
2 plinary input is provided from all regions of the jurisdiction, including
3 high-threat urban areas located in the jurisdiction, and the process for
4 continuing to incorporate input.

5 (f) EXPANDED REPORTING REQUIREMENT.—In addition to the commit-
6 tees specifically enumerated to receive reports under title XII of the Imple-
7 menting Recommendations of the 9/11 Commission Act of 2007 (Public
8 Law 110–53, 121 Stat. 381), any report transmitted under title XII shall
9 be transmitted to the appropriate congressional committees.

10 **§ 10913. Office for Interoperability and Compatibility**

11 (a) CLARIFICATION OF RESPONSIBILITIES.—The Director of the Office
12 for Interoperability and Compatibility shall—

13 (1) assist the Secretary in developing and implementing the science
14 and technology aspects of the program described in subparagraphs (D),
15 (E), (F), and (G) of section 10912(b)(1) of this title;

16 (2) in coordination with the Federal Communications Commission,
17 the National Institute of Standards and Technology, and other Federal
18 departments and agencies with responsibility for standards, support the
19 creation of national voluntary consensus standards for interoperable
20 emergency communications;

21 (3) establish a comprehensive research, development, testing, and
22 evaluation program for improving interoperable emergency communica-
23 tions;

24 (4) establish, in coordination with the Director for Emergency Com-
25 munications, requirements for interoperable emergency communications
26 capabilities, which shall be nonproprietary where standards for the ca-
27 pabilities exist, for all public safety radio and data communications sys-
28 tems and equipment purchased using homeland security assistance ad-
29 ministered by the Department, excluding an alert and warning device,
30 technology, or system;

31 (5) carry out the Department’s responsibilities and authorities relat-
32 ing to research, development, testing, evaluation, or standards-related
33 elements of the SAFECOM Program;

34 (6) evaluate and assess new technology in real-world environments
35 to achieve interoperable emergency communications capabilities;

36 (7) encourage more efficient use of existing resources, including
37 equipment, to achieve interoperable emergency communications capa-
38 bilities;

39 (8) test public safety communications systems that are less prone to
40 failure, support new nonvoice services, use the spectrum more effi-
41 ciently, and cost less than existing systems;

1 (9) coordinate with the private sector to develop solutions to improve
2 emergency communications capabilities and achieve interoperable emer-
3 gency communications capabilities; and

4 (10) conduct pilot projects, in coordination with the Director for
5 Emergency Communications, to test and demonstrate technologies, in-
6 cluding data and video, that enhance—

7 (A) the ability of emergency response providers and relevant
8 government officials to continue to communicate in the event of
9 natural disasters, acts of terrorism, and other man-made disasters;
10 and

11 (B) interoperable emergency communications capabilities.

12 (b) COORDINATION.—The Director of the Office for Interoperability and
13 Compatibility shall coordinate with the Director for Emergency Communica-
14 tions with respect to the SAFECOM program.

15 (c) SUFFICIENCY OF RESOURCES.—The Secretary shall provide the Office
16 for Interoperability and Compatibility the resources and staff necessary to
17 carry out the responsibilities under this section.

18 **§ 10914. Emergency communications interoperability re-**
19 **search and development**

20 (a) DEFINITION OF INTEROPERABLE EMERGENCY COMMUNICATIONS.—
21 In this section, the term “interoperable emergency communications” has the
22 meaning given the term “interoperable communications” under section
23 10912(a) of this title.

24 (b) IN GENERAL.—The Secretary, acting through the Under Secretary for
25 Science and Technology and the Director of the Office for Interoperability
26 and Compatibility, shall establish a comprehensive research and development
27 program to support and promote—

28 (1) the ability of emergency response providers and relevant govern-
29 ment officials to continue to communicate in the event of natural disas-
30 ters, acts of terrorism, and other man-made disasters; and

31 (2) interoperable emergency communications capabilities among
32 emergency response providers and relevant government officials, includ-
33 ing by—

34 (A) supporting research on a competitive basis, including
35 through the Directorate of Science and Technology Homeland Se-
36 curity Advanced Research Projects Agency; and

37 (B) considering the establishment of a Center of Excellence
38 under the Department of Homeland Security Centers of Excel-
39 lence Program focused on improving emergency response pro-
40 viders’ communication capabilities.

1 (c) PURPOSES.—The purposes of the program established under sub-
2 section (b) include—

3 (1) supporting research, development, testing, and evaluation on
4 emergency communication capabilities;

5 (2) understanding the strengths and weaknesses of the public safety
6 communications systems in use;

7 (3) examining how current and emerging technology can make emer-
8 gency response providers more effective, and how Federal, State, local,
9 and tribal government agencies can use this technology in a coherent
10 and cost-effective manner;

11 (4) investigating technologies that could lead to long-term advance-
12 ments in emergency communications capabilities and supporting re-
13 search on advanced technologies and potential systemic changes to dra-
14 matically improve emergency communications; and

15 (5) evaluating and validating advanced technology concepts, and fa-
16 cilitating the development and deployment of interoperable emergency
17 communication capabilities.

18 **§ 10915. National Biosurveillance Integration Center**

19 (a) DEFINITIONS.—In this section:

20 (1) BIOLOGICAL AGENT.—The term “biological agent” has the mean-
21 ing given the term in section 178 of title 18.

22 (2) BIOLOGICAL EVENT OF NATIONAL CONCERN.—The term “bio-
23 logical event of national concern” means—

24 (A) an act of terrorism involving a biological agent or toxin; or

25 (B) a naturally occurring outbreak of an infectious disease that
26 may result in a national epidemic.

27 (3) HOMELAND SECURITY INFORMATION.—The term “homeland se-
28 curity information” has the meaning given the term in section 11907
29 of this title.

30 (4) MEMBER AGENCY.—The term “Member Agency” means any
31 Federal department or agency that, at the discretion of the head of
32 that department or agency, has entered into a memorandum of under-
33 standing regarding participation in the National Biosurveillance Inte-
34 gration Center.

35 (5) PRIVACY OFFICER.—The term “Privacy Officer” means the Pri-
36 vacy Officer appointed under section 10520 of this title.

37 (6) TOXIN.—The term “toxin” has the meaning given the term in
38 section 178 of title 18.

39 (b) ESTABLISHMENT.—The Secretary, acting through the Assistant Sec-
40 retary for the Countering Weapons of Mass Destruction Office, shall estab-
41 lish, operate, and maintain a National Biosurveillance Integration Center

1 (in this section referred to as the “NBIC”) under an office or directorate
2 of the Department that was in existence as of August 3, 2007. The Direct-
3 ing Officer is the head of the NBIC.

4 (e) PRIMARY MISSION.—The primary mission of the NBIC is to—

5 (1) enhance the capability of the Federal Government to—

6 (A) rapidly identify, characterize, localize, and track a biological
7 event of national concern by integrating and analyzing data relat-
8 ing to human health, animal, plant, food, and environmental moni-
9 toring systems (both national and international); and

10 (B) disseminate alerts and other information to Member Agen-
11 cies and, in coordination with (and where possible through) Mem-
12 ber Agencies, to agencies of State, local, and tribal governments,
13 as appropriate, to enhance the ability of the agencies to respond
14 to a biological event of national concern; and

15 (2) oversee development and operation of the National Biosurveil-
16 lance Integration System.

17 (d) REQUIREMENTS.—The NBIC shall detect, as early as possible, a bio-
18 logical event of national concern that presents a risk to the United States
19 or the infrastructure or key assets of the United States, including by—

20 (1) consolidating data from all relevant surveillance systems main-
21 tained by Member Agencies to detect biological events of national con-
22 cern across human, animal, and plant species;

23 (2) seeking private sources of surveillance, both foreign and domes-
24 tic, when the sources would enhance coverage of critical surveillance
25 gaps;

26 (3) using an information technology system that uses the best avail-
27 able statistical and other analytical tools to identify and characterize
28 biological events of national concern in as close to real time as is prac-
29 ticable;

30 (4) providing the infrastructure for integration, including informa-
31 tion technology systems and space, and support for personnel from
32 Member Agencies with sufficient expertise to enable analysis and inter-
33 pretation of data;

34 (5) working with Member Agencies to create information technology
35 systems that use the minimum amount of patient data necessary and
36 consider patient confidentiality and privacy issues at all stages of devel-
37 opment and apprise the Privacy Officer of these efforts; and

38 (6) alerting Member Agencies and, in coordination with (and where
39 possible through) Member Agencies, public health agencies of State,
40 local, and tribal governments regarding an incident that could develop
41 into a biological event of national concern.

- 1 (e) RESPONSIBILITIES OF DIRECTING OFFICER.—
- 2 (1) IN GENERAL.—The Directing Officer of the NBIC shall—
- 3 (A) on an ongoing basis, monitor the availability and appro-
- 4 priateness of surveillance systems used by the NBIC and those
- 5 systems that could enhance biological situational awareness or the
- 6 overall performance of the NBIC;
- 7 (B) on an ongoing basis, review and seek to improve the statis-
- 8 tical and other analytical methods used by the NBIC;
- 9 (C) receive and consider other relevant homeland security infor-
- 10 mation, as appropriate; and
- 11 (D) provide technical assistance, as appropriate, to all Federal,
- 12 regional, State, local, and tribal government entities and private-
- 13 sector entities that contribute data relevant to the operation of the
- 14 NBIC.
- 15 (2) ASSESSMENTS.—The Directing Officer of the NBIC shall—
- 16 (A) on an ongoing basis, evaluate available data for evidence of
- 17 a biological event of national concern; and
- 18 (B) integrate homeland security information with NBIC data to
- 19 provide overall situational awareness and determine whether a bio-
- 20 logical event of national concern has occurred.
- 21 (3) INFORMATION SHARING.—
- 22 (A) IN GENERAL.—The Directing Officer of the NBIC shall—
- 23 (i) establish a method of real-time communication with the
- 24 National Operations Center;
- 25 (ii) in the event that a biological event of national concern
- 26 is detected, notify the Secretary and disseminate results of
- 27 NBIC assessments relating to that biological event of national
- 28 concern to appropriate Federal response entities and, in co-
- 29 ordination with relevant Member Agencies, regional, State,
- 30 local, and tribal governmental response entities in a timely
- 31 manner;
- 32 (iii) provide any report on NBIC assessments to Member
- 33 Agencies and, in coordination with relevant Member Agencies,
- 34 an affected regional, State, local, or tribal government, and
- 35 any private-sector entity considered appropriate that may en-
- 36 hance the mission of the Member Agencies, governments, or
- 37 entities or the ability of the Nation to respond to biological
- 38 events of national concern; and
- 39 (iv) share NBIC incident or situational awareness reports,
- 40 and other relevant information, consistent with the informa-
- 41 tion sharing environment established under section 11908 of

1 this title and policies, guidelines, procedures, instructions, or
2 standards established under that section.

3 (B) CONSULTATION.—The Directing Officer of the NBIC shall
4 implement the activities described in subparagraph (A) consistent
5 with the policies, guidelines, procedures, instructions, or standards
6 established under section 11908 of this title and in consultation
7 with the Director of National Intelligence, the Under Secretary for
8 Intelligence and Analysis, and other offices or agencies of the Fed-
9 eral Government, as appropriate.

10 (f) RESPONSIBILITIES OF MEMBER AGENCIES.—Each Member Agency
11 shall—

12 (1) use its best efforts to integrate biosurveillance information into
13 the NBIC, with the goal of promoting information sharing between
14 Federal, State, local, and tribal governments to detect biological events
15 of national concern;

16 (2) provide timely information to assist the NBIC in maintaining bi-
17 ological situational awareness for accurate detection and response pur-
18 poses;

19 (3) enable the NBIC to receive and use biosurveillance information
20 from Member Agencies to carry out its requirements under subsection
21 (d);

22 (4) connect the biosurveillance data systems of that Member Agency
23 to the NBIC data system under mutually agreed protocols that are
24 consistent with subsection (d)(5);

25 (5) participate in the formation of strategy and policy for the oper-
26 ation of the NBIC and its information sharing;

27 (6) provide personnel to the NBIC under an interagency personnel
28 agreement and consider the qualifications of the personnel necessary to
29 provide human, animal, and environmental data analysis and interpre-
30 tation support to the NBIC; and

31 (7) retain responsibility for the surveillance and intelligence systems
32 of that department or agency, if applicable.

33 (g) ADMINISTRATIVE AUTHORITIES.—

34 (1) HIRING OF EXPERTS.—The Directing Officer of the NBIC shall
35 hire individuals with the necessary expertise to develop and operate the
36 NBIC.

37 (2) DETAIL OF PERSONNEL.—On request of the Directing Officer of
38 the NBIC, the head of a Federal department or agency may detail, on
39 a reimbursable basis, personnel of the department or agency to the De-
40 partment to assist the NBIC in carrying out this section.

1 (h) NBIC INTERAGENCY WORKING GROUP.—The Directing Officer of the
2 NBIC shall—

3 (1) establish an interagency working group to facilitate interagency
4 cooperation and to advise the Directing Officer of the NBIC regarding
5 recommendations to enhance the biosurveillance capabilities of the De-
6 partment; and

7 (2) invite Member Agencies to serve on that working group.

8 (i) RELATIONSHIP TO OTHER DEPARTMENTS AND AGENCIES.—The au-
9 thority of the Directing Officer of the NBIC under this section shall not
10 affect the authority or responsibility of another department or agency of the
11 Federal Government with respect to biosurveillance activities under a pro-
12 gram administered by that department or agency.

13 **§ 10916. Promoting anti-terrorism through international co-**
14 **operation program**

15 (a) DEFINITIONS.—In this section:

16 (1) DIRECTOR.—The term “Director” means the Director selected
17 under subsection (b)(2).

18 (2) INTERNATIONAL COOPERATIVE ACTIVITY.—The term “inter-
19 national cooperative activity” includes—

20 (A) coordinated research projects, joint research projects, or
21 joint ventures;

22 (B) joint studies or technical demonstrations;

23 (C) coordinated field exercises, scientific seminars, conferences,
24 symposia, and workshops;

25 (D) training of scientists and engineers;

26 (E) visits and exchanges of scientists, engineers, or other appro-
27 priate personnel;

28 (F) exchanges or sharing of scientific and technological informa-
29 tion; and

30 (G) joint use of laboratory facilities and equipment.

31 (b) SCIENCE AND TECHNOLOGY HOMELAND SECURITY INTERNATIONAL
32 COOPERATIVE PROGRAMS OFFICE.—

33 (1) ESTABLISHMENT.—There is in the Department the Science and
34 Technology Homeland Security International Cooperative Programs Of-
35 fice.

36 (2) DIRECTOR.—A Director is the head of the Office. The Direc-
37 tor—

38 (A) shall be selected, in consultation with the Assistant Sec-
39 retary for International Affairs, by and shall report to the Under
40 Secretary for Science and Technology; and

1 (B) may be an officer of the Department serving in another po-
2 sition.

3 (3) RESPONSIBILITIES.—

4 (A) DEVELOPMENT OF MECHANISMS.—The Director is respon-
5 sible for developing, in coordination with the Department of State
6 and, as appropriate, the Department of Defense, the Department
7 of Energy, and other Federal agencies, understandings and agree-
8 ments to allow and to support international cooperative activity in
9 support of homeland security.

10 (B) PRIORITIES.—The Director is responsible for developing, in
11 coordination with the Office of International Affairs and other
12 Federal agencies, strategic priorities for international cooperative
13 activity for the Department in support of homeland security.

14 (C) ACTIVITIES.—The Director shall facilitate the planning, de-
15 velopment, and implementation of international cooperative activ-
16 ity to address the strategic priorities developed under subpara-
17 graph (B) through mechanisms the Under Secretary for Science
18 and Technology considers appropriate, including grants, coopera-
19 tive agreements, or contracts to or with foreign public or private
20 entities, governmental organizations, businesses (including small
21 businesses and socially and economically disadvantaged small busi-
22 nesses (as the terms are defined in sections 3 and 8 of the Small
23 Business Act (15 U.S.C. 632 and 637), respectively)), federally
24 funded research and development centers, and universities.

25 (D) IDENTIFICATION OF PARTNERS.—The Director shall facili-
26 tate the matching of United States entities engaged in homeland
27 security research with non-United States entities engaged in home-
28 land security research so that they may partner in homeland secu-
29 rity research activities.

30 (4) COORDINATION.—The Director shall ensure that the activities
31 under this subsection are coordinated with the Office of International
32 Affairs and the Department of State and, as appropriate, the Depart-
33 ment of Defense, the Department of Energy, and other relevant Fed-
34 eral agencies or interagency bodies. The Director may enter into joint
35 activities with other Federal agencies.

36 (e) MATCHING FUNDING.—

37 (1) IN GENERAL.—

38 (A) EQUITABILITY.—The Director shall ensure that funding
39 and resources expended in international cooperative activity will be
40 equitably matched by the foreign partner government or other en-

1 tity through direct funding, funding of complementary activities,
2 or the provision of staff, facilities, material, or equipment.

3 (B) GRANT MATCHING AND REPAYMENT.—

4 (i) IN GENERAL.—The Secretary may require a recipient of
5 a grant under this section—

6 (I) to make a matching contribution of not more than
7 50 percent of the total cost of the proposed project for
8 which the grant is awarded; and

9 (II) to repay to the Secretary the amount of the grant
10 (or a portion thereof), interest on the amount at an ap-
11 propriate rate, and charges for administration of the
12 grant the Secretary determines appropriate.

13 (ii) LIMIT ON REPAYMENT.—The Secretary may not re-
14 quire that repayment under clause (i)(II) be more than 150
15 percent of the amount of the grant, adjusted for inflation on
16 the basis of the Consumer Price Index.

17 (2) FOREIGN PARTNERS.—Partners may include Israel, the United
18 Kingdom, Canada, Australia, Singapore, and other allies in the global
19 war on terrorism as determined to be appropriate by the Secretary and
20 the Secretary of State.

21 (3) LOANS OF EQUIPMENT.—The Director may make or accept loans
22 of equipment for research and development and comparative testing
23 purposes.

24 (d) FOREIGN REIMBURSEMENTS.—If the Science and Technology Home-
25 land Security International Cooperative Programs Office participates in an
26 international cooperative activity with a foreign partner on a cost-sharing
27 basis, reimbursements or contributions received from that foreign partner
28 to meet its share of the project may be credited to appropriate current ap-
29 propriations accounts of the Directorate of Science and Technology.

30 (e) REPORT TO CONGRESS ON INTERNATIONAL COOPERATIVE ACTIVI-
31 TIES.—The Secretary, acting through the Under Secretary for Science and
32 Technology and the Director, shall submit to Congress not later than 1 year
33 after August 3, 2007, and every 5 years thereafter a report containing—

34 (1) a brief description of each grant, cooperative agreement, or con-
35 tract made or entered into under subsection (b)(3)(C), including the
36 participants, goals, and amount and sources of funding;

37 (2) a list of international cooperative activities underway, including
38 the participants, goals, expected duration, and amount and sources of
39 funding, including resources provided to support the activities in lieu
40 of direct funding;

1 (3) for international cooperative activities identified in the previous
2 reporting period, a status update on the progress of such activities, in-
3 cluding whether goals were realized, explaining any lessons learned, and
4 evaluating overall success; and

5 (4) a discussion of obstacles encountered in the course of forming,
6 executing, or implementing agreements for international cooperative ac-
7 tivities, including administrative, legal, or diplomatic challenges or re-
8 source constraints.

9 (f) ANIMAL AND ZOOLOGICAL DISEASES.—As part of the international co-
10 operative activities authorized in this section, the Under Secretary for
11 Science and Technology, in coordination with the Assistant Secretary for the
12 Office, the Department of State, and appropriate officials of the Depart-
13 ment of Agriculture, the Department of Defense, and the Department of
14 Health and Human Services, may enter into cooperative activities with for-
15 eign countries, including African nations, to strengthen American prepared-
16 ness against foreign animal and zoonotic diseases overseas that could harm
17 the Nation’s agricultural and public health sectors if they were to reach the
18 United States.

19 (g) CYBERSECURITY.—As part of the international cooperative activities
20 authorized in this section, the Under Secretary for Science and Technology,
21 in coordination with the Department of State and appropriate Federal offi-
22 cials, may enter into cooperative research activities with Israel to strengthen
23 preparedness against cyber threats and enhance capabilities in cybersecu-
24 rity.

25 (h) CONSTRUCTION; AUTHORITIES OF THE SECRETARY OF STATE.—
26 Nothing in this section shall be construed to alter or affect the following
27 provisions of law:

28 (1) Section 112b(e) of title 1.

29 (2) Section 622(c) of the Foreign Assistance Act of 1961 (22 U.S.C.
30 2382(c)).

31 (3) Section 1(e)(2) of the State Department Basic Authorities Act
32 of 1956 (22 U.S.C. 2651a(e)(2)).

33 (4) Title V of the Foreign Relations Authorization Act, Fiscal Year
34 1979 (22 U.S.C. 2656a et seq.).

35 (5) Sections 2 and 27 of the Arms Export Control Act (22 U.S.C.
36 2752, 2767).

37 **§ 10917. Transparency in research and development**

38 (a) DEFINITIONS.—In this section:

39 (1) ALL APPROPRIATE DETAILS.—The term “all appropriate details”
40 means, with respect to a research and development project—

- 1 (A) the name of the project, including classified and unclassified
- 2 names if applicable;
- 3 (B) the name of the component of the Department carrying out
- 4 the project;
- 5 (C) an abstract or summary of the project;
- 6 (D) funding levels for the project;
- 7 (E) project duration or timeline;
- 8 (F) the name of each contractor, grantee, or cooperative agree-
- 9 ment partner involved in the project;
- 10 (G) expected objectives and milestones for the project; and
- 11 (H) to the maximum extent practicable, relevant literature and
- 12 patents that are associated with the project.

13 (2) CLASSIFIED.—The term “classified” means anything con-

14 taining—

- 15 (A) classified national security information as defined in section
- 16 6.1 of Executive Order 13526 (50 U.S.C. 3161 note) or any suc-
- 17 cessor order;
- 18 (B) Restricted Data or data that was formerly Restricted Data,
- 19 as defined in section 11(y) of the Atomic Energy Act of 1954 (42
- 20 U.S.C. 2014(y));
- 21 (C) material classified at the Sensitive Compartmented Informa-
- 22 tion (SCI) level, as defined in section 309 of the Intelligence Au-
- 23 thorization Act for Fiscal Year 2001 (50 U.S.C. 3345); or
- 24 (D) information relating to a special access program, as defined
- 25 in section 6.1 of Executive Order 13526 (50 U.S.C. 3161 note)
- 26 or any successor order.

27 (3) CONTROLLED UNCLASSIFIED INFORMATION.—The term “con-

28 trolled unclassified information” means information described as “Con-

29 trolled Unclassified Information” under Executive Order 13556 (44

30 U.S.C. 3501 note) or any successor order.

31 (4) PROJECT.—The term “project” means a research or development

32 project, program, or activity administered by the Department, whether

33 ongoing, completed, or otherwise terminated.

34 (b) REQUIREMENT TO LIST RESEARCH AND DEVELOPMENT

35 PROJECTS.—

36 (1) IN GENERAL.—The Secretary shall maintain a detailed list of the

37 following:

- 38 (A) Each classified and unclassified research and development
- 39 project, and all appropriate details for each project, including the
- 40 component of the Department responsible for each project.

1 (B) Each task order for a federally funded research and devel-
2 opment center not associated with a research and development
3 project.

4 (C) Each task order for a university-based center of excellence
5 not associated with a research and development project.

6 (D) The indicators developed and tracked by the Under Sec-
7 retary for Science and Technology with respect to transitioned
8 projects pursuant to subsection (d).

9 (2) EXCEPTION.—Paragraph (1) shall not apply to a project com-
10 pleted or otherwise terminated before December 23, 2016.

11 (3) UPDATES.—The list required under paragraph (1) shall be up-
12 dated as frequently as possible, but not less frequently than once per
13 quarter.

14 (4) PROVIDE DEFINITION OF RESEARCH AND DEVELOPMENT.—For
15 purposes of the list required under paragraph (1), the Secretary shall
16 provide a definition for the term “research and development”.

17 (c) REPORT.—The Secretary each year shall submit to the Committee on
18 Homeland Security of the House of Representatives and the Committee on
19 Homeland Security and Governmental Affairs of the Senate a classified and
20 unclassified report, as applicable, that lists each ongoing classified and un-
21 classified project at the Department, including all appropriate details of
22 each project.

23 (d) INDICATORS OF SUCCESS FOR TRANSITIONED PROJECTS.—

24 (1) IN GENERAL.—For each project that has been transitioned to
25 practice from research and development, the Under Secretary for
26 Science and Technology shall develop and track indicators to dem-
27 onstrate the uptake of the technology or project among customers or
28 end-users.

29 (2) PERIOD OF TRACKING.—To the fullest extent possible, the track-
30 ing of a project required under paragraph (1) shall continue for the
31 3-year period beginning on the date the project was transitioned to
32 practice from research and development.

33 (e) LIMITATION.—Nothing in this section overrides or otherwise affects
34 the requirements specified in section 10312 of this title.

35 **§ 10918. EMP and GMD mitigation research and develop-**
36 **ment and threat assessment, response, and recov-**
37 **ery**

38 (a) IN GENERAL.—In furtherance of domestic preparedness and response,
39 the Secretary, acting through the Under Secretary for Science and Tech-
40 nology, and in consultation with other relevant executive agencies, relevant
41 State, local, and tribal governments, and relevant owners and operators of

1 critical infrastructure, shall, to the extent practicable, conduct research and
2 development to mitigate the consequences of threats of EMP and GMD.

3 (b) SCOPE.—The scope of the research and development under subsection
4 (a) shall include the following:

5 (1) An objective scientific analysis evaluating the risks to critical in-
6 frastructure from a range of threats of EMP and GMD that shall—

7 (A) be conducted in conjunction with the Office of Intelligence
8 and Analysis; and

9 (B) include a review and comparison of the range of threats and
10 hazards facing critical infrastructure of the electrical grid.

11 (2) A determination of the critical utilities and national security as-
12 sets and infrastructure that are at risk from EMP and GMD.

13 (3) An evaluation of emergency planning and response technologies
14 that would address the findings and recommendations of experts, in-
15 cluding those of the Commission to Assess the Threat to the United
16 States from Electromagnetic Pulse Attack, which shall include a review
17 of the feasibility of rapidly isolating 1 or more portions of the electrical
18 grid from the main electrical grid.

19 (4) An analysis of technology options that are available to improve
20 the resiliency of critical infrastructure to threats of EMP and GMD,
21 including an analysis of neutral current blocking devices that may pro-
22 tect high-voltage transmission lines.

23 (5) The restoration and recovery capabilities of critical infrastructure
24 under different levels of damage and disruption from various threats
25 of EMP and GMD, as informed by the scientific analysis conducted
26 under paragraph (1).

27 (6) An analysis of the feasibility of a real-time alert system to inform
28 electoral grid operators and other stakeholders within milliseconds of
29 a high-altitude nuclear explosion.

30 (c) EXEMPTION FROM DISCLOSURE.—

31 (1) INFORMATION SHARED WITH FEDERAL GOVERNMENT.—Section
32 10733 of this title, and any regulations issued pursuant to section
33 10733 of this title, apply to any information shared with the Federal
34 Government under this section.

35 (2) INFORMATION SHARED BY FEDERAL GOVERNMENT.—Informa-
36 tion shared by the Federal Government with a State, local, or tribal
37 government under this section is exempt from disclosure under any
38 provision of State, local, or tribal freedom of information law, open gov-
39 ernment law, open meetings law, open records law, sunshine law, or
40 similar law requiring the disclosure of information or records.

41 (d) THREAT ASSESSMENT, RESPONSE, AND RECOVERY.—

1 (1) DEFINITIONS.—In this subsection:

2 (A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term
3 “appropriate congressional committees” means—

4 (i) the Committee on Homeland Security and Govern-
5 mental Affairs, the Committee on Armed Services, the Com-
6 mittee on Energy and Natural Resources, and the Committee
7 on Commerce, Science, and Transportation of the Senate; and

8 (ii) the Committee on Transportation and Infrastructure,
9 the Committee on Homeland Security, the Committee on
10 Armed Services, the Committee on Energy and Commerce,
11 and the Committee on Science, Space and Technology of the
12 House of Representatives.

13 (B) PREPARE; PREPAREDNESS.—The terms “prepare” and
14 “preparedness” mean the actions taken to plan, organize, equip,
15 train, and exercise to build and sustain the capabilities necessary
16 to prevent, protect against, mitigate the effects of, respond to, and
17 recover from those threats that pose the greatest risk to the secu-
18 rity of the homeland, including the prediction and notification of
19 impending EMPs and GMDs.

20 (C) SECTOR RISK MANAGEMENT AGENCY.—The term “Sector
21 Risk Management Agency” has the meaning given that term in
22 section 10701 of this title.

23 (2) ROLES AND RESPONSIBILITIES.—

24 (A) DISTRIBUTION OF INFORMATION.—

25 (i) IN GENERAL.—The Secretary shall provide timely dis-
26 tribution of information on EMPs and GMDs to Federal,
27 State, and local governments, owners and operators of critical
28 infrastructure, and other persons determined appropriate by
29 the Secretary.

30 (ii) BRIEFING.—The Secretary shall brief the appropriate
31 congressional committees on the effectiveness of the distribu-
32 tion of information under clause (i).

33 (B) RESPONSE AND RECOVERY.—

34 (i) IN GENERAL.—The Administrator of the Federal Emer-
35 gency Management Agency shall—

36 (I) coordinate the response to and recovery from the
37 effects of EMPs and GMDs on critical infrastructure, in
38 coordination with the heads of appropriate Sector Risk
39 Management Agencies, and on matters related to the
40 bulk power system, in consultation with the Secretary of

1 Energy and the Federal Energy Regulatory Commission;
2 and

3 (II) to the extent practicable, incorporate events that
4 include EMPs and extreme GMDs as a factor in pre-
5 paredness scenarios and exercises.

6 (ii) IMPLEMENTATION.—The Administrator of the Federal
7 Emergency Management Agency, in coordination with the Di-
8 rector of the Cybersecurity and Infrastructure Security Agen-
9 cy, and on matters related to the bulk power system, the Sec-
10 retary of Energy and the Federal Energy Regulatory Com-
11 mission, shall—

12 (I) develop plans and procedures to coordinate the re-
13 sponse to and recovery from EMP and GMD events; and

14 (II) not later than December 21, 2020, conduct a na-
15 tional exercise to test the preparedness and response of
16 the Nation to the effect of an EMP or extreme GMD
17 event.

18 (C) RESEARCH AND DEVELOPMENT.—

19 (i) IN GENERAL.—The Secretary, in coordination with the
20 heads of relevant Sector Risk Management Agencies, shall—

21 (I) without duplication of existing or ongoing efforts,
22 conduct research and development to better understand
23 and more effectively model the effects of EMPs and
24 GMDs on critical infrastructure (which shall not include
25 any system or infrastructure of the Department of De-
26 fense or any system or infrastructure of the Department
27 of Energy associated with nuclear weapons activities);
28 and

29 (II) develop technologies to enhance the resilience of
30 and better protect critical infrastructure.

31 (ii) PLAN.—In coordination with the heads of relevant Sec-
32 tor Risk Management Agencies, the Secretary shall submit to
33 the appropriate congressional committees a research and de-
34 velopment action plan to rapidly address modeling shortfall
35 and technology development.

36 (D) EMERGENCY INFORMATION SYSTEM.—

37 (i) IN GENERAL.—The Administrator of the Federal Emer-
38 gency Management Agency, in coordination with relevant
39 stakeholders, shall maintain a network of systems, such as
40 the alerting capabilities of the integrated public alert and
41 warning system authorized under section 11322 of this title,

1 that are capable of providing appropriate emergency informa-
2 tion to the public before (if possible), during, and in the
3 aftermath of an EMP or GMD.

4 (ii) BRIEFING.—Not later than December 21, 2020, the
5 Administrator of the Federal Emergency Management Agen-
6 cy, shall brief the appropriate congressional committees re-
7 garding the maintenance of systems, including the alerting
8 capabilities of the integrated public alert and warning system
9 authorized under section 11322 of this title.

10 (E) QUADRENNIAL RISK ASSESSMENTS.—

11 (i) IN GENERAL.—The Secretary, in coordination with the
12 Secretary of Defense, the Secretary of Energy, and the Sec-
13 retary of Commerce, and informed by intelligence-based
14 threat assessments, shall conduct a quadrennial EMP and
15 GMD risk assessment.

16 (ii) BRIEFINGS.—Not later than March 26, 2020, and
17 every four years thereafter until 2032, the Secretary, the Sec-
18 retary of Defense, the Secretary of Energy, and the Secretary
19 of Commerce shall provide a briefing to the appropriate con-
20 gressional committees regarding the quadrennial EMP and
21 GMD risk assessment.

22 (iii) ENHANCING RESILIENCE.—The Secretary, in coordina-
23 tion with the Secretary of Defense, the Secretary of Energy,
24 the Secretary of Commerce, and the heads of other relevant
25 Sector Risk Management Agencies, shall use the results of
26 the quadrennial EMP and GMD risk assessments to better
27 understand and to improve resilience to the effects of EMPs
28 and GMDs across all critical infrastructure sectors, including
29 coordinating the prioritization of critical infrastructure at
30 greatest risk to the effects of EMPs and GMDs.

31 (3) COORDINATION.—

32 (A) REPORT ON TECHNOLOGICAL OPTIONS.—Not later than De-
33 cember 21, 2020, and every four years thereafter until 2032, the
34 Secretary, in coordination with the Secretary of Defense, the Sec-
35 retary of Energy, the heads of other appropriate agencies, and, as
36 appropriate, private-sector partners, shall submit to the appro-
37 priate congressional committees, a report that—

38 (i) assesses the technological options available to improve
39 the resilience of critical infrastructure to the effects of EMPs
40 and GMDs; and

1 (ii) identifies gaps in available technologies and opportuni-
2 ties for technological developments to inform research and de-
3 velopment activities.

4 (B) TEST DATA.—

5 (i) IN GENERAL.—Not later than December 20, 2020, the
6 Secretary, in coordination with the heads of Sector Risk Man-
7 agement Agencies, the Secretary of Defense, and the Sec-
8 retary of Energy, shall—

9 (I) review test data regarding the effects of EMPs and
10 GMDs on critical infrastructure systems, networks, and
11 assets representative of those throughout the Nation;
12 and

13 (II) identify gaps in the test data.

14 (ii) PLAN.—Not later than 180 days after identifying gaps
15 in test data under clause (i), the Secretary, in coordination
16 with the heads of Sector Risk Management Agencies and in
17 consultation with the Secretary of Defense and the Secretary
18 of Energy, shall use the sector partnership structure identi-
19 fied in the National Infrastructure Protection Plan to develop
20 an integrated cross-sector plan to address the identified gaps.

21 (iii) IMPLEMENTATION.—The heads of each agency identi-
22 fied in the plan developed under clause (ii) shall implement
23 the plan in collaboration with the voluntary efforts of the pri-
24 vate sector, as appropriate.

25 (e) CONSTRUCTION.—Nothing in this section may be construed—

26 (1) to affect in any manner the authority of the executive branch to
27 implement Executive Order 13865 (March 26, 2019, 84 Fed. Reg.
28 12041) or any other authority existing on the day before December 20,
29 2019, of any other component of the Department or any other Federal
30 department or agency, including the authority provided to the Sector
31 Risk Management Agency specified in section 61003(e) of division F
32 of the Fixing America’s Surface Transportation Act (Public Law 114–
33 94, 129 Stat. 1778), including the authority under section 215 of the
34 Federal Power Act (16 U.S.C. 824o), and including the authority of
35 independent agencies to be independent; or

36 (2) as diminishing or transferring any authorities vested in the Ad-
37 ministrator of the Federal Emergency Management Agency or in the
38 Agency prior to December 20, 2019.

39 **§ 10919. National Urban Security Technology Laboratory**

40 (a) DESIGNATION.—The Secretary, acting through the Under Secretary
41 for Science and Technology, shall designate as an additional laboratory pur-

1 pursuant to the authority under section 10907(c)(2) of this title the laboratory
2 known, as of December 27, 2021, as the National Urban Security Tech-
3 nology Laboratory and transferred to the Department pursuant to section
4 10902(1)(E) of this title.

5 (b) USES.— The National Urban Security Technology Laboratory shall
6 be used to test and evaluate emerging technologies and conduct research
7 and development to assist emergency response providers in preparing for,
8 and protecting against, threats of terrorism.

9 (c) ACTIVITIES.—The National Urban Security Technology Laboratory
10 shall—

11 (1) conduct tests, evaluations, and assessments of current and
12 emerging technologies, including, as appropriate, the cybersecurity of
13 technologies that can connect to the internet, for emergency response
14 providers;

15 (2) act as a technical advisor to emergency response providers; and

16 (3) carry out other such activities as the Secretary determines appro-
17 priate.

18 (d) RULE OF CONSTRUCTION.—Nothing in this section may be construed
19 as affecting in any manner the authorities or responsibilities of the Coun-
20 tering Weapons of Mass Destruction Office of the Department.

21 **§ 10920. Chemical Security Analysis Center**

22 (a) DESIGNATION.—The Secretary, acting through the Under Secretary
23 for Science and Technology, shall designate as an additional laboratory pur-
24 suant to the authority under section 10907(c)(2) of this title the laboratory
25 known, as of December 23, 2022, as the Chemical Security Analysis Center.

26 (b) USES.— The Chemical Security Analysis Center shall be used to con-
27 duct studies, analysis, and research to assess and address domestic chemical
28 security events.

29 (c) ACTIVITIES.—Pursuant to the authority under section 10910(4) of
30 this title, the Chemical Security Analysis Center shall—

31 (1) identify and develop approaches and mitigation strategies to do-
32 mestic chemical security threats, including the development of com-
33 prehensive, research-based definable goals relating to those approaches
34 and mitigation strategies;

35 (2) provide an enduring science-based chemical threat and hazard
36 analysis capability;

37 (3) provide expertise regarding risk and consequence modeling,
38 chemical sensing and detection, analytical chemistry, acute chemical
39 toxicology, synthetic chemistry and reaction characterization, and non-
40 traditional chemical agents and emerging chemical threats;

1 (4) staff and operate a technical assistance program that provides
2 operational support and subject matter expertise, design and execute
3 laboratory and field tests, and provide a comprehensive knowledge re-
4 pository of chemical threat information that is continuously updated
5 with data from scientific intelligence, operational, and private sector
6 sources;

7 (5) consult, as appropriate, with the Countering Weapons of Mass
8 Destruction Office of the Department to mitigate, prepare for, and re-
9 spond to, threats, hazards, and risks associated with domestic chemical
10 security threats; and

11 (6) carry out such other activities authorized under this section as
12 the Secretary considers appropriate.

13 (d) SPECIAL RULE.—Nothing in this section amends, alters, or affects—

14 (1) the responsibilities of the Countering Weapons of Mass Destruction
15 Office of the Department; or

16 (2) the activities or requirements authorized to other entities in the
17 Federal Government, including the activities and requirements of the
18 Environmental Protection Agency under section 112(r) of the Clean Air
19 Act (42 U.S.C. 7412(r)), the Toxic Substances Control Act (15 U.S.C.
20 2601 et seq.), and the Comprehensive Environmental Response, Com-
21 pensation, and Liability Act of 1980 (42 U.S.C. 9601 et seq.).

22 **Subchapter II—Supporting Anti-Terrorism** 23 **by Protecting Effective Technologies**

24 **§ 10931. Definitions**

25 In this subchapter:

26 (1) ACT OF TERRORISM.—The term “act of terrorism” means an act
27 that the Secretary determines meets all of the following requirements,
28 as the requirements are further defined and specified by the Secretary:

29 (A) The act is unlawful.

30 (B) The act causes harm to a person, property, or entity, in the
31 United States, or in the case of a domestic United States air car-
32 rier or a United States-flag vessel (or a vessel based principally
33 in the United States on which United States income tax is paid
34 and whose insurance coverage is subject to regulation in the
35 United States), in or outside the United States.

36 (C) The act uses or attempts to use instrumentalities, weapons,
37 or other methods designed or intended to cause mass destruction,
38 injury, or other loss to citizens or institutions of the United
39 States.

40 (2) INSURANCE CARRIER.—The term “insurance carrier” means a
41 corporation, association, society, order, firm, company, mutual, part-

1 nership, individual aggregation of individuals, or another legal entity
2 that provides commercial property and casualty insurance, including an
3 affiliate of a commercial insurance carrier.

4 (3) LIABILITY INSURANCE.—The term “liability insurance” means
5 insurance for legal liabilities incurred by the insured resulting from—

6 (A) loss of, or damage to, property of others;

7 (B) ensuing loss of income or extra expense incurred because
8 of loss of, or damage to, property of others;

9 (C) bodily injury, including to persons other than the insured
10 or its employees; or

11 (D) loss resulting from debt or default of another.

12 (4) LOSS.—The term “loss” means death, bodily injury, or loss of,
13 or damage to, property, including business interruption loss.

14 (5) NON-FEDERAL GOVERNMENT CUSTOMERS.—The term “non-Fed-
15 eral Government customers” means a customer of a Seller that is not
16 an agency or instrumentality of the United States Government with au-
17 thority under Public Law 85–804 (50 U.S.C. 1431 et seq.) to provide
18 for indemnification under certain circumstances for third party claims
19 against its contractors, including State and local authorities and com-
20 mercial entities.

21 (6) QUALIFIED ANTI-TERRORISM TECHNOLOGY.—The term “quali-
22 fied anti-terrorism technology” means a product, equipment, service
23 (including support services), device, or technology (including informa-
24 tion technology) designed, developed, modified, or procured for the spe-
25 cific purpose of preventing, detecting, identifying, or deterring acts of
26 terrorism or limiting the harm the acts might otherwise cause, that is
27 designated as such by the Secretary.

28 (7) SELLER.—The term “Seller” means a person or entity that sells
29 or otherwise provides a qualified anti-terrorism technology to Federal
30 and non-Federal Government customers.

31 **§ 10932. Administration**

32 (a) IN GENERAL.—The Secretary is responsible for the administration of
33 this subchapter.

34 (b) DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES.—
35 The Secretary may designate anti-terrorism technologies that qualify for
36 protection under the system of risk management set forth in this subchapter
37 in accordance with criteria that shall include the following:

38 (1) Prior United States Government use or demonstrated substantial
39 utility and effectiveness.

40 (2) Availability of the technology for immediate deployment in public
41 and private settings.

1 (3) Existence of extraordinarily large or extraordinarily
2 unquantifiable potential third party liability risk exposure to the Seller
3 or other provider of the anti-terrorism technology.

4 (4) Substantial likelihood that the anti-terrorism technology will not
5 be deployed unless protections under the system of risk management
6 provided under this subchapter are extended.

7 (5) Magnitude of risk exposure to the public if the anti-terrorism
8 technology is not deployed.

9 (6) Evaluation of all scientific studies that can be feasibly conducted
10 in order to assess the capability of the technology to substantially re-
11 duce risks of harm.

12 (7) Anti-terrorism technology that would be effective in facilitating
13 the defense against acts of terrorism, including technologies that pre-
14 vent, defeat, or respond to the acts.

15 (e) REGULATIONS.—The Secretary may issue regulations, after notice
16 and comment under section 553 of title 5, necessary to carry out this sub-
17 chapter.

18 **§ 10933. Litigation management**

19 (a) FEDERAL CAUSE OF ACTION.—

20 (1) IN GENERAL.—There shall exist a Federal cause of action for
21 claims arising out of, relating to, or resulting from, an act of terrorism
22 when qualified anti-terrorism technologies have been deployed in de-
23 fense against, in response to, or in recovery from the act, and the
24 claims result, or may result, in loss to the Seller. The substantive law
25 for decision in any action shall be derived from the law, including
26 choice of law principles, of the State in which the act of terrorism oc-
27 curred, unless the law is inconsistent with or preempted by Federal
28 law. The Federal cause of action shall be brought only for claims for
29 injuries that are proximately caused by Sellers that provide qualified
30 anti-terrorism technology to Federal and non-Federal Government cus-
31 tomers.

32 (2) JURISDICTION.—An appropriate district court of the United
33 States shall have original and exclusive jurisdiction over all actions for
34 any claim for loss of property, personal injury, or death arising out of,
35 relating to, or resulting from, an act of terrorism when qualified anti-
36 terrorism technologies have been deployed in defense against, in re-
37 sponse to, or in recovery from the act, and the claims result, or may
38 result, in loss to the Seller.

39 (b) SPECIAL RULES.—In an action brought under this section for dam-
40 ages, the following provisions apply:

1 (1) PUNITIVE DAMAGES; INTEREST.—No punitive damages intended
2 to punish or deter, exemplary damages, or other damages not intended
3 to compensate a plaintiff for actual losses may be awarded, nor shall
4 any party be liable for interest prior to the judgment.

5 (2) NONECONOMIC DAMAGES.—

6 (A) DEFINITION OF NONECONOMIC DAMAGES.—In this para-
7 graph, the term “noneconomic damages” means damages for
8 losses for physical and emotional pain, suffering, inconvenience,
9 physical impairment, mental anguish, disfigurement, loss of enjoy-
10 ment of life, loss of society and companionship, loss of consortium,
11 hedonic damages, injury to reputation, and any other nonpecu-
12 niary losses.

13 (B) WHEN AWARDED.—Noneconomic damages may be awarded
14 against a defendant only in an amount directly proportional to the
15 percentage of responsibility of the defendant for the harm to the
16 plaintiff, and no plaintiff may recover noneconomic damages un-
17 less the plaintiff suffered physical harm.

18 (c) COLLATERAL SOURCES.—Any recovery by a plaintiff in an action
19 under this section shall be reduced by the amount of collateral source com-
20 pensation, if any, that the plaintiff has received or is entitled to receive as
21 a result of the act of terrorism that results or may result in loss to the Sell-
22 er.

23 (d) GOVERNMENT CONTRACTOR DEFENSE.—

24 (1) IN GENERAL.—Should a product liability or other lawsuit be filed
25 for claims arising out of, relating to, or resulting from, an act of ter-
26 rorism when qualified anti-terrorism technologies approved by the Sec-
27 retary, as provided in paragraphs (2) and (3), have been deployed in
28 defense against, in response to, or in recovery from the act, and the
29 claims result, or may result, in loss to the Seller, there shall be a rebut-
30 table presumption that the government contractor’s defense applies in
31 the lawsuit. This presumption shall only be overcome by evidence show-
32 ing that the Seller acted fraudulently or with willful misconduct in sub-
33 mitting information to the Secretary during the course of the Sec-
34 retary’s consideration of the technology under this subsection. This pre-
35 sumption of the government contractor’s defense shall apply regardless
36 of whether the claim against the Seller arises from a sale of the prod-
37 uct to Federal Government or non-Federal Government customers.

38 (2) EXCLUSIVE RESPONSIBILITY.—The Secretary is exclusively re-
39 sponsible for the review and approval of anti-terrorism technology for
40 purposes of establishing a government contractor’s defense in any prod-
41 uct liability lawsuit for claims arising out of, relating to, or resulting

1 from, an act of terrorism when qualified anti-terrorism technologies ap-
2 proved by the Secretary, as provided in this paragraph and paragraph
3 (3), have been deployed in defense against, in response to, or in recov-
4 ery from the act, and the claims result, or may result, in loss to the
5 Seller. Upon the Seller's submission to the Secretary for approval of
6 anti-terrorism technology, the Secretary shall conduct a comprehensive
7 review of the design of the technology and determine whether it will
8 perform as intended, conforms to the Seller's specifications, and is safe
9 for use as intended. The Seller shall conduct safety and hazard anal-
10 yses on the technology and shall supply the Secretary with all such in-
11 formation relating to the analyses.

12 (3) CERTIFICATE.—For anti-terrorism technology reviewed and ap-
13 proved by the Secretary, the Secretary shall issue a certificate of con-
14 formance to the Seller and place the anti-terrorism technology on an
15 Approved Product List for Homeland Security.

16 (e) EXCLUSION.—Nothing in this section shall in any way limit the ability
17 of any person to seek any form of recovery from any person, government,
18 or other entity that—

19 (1) attempts to commit, knowingly participates in, aids and abets,
20 or commits any act of terrorism, or any criminal act related to or re-
21 sulting from the act of terrorism; or

22 (2) participates in a conspiracy to commit an act of terrorism or a
23 criminal act.

24 **§ 10934. Risk management**

25 (a) IN GENERAL.—

26 (1) LIABILITY INSURANCE REQUIRED.—The Seller shall obtain liabil-
27 ity insurance of the types and in the amounts as required under this
28 section and certified by the Secretary to satisfy otherwise compensable
29 third party claims arising out of, relating to, or resulting from, an act
30 of terrorism when qualified anti-terrorism technologies have been de-
31 ployed in defense against, in response to, or in recovery from the act.

32 (2) MAXIMUM AMOUNT.—For the total claims related to 1 act of ter-
33 rorism, the Seller is not required to obtain liability insurance of more
34 than the maximum amount of liability insurance reasonably available
35 from private sources on the world market at prices and terms that will
36 not unreasonably distort the sales price of Seller's anti-terrorism tech-
37 nologies.

38 (3) SCOPE OF COVERAGE.—Liability insurance obtained under this
39 subsection shall protect, in addition to the Seller, the following, to the
40 extent of their potential liability for involvement in the manufacture,
41 qualification, sale, use, or operation of qualified anti-terrorism tech-

1 nologies deployed in defense against, in response to, or in recovery from
2 an act of terrorism:

3 (A) Contractors, subcontractors, suppliers, vendors and cus-
4 tomers of the Seller.

5 (B) Contractors, subcontractors, suppliers, and vendors of the
6 customer.

7 (4) **THIRD PARTY CLAIMS.**—The liability insurance under this sec-
8 tion shall provide coverage against third party claims arising out of,
9 relating to, or resulting from the sale or use of anti-terrorism tech-
10 nologies.

11 (b) **RECIPROCAL WAIVER OF CLAIMS.**—The Seller shall enter into a re-
12 ciprocal waiver of claims with its contractors, subcontractors, suppliers, ven-
13 dors and customers, and contractors and subcontractors of the customers,
14 involved in the manufacture, sale, use, or operation of qualified anti-ter-
15 rorism technologies, under which each party to the waiver agrees to be re-
16 sponsible for losses, including business interruption losses, that it sustains,
17 or for losses sustained by its own employees resulting from an activity re-
18 sulting from an act of terrorism when qualified anti-terrorism technologies
19 have been deployed in defense against, in response to, or in recovery from
20 the act.

21 (c) **EXTENT OF LIABILITY.**—Notwithstanding another law, liability for all
22 claims against a Seller arising out of, relating to, or resulting from, an act
23 of terrorism when qualified anti-terrorism technologies have been deployed
24 in defense against, in response to, or in recovery from the act, and the
25 claims result, or may result, in loss to the Seller, whether for compensatory
26 or punitive damages or for contribution or indemnity, shall not be in an
27 amount greater than the limits of liability insurance coverage required to
28 be maintained by the Seller under this section.

29 **Subchapter III—Biodefense**

30 **§ 10941. National biodefense strategy and implementation** 31 **plan**

32 (a) **DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEE.**—In this
33 section, the term “appropriate congressional committee” means the fol-
34 lowing:

35 (1) The Committees on Armed Services and Appropriations of the
36 House of Representatives and the Senate.

37 (2) The Committee on Energy and Commerce of the House of Rep-
38 resentatives and the Committee on Health, Education, Labor, and Pen-
39 sions of the Senate.

1 (3) The Committee on Homeland Security of the House of Rep-
2 representatives and the Committee on Homeland Security and Govern-
3 mental Affairs of the Senate.

4 (4) The Committee on Agriculture of the House of Representatives
5 and the Committee on Agriculture, Nutrition, and Forestry of the Sen-
6 ate.

7 (b) STRATEGY AND IMPLEMENTATION PLAN.—The Secretary and the
8 Secretaries of Defense, Health and Human Services, and Agriculture jointly
9 shall develop a national biodefense strategy and associated implementation
10 plan, which shall include a review and assessment of biodefense policies,
11 practices, programs, and initiatives. The Secretaries shall review and, as ap-
12 propriate, revise the strategy biennially.

13 (c) ELEMENTS OF STRATEGY AND PLAN.—The strategy and associated
14 implementation plan required under subsection (b) shall include each of the
15 following:

16 (1) An inventory and assessment of all existing strategies, plans,
17 policies, laws, and interagency agreements relating to biodefense, in-
18 cluding prevention, deterrence, preparedness, detection, response, attri-
19 bution, recovery, and mitigation.

20 (2) A description of the biological threats, including biological war-
21 fare, bioterrorism, naturally occurring infectious diseases, and acci-
22 dental exposures.

23 (3) A description of the current program, efforts, or activities of the
24 United States Government with respect to preventing the acquisition,
25 proliferation, and use of a biological weapon, preventing an accidental
26 or naturally occurring biological outbreak, and mitigating the effects of
27 a biological epidemic.

28 (4) A description of the roles and responsibilities of the executive
29 agencies, including internal and external coordination procedures, in
30 identifying and sharing information relating to, warning of, and pro-
31 tecting against, acts of terrorism using biological agents and weapons
32 and accidental or naturally occurring biological outbreaks.

33 (5) An articulation of related or required interagency capabilities and
34 whole-of-Government activities required to support the national bio-
35 defense strategy.

36 (6) Recommendations for strengthening and improving the current
37 biodefense capabilities, authorities, and command structure of the
38 United States Government.

39 (7) Recommendations for improving and formalizing interagency co-
40 ordination and support mechanisms with respect to providing a robust
41 national biodefense.

1 (8) Any other matters the Secretary and the Secretaries of Defense,
2 Health and Human Services, and Agriculture determine necessary.

3 (d) SUBMITTAL TO CONGRESS.—The Secretary and the Secretaries of
4 Defense, Health and Human Services, and Agriculture shall submit to the
5 appropriate congressional committees the strategy and associated implemen-
6 tation plan required by subsection (b). The strategy and implementation
7 plan shall be submitted in unclassified form but may include a classified
8 annex.

9 (e) BRIEFINGS.—Not later than March 1, 2021, and annually thereafter
10 until March 1, 2025, the Secretary and the Secretaries of Defense, Health
11 and Human Services, and Agriculture shall provide to the Committees on
12 Armed Services, Energy and Commerce, Homeland Security, and Agri-
13 culture of the House of Representatives a joint briefing on the strategy de-
14 veloped under subsection (b) and the status of the implementation of the
15 strategy.

16 (f) COMPTROLLER GENERAL REVIEW.—Not later than 180 days after the
17 date of the submittal of the strategy and implementation plan under sub-
18 section (d), the Comptroller General shall conduct a review of the strategy
19 and implementation plan to analyze gaps and resources mapped against the
20 requirements of the national biodefense strategy and existing United States
21 biodefense policy documents.

22 **§ 10942. Update of national biodefense implementation plan**

23 (a) DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEES.—In
24 this section, the term “appropriate congressional committees” means the
25 following:

26 (1) The Committees on Armed Services of the House of Representa-
27 tives and the Senate.

28 (2) The Committee on Energy and Commerce of the House of Rep-
29 resentatives and the Committee on Health, Education, Labor, and Pen-
30 sions of the Senate.

31 (3) The Committee on Homeland Security of the House of Rep-
32 resentatives and the Committee on Homeland Security and Govern-
33 mental Affairs of the Senate.

34 (4) The Committee on Agriculture of the House of Representatives
35 and the Committee on Agriculture, Nutrition, and Forestry of the Sen-
36 ate.

37 (5) The Permanent Select Committee on Intelligence of the House
38 of Representatives and the Select Committee on Intelligence of the Sen-
39 ate.

40 (6) The Committee on Foreign Affairs of the House of Representa-
41 tives and the Committee on Foreign Relations of the Senate.

1 (b) RULE OF CONSTRUCTION.—Nothing in this section shall be construed
2 to alter, limit, or duplicate the roles, responsibilities, authorities, or current
3 activities, as established in statute or otherwise through existing practice or
4 policy, of each Federal department or agency with responsibilities for bio-
5 defense or otherwise relevant to implementation of the national biodefense
6 strategy.

7 (c) UPDATED BIODEFENSE THREAT ASSESSMENT.—

8 (1) IN GENERAL.—The Secretary and the Secretaries of Health and
9 Human Services, Defense, and Agriculture shall jointly, and in con-
10 sultation with the Director of National Intelligence, and other agency
11 heads as appropriate—

12 (A) conduct an assessment of current and potential biological
13 threats against the United States, both naturally occurring and
14 man-made, either accidental or deliberate, including the potential
15 for catastrophic biological threats, such as a pandemic;

16 (B) not later than 1 year after January 1, 2021, submit the
17 findings of the assessment conducted under subparagraph (A) to
18 the Federal officials described in subsection (d)(1) and the appro-
19 priate congressional committees;

20 (C) not later than 30 days after the date on which the assess-
21 ment is submitted under subparagraph (B), conduct a briefing for
22 the appropriate congressional committees on the findings of the
23 assessment;

24 (D) update the assessment under subparagraph (A) biennially,
25 as appropriate, and provide the findings of the updated assess-
26 ments to the Federal officials described in this paragraph and the
27 appropriate congressional committees; and

28 (E) conduct briefings for the appropriate congressional commit-
29 tees as needed any time an assessment under this paragraph is
30 updated.

31 (2) CLASSIFICATION AND FORMAT.—Assessments under paragraph
32 (1) shall be submitted in an unclassified format and include a classified
33 annex, as appropriate.

34 (d) UPDATED NATIONAL BIODEFENSE IMPLEMENTATION PLAN.—The
35 Secretary, the Secretaries of Health and Human Services, Defense, and Ag-
36 riculture, and all other departments and agencies with responsibilities for
37 biodefense, such as the Department of State, in consultation with the As-
38 sistant to the President for National Security Affairs and the Director of
39 the Office of Management and Budget, as appropriate, shall jointly, after
40 reviewing the biodefense threat assessment described in subsection (c) and
41 any relevant input from external stakeholders, as appropriate, update the

1 national biodefense implementation plan developed under section 10941 of
2 this title to clearly document established processes, roles, and responsibil-
3 ities related to the national biodefense strategy.

4 (e) SPECIFIC UPDATES.—The updated national biodefense implementa-
5 tion plan shall—

6 (1) describe the roles and responsibilities of the Federal departments
7 and agencies, including internal and external coordination procedures,
8 in identifying and sharing information between and among Federal de-
9 partments and agencies, as described in section 10941(c)(4) of this
10 title and consistent with the statutory roles and authorities of those de-
11 partments and agencies;

12 (2) describe roles, responsibilities, and processes for decision-making,
13 including decisions regarding use of resources for effective risk man-
14 agement across the enterprise;

15 (3) describe resource plans for each department and agency with re-
16 sponsibility for biodefense to support implementation of the strategy
17 within the jurisdiction of the department or agency, including for the
18 biodefense coordination team, as appropriate;

19 (4) describe guidance and methods for analyzing the data collected
20 from agencies to include non-Federal resources and capabilities to the
21 extent practicable; and

22 (5) describe and update, as appropriate, short-, medium-, and long-
23 term goals for executing the national biodefense strategy and metrics
24 for meeting each objective of the strategy.

25 (f) SUBMITTAL TO CONGRESS.—The Secretary and the Secretary of
26 Health and Human Services, the Secretary of Defense, and the Secretary
27 of Agriculture shall, not later than 6 months after the date of the comple-
28 tion of the assessment in subsection (c)(1)(A), submit the updated national
29 biodefense implementation plan to the appropriate congressional committees.

30 **§ 10943. Biodefense analysis and budget submission**

31 (a) ANNUAL ANALYSIS.—For each fiscal year, beginning in fiscal year
32 2023, the Director of the Office of Management and Budget, in consultation
33 with the Secretary of Health and Human Services, shall—

34 (1) conduct a detailed and comprehensive analysis of Federal bio-
35 defense programs; and

36 (2) develop an integrated biodefense budget submission.

37 (b) DEVELOPMENT OF DEFINITION OF BIODEFENSE.—In accordance
38 with the national biodefense strategy, the Director of the Office of Manage-
39 ment and Budget shall develop and disseminate to all Federal departments
40 and agencies a unified definition of the term “biodefense” to identify which

1 programs and activities are included in the annual budget submission re-
2 quired under subsection (a).

3 (c) REQUIREMENTS FOR ANALYSIS.—The analysis required under sub-
4 section (a) shall include—

5 (1) the display of all funds requested for biodefense activities, both
6 mandatory and discretionary, by agency and categorized by biodefense
7 enterprise element, such as threat awareness, prevention, deterrence,
8 preparedness, surveillance and detection, response, attribution (includ-
9 ing bioforensic capabilities), recovery, and mitigation; and

10 (2) detailed explanations of how each program and activity included
11 aligns with biodefense goals and objectives as part of the national bio-
12 defense strategy required under section 10941 of this title.

13 (d) SUBMITTAL TO CONGRESS.—The Director of the Office of Manage-
14 ment and Budget, in consultation with the Secretary of Health and Human
15 Services, shall submit to Congress the analysis required under subsection
16 (a) for a fiscal year concurrently with the President’s annual budget request
17 for that fiscal year.

18 **Chapter 111—Border Security**

Subchapter I—Border Security Responsibilities and Functions

Sec.

11101. Secretary.

11102. Commissioner of U.S. Customs and Border Protection.

11103. Limitation on reorganization of functions and units.

11104. Employee discipline.

Subchapter II—Customs and Border Protection

Part A—In General

11111. Separate budget request for U.S. Customs and Border Protection.

11112. Allocation of resources by the Secretary.

11113. Polygraph and background examinations for law enforcement personnel of U.S. Customs and Border Protection.

11114. Fees authorized for Advanced Training Center.

11115. Border security metrics.

11116. Reports relating to border between United States and Mexico.

11117. Trusted traveler program.

11118. Asia-Pacific Economic Cooperation Business Travel Cards.

11119. Hiring members of the armed forces separating from military service.

11120. Protecting America’s food and agriculture.

11121. Large-scale non-intrusive inspection scanning plan.

Part B—Customs Functions

11131. Definition of customs revenue function.

11132. Retention of customs revenue functions by Secretary of the Treasury.

11133. Preservation of customs funds.

Part C—Drug Interdiction

11141. Methamphetamine and methamphetamine precursor chemicals.

11142. Protection against potential synthetic opioid exposure.

11143. Reports, evaluations, and research regarding drug interdiction at and between ports
of entry.

Subchapter III—Immigration Enforcement Functions

11151. Transfer of functions.

11152. Responsibilities of U.S. Immigration and Customs Enforcement officials.

11153. Professional responsibility and quality review.

11154. Annual report on cross-border tunnels.

11155. Illicit cross-border tunnel defense.

Subchapter IV—Citizenship and Immigration Services

- 11171. Transfer of functions to Director of U.S. Citizenship and Immigration Services.
- 11172. Responsibilities of U.S. Citizenship and Immigration Services officials.
- 11173. Citizenship and Immigration Services Ombudsman.
- 11174. Professional responsibility and quality review.
- 11175. Employee discipline.
- 11176. Transition.
- 11177. Application of Internet-based technologies.

Subchapter V—General Immigration Provisions

- 11191. Director of Shared Services.
- 11192. Separation of funding.
- 11193. Annual immigration functions report.

Subchapter VI—U.S. Customs and Border Protection Public-Private Partnerships

- 11201. Definitions.
- 11202. Fee agreements for certain services at ports of entry.
- 11203. Port of entry donation authority.
- 11204. Current and proposed agreements.

Subchapter VII—Miscellaneous Provisions

- 11211. Coordination of information and information technology.
- 11212. Visa issuance.
- 11213. Information on visa denials required to be entered into electronic data system.
- 11214. Purpose and responsibilities of Office of Cargo Security Policy.
- 11215. Purpose, composition, and operation of Border Enforcement Security Task Force.
- 11216. Cyber Crimes Center.
- 11217. Human trafficking.

1 **Subchapter I—Border Security**
 2 **Responsibilities and Functions**

3 **§ 11101. Secretary**

- 4 (a) IN GENERAL.—The Secretary is responsible for the following:
- 5 (1) Preventing the entry of terrorists and the instruments of terrorism into the United States.
- 6
- 7 (2) Securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States, including managing and coordinating those functions transferred to the Department at ports of entry.
- 8
- 9 (3) Carrying out the immigration enforcement functions vested by statute in, or performed by, the Commissioner of Immigration and Naturalization (or an officer, employee, or component of the Immigration and Naturalization Service) immediately before the date on which the transfer of functions specified under section 11151 of this title takes effect.
- 10
- 11 (4) Establishing and administering rules, under section 11212 of this title, governing the granting of visas or other forms of permission, including parole, to enter the United States to individuals who are not citizens or aliens lawfully admitted for permanent residence in the United States.
- 12
- 13 (5) Establishing national immigration enforcement policies and priorities.
- 14
- 15 (6) Except as provided in sections 11211 through 11215 of this title, administering the customs laws of the United States.
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25

1 (7) Conducting the inspection and related administrative functions of
2 the Department of Agriculture transferred to the Secretary under sub-
3 section (b)(2).

4 (8) In carrying out the foregoing responsibilities, ensuring the
5 speedy, orderly, and efficient flow of lawful traffic and commerce.

6 (b) FUNCTIONS TRANSFERRED.—

7 (1) IN GENERAL.—The Secretary succeeds to the functions, per-
8 sonnel, assets, and liabilities of—

9 (A) the United States Customs Service of the Department of
10 the Treasury, including the functions of the Secretary of the
11 Treasury relating thereto;

12 (B) the Transportation Security Administration of the Depart-
13 ment of Transportation, including the functions of the Secretary
14 of Transportation, and of the Under Secretary of Transportation
15 for Security, relating thereto;

16 (C) the Federal Protective Service of the General Services Ad-
17 ministration, including the functions of the Administrator of Gen-
18 eral Services relating thereto;

19 (D) the Federal Law Enforcement Training Center of the De-
20 partment of the Treasury; and

21 (E) the Office for Domestic Preparedness of the Office of Jus-
22 tice Programs, including the functions of the Attorney General re-
23 lating thereto.

24 (2) CERTAIN AGRICULTURAL INSPECTION FUNCTIONS OF THE DE-
25 PARTMENT OF AGRICULTURE.—

26 (A) EXCLUSION OF QUARANTINE ACTIVITIES.—In this section,
27 the term “functions” does not include quarantine activities carried
28 out under the laws specified in subparagraph (B).

29 (B) TRANSFER OF AGRICULTURAL IMPORT AND ENTRY IN-
30 SPECTION FUNCTIONS.—The Secretary succeeds to the functions
31 of the Secretary of Agriculture relating to agricultural import and
32 entry inspection activities under the following laws:

33 (i) Section 1 of the Act of August 31, 1922 (known as the
34 Honeybee Act) (7 U.S.C. 281).

35 (ii) Title III of the Federal Seed Act (7 U.S.C. 1581 et
36 seq.).

37 (iii) The Plant Protection Act (7 U.S.C. 7701 et seq.).

38 (iv) The Animal Health Protection Act (7 U.S.C. 8301 et
39 seq.).

40 (v) Section 11 of the Endangered Species Act of 1973 (16
41 U.S.C. 1540).

1 (vi) The Lacey Act Amendments of 1981 (16 U.S.C. 3371
2 et seq.).

3 (vii) The 8th paragraph under the heading “Bureau of Ani-
4 mal Industry” in the Act of March 4, 1913 (known as the
5 Virus-Serum-Toxin Act) (21 U.S.C. 151 et seq.).

6 (C) EFFECT OF TRANSFER.—

7 (i) COMPLIANCE WITH DEPARTMENT OF AGRICULTURE
8 REGULATIONS.—The authority transferred under subpara-
9 graph (B) shall be exercised by the Secretary in accordance
10 with the regulations, policies, and procedures issued by the
11 Secretary of Agriculture regarding the administration of the
12 laws specified in subparagraph (B).

13 (ii) RULEMAKING COORDINATION.—The Secretary of Agri-
14 culture shall coordinate with the Secretary when the Sec-
15 retary of Agriculture prescribes regulations, policies, or proce-
16 dures for administering the functions transferred under sub-
17 paragraph (B) under a law specified in subparagraph (B).

18 (iii) EFFECTIVE ADMINISTRATION.—The Secretary, in con-
19 sultation with the Secretary of Agriculture, may issue direc-
20 tives and guidelines necessary to ensure the effective use of
21 personnel of the Department to carry out the functions trans-
22 ferred under subparagraph (B).

23 (D) PERIODIC TRANSFER OF FUNDS TO DEPARTMENT.—Out of
24 funds collected by fees authorized under sections 2508 and 2509
25 of the Food, Agriculture, Conservation, and Trade Act of 1990
26 (21 U.S.C. 136, 136a), the Secretary of Agriculture shall transfer,
27 from time to time to the Secretary, funds for activities carried out
28 by the Secretary for which fees were collected. The proportion of
29 fees collected that are transferred to the Secretary under this sub-
30 paragraph may not exceed the proportion of costs incurred by the
31 Secretary to all costs incurred to carry out activities funded by the
32 fees.

33 **§ 11102. Commissioner of U.S. Customs and Border Protec-**
34 **tion**

35 (a) DEFINITIONS.—In this section, the terms “commercial operations”,
36 “customs and trade laws of the United States”, “trade enforcement”, and
37 “trade facilitation” have the meanings given the terms in section 2 of the
38 Trade Facilitation and Trade Enforcement Act of 2015 (19 U.S.C. 4301).

39 (b) IN GENERAL.—The Commissioner of U.S. Customs and Border Pro-
40 tection (in this section referred to as the “Commissioner”) shall—

- 1 (1) coordinate and integrate the security, trade facilitation, and
2 trade enforcement functions of U.S. Customs and Border Protection;
- 3 (2) ensure the interdiction of individuals and goods illegally entering
4 or exiting the United States;
- 5 (3) facilitate and expedite the flow of legitimate travelers and trade;
- 6 (4) direct and administer the commercial operations of U.S. Customs
7 and Border Protection and the enforcement of the customs and trade
8 laws of the United States;
- 9 (5) detect, respond to, and interdict terrorists, drug smugglers and
10 traffickers, human smugglers and traffickers, and other individuals who
11 may undermine the security of the United States, in cases in which the
12 individuals are entering, or have recently entered, the United States;
- 13 (6) safeguard the borders of the United States to protect against the
14 entry of dangerous goods;
- 15 (7) ensure the overall economic security of the United States is not
16 diminished by efforts, activities, and programs aimed at securing the
17 homeland;
- 18 (8) in coordination with U.S. Immigration and Customs Enforcement
19 and United States Citizenship and Immigration Services, enforce and
20 administer all immigration laws, as the term is defined in section
21 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)), in-
22 cluding—
 - 23 (A) the inspection, processing, and admission of individuals who
24 seek to enter or depart the United States; and
 - 25 (B) the detection, interdiction, removal, departure from the
26 United States, short-term detention, and transfer of individuals
27 unlawfully entering, or who have recently unlawfully entered, the
28 United States;
- 29 (9) develop and implement screening and targeting capabilities, in-
30 cluding the screening, reviewing, identifying, and prioritizing of pas-
31 sengers and cargo across all international modes of transportation,
32 both inbound and outbound;
- 33 (10) in coordination with the Secretary, deploy technology to collect
34 the data necessary for the Secretary to administer the biometric entry
35 and exit data system pursuant to section 7208 of the Intelligence Re-
36 form and Terrorism Prevention Act of 2004 (8 U.S.C. 1365b);
- 37 (11) enforce and administer the laws relating to agricultural import
38 and entry inspection referred to in section 11101(b)(2) of this title;
- 39 (12) in coordination with the Under Secretary for Management of
40 the Department, ensure U.S. Customs and Border Protection complies
41 with Federal law, the Federal Acquisition Regulation, and the Depart-

1 ment's acquisition management directives for major acquisition pro-
2 grams of U.S. Customs and Border Protection;

3 (13) ensure that the policies and regulations of U.S. Customs and
4 Border Protection are consistent with the obligations of the United
5 States pursuant to international agreements;

6 (14) enforce and administer—

7 (A) the Container Security Initiative program under section
8 30505 of this title; and

9 (B) the Customs-Trade Partnership Against Terrorism program
10 under subchapter II of chapter 305 of this title;

11 (15) conduct polygraph examinations in accordance with section
12 11113(a)(1) of this title;

13 (16) establish the standard operating procedures described in sub-
14 section (c);

15 (17) carry out the training required under subsection (d);

16 (18) carry out section 11118 of this title relating to the issuance of
17 Asia-Pacific Economic Cooperation Business Travel Cards; and

18 (19) carry out other duties and powers prescribed by law or dele-
19 gated by the Secretary.

20 (c) STANDARD OPERATING PROCEDURES.—

21 (1) IN GENERAL.—The Commissioner shall establish—

22 (A) standard operating procedures for searching, reviewing, re-
23 taining, and sharing information contained in communication,
24 electronic, or digital devices encountered by U.S. Customs and
25 Border Protection personnel at United States ports of entry;

26 (B) standard use of force procedures that officers and agents
27 of U.S. Customs and Border Protection may employ in the execu-
28 tion of their duties, including the use of deadly force;

29 (C) a uniform, standardized, and publicly available procedure
30 for processing and investigating complaints against officers,
31 agents, and employees of U.S. Customs and Border Protection for
32 violations of professional conduct, including the timely disposition
33 of complaints and a written notification to the complainant of the
34 status or outcome, as appropriate, of the related investigation, in
35 accordance with section 552a of title 5 (known as the Privacy Act
36 of 1974);

37 (D) an internal, uniform reporting mechanism regarding inci-
38 dents involving the use of deadly force by an officer or agent of
39 U.S. Customs and Border Protection, including an evaluation of
40 the degree to which the procedures required under subparagraph
41 (B) were followed; and

1 (E) standard operating procedures, acting through the Assistant
2 Commissioner for Air and Marine Operations and in coordination
3 with the Office for Civil Rights and Civil Liberties and the Office
4 of Privacy of the Department, to provide command, control, com-
5 munication, surveillance, and reconnaissance assistance through
6 the use of unmanned aerial systems, including the establishment
7 of—

8 (i) a process for other Federal, State, and local law en-
9 forcement agencies to submit mission requests;

10 (ii) a formal procedure to determine whether to approve or
11 deny a mission request;

12 (iii) a formal procedure to determine how mission requests
13 are prioritized and coordinated; and

14 (iv) a process regarding the protection and privacy of data
15 and images collected by U.S. Customs and Border Protection
16 through the use of unmanned aerial systems.

17 (2) REQUIREMENTS REGARDING CERTAIN NOTIFICATIONS.—The
18 standard operating procedures established pursuant to paragraph
19 (1)(A) shall require—

20 (A) in the case of a search of information conducted on an elec-
21 tronic device by U.S. Customs and Border Protection personnel,
22 the Commissioner to notify the individual subject to the search of
23 the purpose and authority for the search and how the individual
24 may obtain information on reporting concerns about the search;
25 and

26 (B) in the case of information collected by U.S. Customs and
27 Border Protection through a search of an electronic device, if the
28 information is transmitted to another Federal agency for subject
29 matter assistance, translation, or decryption, the Commissioner to
30 notify the individual subject to the search of the transmission.

31 (3) EXCEPTIONS.—The Commissioner may withhold the notifications
32 required under paragraphs (1)(C) and (2) if the Commissioner deter-
33 mines, in the sole and unreviewable discretion of the Commissioner,
34 that the notifications would impair national security, law enforcement,
35 or other operational interests.

36 (4) UPDATE AND REVIEW.—The Commissioner shall review and up-
37 date every 3 years the standard operating procedures required under
38 this subsection.

39 (5) AUDITS.—The Inspector General of the Department shall de-
40 velop and annually administer, during 2017, 2018, and 2019, an audit-
41 ing mechanism to review whether searches of electronic devices at or

1 between United States ports of entry are being conducted in conformity
2 with the standard operating procedures required under paragraph
3 (1)(A). Audits shall be submitted to the Committee on Homeland Security
4 of the House of Representatives and the Committee on Homeland
5 Security and Governmental Affairs of the Senate and shall include the
6 following:

7 (A) A description of the activities of officers and agents of U.S.
8 Customs and Border Protection with respect to the searches.

9 (B) The number of searches.

10 (C) The number of instances in which information contained in
11 devices that were subjected to searches was retained, copied,
12 shared, or entered in an electronic database.

13 (D) The number of devices detained as the result of searches.

14 (E) The number of instances in which information collected
15 from a device that was subjected to searches was transmitted to
16 another Federal agency, including whether the transmission re-
17 sulted in a prosecution or conviction.

18 (6) REQUIREMENTS REGARDING OTHER NOTIFICATIONS.—The
19 standard operating procedures established pursuant to paragraph
20 (1)(B) shall require—

21 (A) in the case of an incident of the use of deadly force by U.S.
22 Customs and Border Protection personnel, the Commissioner to
23 notify the Committee on Homeland Security of the House of Rep-
24 resentatives and the Committee on Homeland Security and Gov-
25 ernmental Affairs of the Senate; and

26 (B) the Commissioner to provide to those committees a copy of
27 the evaluation pursuant to paragraph (1)(D) not later than 30
28 days after completion of the evaluation.

29 (7) REPORT ON UNMANNED AERIAL SYSTEMS.—The Commissioner
30 shall submit to the Committee on Homeland Security of the House of
31 Representatives and the Committee on Homeland Security and Govern-
32 mental Affairs of the Senate, during 2017, 2018, and 2019, an annual
33 report that reviews whether the use of unmanned aerial systems is
34 being conducted in conformity with the standard operating procedures
35 required under paragraph (1)(E). The report—

36 (A) shall be submitted with the President's annual budget;

37 (B) may be submitted in classified form if the Commissioner de-
38 termines that it is appropriate; and

39 (C) shall include—

40 (i) a detailed description of how, where, and for how long
41 data and images collected through the use of unmanned aerial

1 systems by U.S. Customs and Border Protection are collected
2 and stored; and

3 (ii) a list of Federal, State, and local law enforcement
4 agencies that submitted mission requests in the previous year
5 and the disposition of the requests.

6 (d) TRAINING.—The Commissioner shall require all officers and agents
7 of U.S. Customs and Border Protection to participate in a specified amount
8 of continuing education (to be determined by the Commissioner) to maintain
9 an understanding of Federal legal rulings, court decisions, and departmental
10 policies, procedures, and guidelines.

11 (e) SHORT-TERM DETENTION STANDARDS.—

12 (1) DEFINITION OF SHORT-TERM DETENTION.—In this subsection,
13 the term “short-term detention” means detention in a U.S. Customs
14 and Border Protection processing center for 72 hours or less, before
15 repatriation to a country of nationality or last habitual residence.

16 (2) ACCESS TO FOOD AND WATER.—The Commissioner shall make
17 every effort to ensure that adequate access to food and water is pro-
18 vided to an individual apprehended and detained at or between a
19 United States port of entry as soon as practicable following the time
20 of the apprehension or during subsequent short-term detention.

21 (3) ACCESS TO INFORMATION ON DETAINEE RIGHTS AT BORDER PA-
22 TROL PROCESSING CENTERS.—

23 (A) IN GENERAL.—The Commissioner shall ensure that an indi-
24 vidual apprehended by a U.S. Border Patrol agent or an Office
25 of Field Operations officer is provided with information concerning
26 the individual’s rights, including the right to contact a representa-
27 tive of the individual’s government for purposes of United States
28 treaty obligations.

29 (B) HOW INFORMATION IS TO BE PROVIDED.—The information
30 referred to in subparagraph (A) may be provided either orally or
31 in writing and shall be posted in the detention holding cell in
32 which the individual is being held. The information shall be pro-
33 vided in a language understandable to the individual.

34 (4) DAYTIME REPATRIATION.—When practicable, repatriations shall
35 be limited to daylight hours and avoid locations that are determined
36 to have high indices of crime and violence.

37 (5) REPORT ON PROCUREMENT PROCESS AND STANDARDS.—Not
38 later than 180 days after February 24, 2016, the Comptroller General
39 shall submit to the Committee on Homeland Security of the House of
40 Representatives and the Committee on Homeland Security and Govern-
41 mental Affairs of the Senate a report on the procurement process and

1 standards of entities with which U.S. Customs and Border Protection
2 has contracts for the transportation and detention of individuals apprehended by agents or officers of U.S. Customs and Border Protection.
3 The report should also consider the operational efficiency of contracting
4 the transportation and detention of those individuals.
5

6 (6) REPORT ON INSPECTIONS OF SHORT-TERM CUSTODY FACILITIES.—The Commissioner shall—
7

8 (A) annually inspect all facilities utilized for short-term detention; and
9

10 (B) make publicly available information collected pursuant to the inspections, including information regarding the requirements under paragraphs (2) and (3), and, where appropriate, issue recommendations to improve the conditions of the facilities.
11
12
13

14 (f) WAIT TIMES TRANSPARENCY.—

15 (1) IN GENERAL.—The Commissioner shall—

16 (A) publish live wait times at the 20 United States airports that support the highest volume of international travel (as determined by available Federal flight data);
17
18

19 (B) make information about the wait times available to the public in real time through the U.S. Customs and Border Protection website;
20
21

22 (C) submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, during 2017, 2018, 2019, 2020, and 2021, a report that includes compilations of all those wait times and a ranking of those United States airports by wait times; and
23
24
25
26
27

28 (D) provide adequate staffing at the U.S. Customs and Border Protection information center to ensure timely access for travelers attempting to submit comments or speak with a representative about their entry experiences.
29
30
31

32 (2) CALCULATION.—The wait times referred to in paragraph (1)(A) shall be determined by calculating the time elapsed between an individual's entry into the U.S. Customs and Border Protection inspection area and the individual's clearance by a U.S. Customs and Border Protection officer.
33
34
35
36

37 (g) CONTINUED SUBMISSION OF REPORTS TO COMMITTEES.—The Commissioner shall continue to submit to the Committee on Homeland Security and the Committee on Ways and Means of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and
38
39
40

1 the Committee on Finance of the Senate any report required to be sub-
2 mitted on February 23, 2016, under any provision of law.

3 (h) AUTHORITY OF OTHER FEDERAL AGENCIES NOT AFFECTED.—Noth-
4 ing in this section may be construed as affecting in any manner the author-
5 ity, which existed on February 23, 2016, of any other Federal agency or
6 component of the Department.

7 **§ 11103. Limitation on reorganization of functions and units**

8 The authority provided by section 1502 of the Homeland Security Act of
9 2002 (Public Law 107–296, 116 Stat. 2308) may be used to reorganize
10 functions or organizational units in U.S. Immigration and Customs Enforce-
11 ment or U. S. Citizenship and Immigration Services, but may not be used
12 to recombine U.S. Immigration and Customs Enforcement and U.S. Citizen-
13 ship and Immigration Services into a single agency or otherwise to combine,
14 join, or consolidate functions or organizational units of U.S. Immigration
15 and Customs Enforcement and U.S. Citizenship and Immigration Services
16 with each other.

17 **§ 11104. Employee discipline**

18 Notwithstanding another law, the Secretary may impose disciplinary ac-
19 tion on an employee of U.S. Immigration and Customs Enforcement and
20 U.S. Customs and Border Protection who willfully deceives Congress or
21 agency leadership on any matter.

22 **Subchapter II—Customs and Border**
23 **Protection**
24 **Part A—In General**

25 **§ 11111. Separate budget request for U.S. Customs and Bor-**
26 **der Protection**

27 (a) IN GENERAL.—The President shall include in each budget trans-
28 mitted to Congress under section 1105 of title 31 a separate budget request
29 for U.S. Customs and Border Protection.

30 (b) FIVE-YEAR PLAN FOR LAND BORDER PORT OF ENTRY PROJECTS.—
31 The annual budget submission of U. S. Customs and Border Protection for
32 “Construction and Facilities Management” shall, in consultation with the
33 General Services Administration, include a detailed 5-year plan for all Fed-
34 eral land border port-of-entry projects, with a yearly update of total pro-
35 jected future funding needs delineated by Federal land border port of entry.

36 **§ 11112. Allocation of resources by the Secretary**

37 (a) DEFINITION OF CUSTOMS REVENUE SERVICES.—In this section, the
38 term “customs revenue services” means those customs revenue functions de-
39 scribed in section 11131(1) through (6) and (8) of this title.

1 (b) IN GENERAL.—The Secretary shall ensure that adequate staffing is
2 provided to ensure that levels of customs revenue services provided on Janu-
3 ary 23, 2003, shall continue to be provided.

4 (c) NOTIFICATION OF CONGRESS.—The Secretary shall notify the Com-
5 mittee on Ways and Means of the House of Representatives and the Com-
6 mittee on Finance of the Senate at least 90 days prior to taking an action
7 that would—

8 (1) result in a significant reduction in customs revenue services, in-
9 cluding hours of operation, provided at an office within the Department
10 or a port of entry;

11 (2) eliminate or relocate an office of the Department that provides
12 customs revenue services; or

13 (3) eliminate a port of entry.

14 **§ 11113. Polygraph and background examinations for law**
15 **enforcement personnel of U.S. Customs and Bor-**
16 **der Protection**

17 (a) IN GENERAL.—The Secretary shall ensure that—

18 (1) all applicants for law enforcement positions with U.S. Customs
19 and Border Protection (except as provided in subsection (b)) receive
20 polygraph examinations before being hired for a position; and

21 (2) U.S. Customs and Border Protection initiates all periodic back-
22 ground reinvestigations for all law enforcement personnel of U.S. Cus-
23 toms and Border Protection who should receive periodic background re-
24 investigations pursuant to relevant policies of U.S. Customs and Bor-
25 der Protection in effect on January 3, 2011.

26 (b) WAIVER.—The Commissioner of U.S. Customs and Border Protection
27 may waive the polygraph examination requirement under subsection (a)(1)
28 for any applicant who—

29 (1) is considered suitable for employment;

30 (2) holds a current, active Top Secret/Sensitive Compartmented In-
31 formation Clearance;

32 (3) has a current Single Scope Background Investigation;

33 (4) was not granted any waivers to obtain his or her clearance; and

34 (5) is a veteran (as defined in section 2108 of title 5).

35 **§ 11114. Fees authorized for Advanced Training Center**

36 U.S. Customs and Border Protection's Advanced Training Center may
37 charge fees for a service and/or thing of value it provides to Federal Govern-
38 ment or non-government entities or individuals, so long as the fees charged
39 do not exceed the full costs associated with the service or thing of value pro-
40 vided. Notwithstanding 31 U.S.C. 3302(b), fees collected by the Advanced
41 Training Center—

1 (1) shall be deposited in a separate account entitled “Advanced
2 Training Center Revolving Fund”;

3 (2) shall be available, without further appropriations, for necessary
4 expenses of the Advanced Training Center program; and

5 (3) shall remain available until expended.

6 **§ 11115. Border security metrics**

7 (a) DEFINITIONS.—In this section:

8 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
9 priate congressional committees” means—

10 (A) the Committee on Homeland Security and Governmental
11 Affairs of the Senate; and

12 (B) the Committee on Homeland Security of the House of Rep-
13 resentatives.

14 (2) CONSEQUENCE DELIVERY SYSTEM.—The term “Consequence De-
15 livery System” means the series of consequences applied by the U.S.
16 Border Patrol in collaboration with other Federal agencies to individ-
17 uals unlawfully entering the United States, to prevent unlawful border
18 crossing recidivism.

19 (3) GOT AWAY.—The term “got away” means an unlawful border
20 crosser who—

21 (A) is directly or indirectly observed making an unlawful entry
22 into the United States;

23 (B) is not apprehended; and

24 (C) is not a turn back.

25 (4) KNOWN MARITIME MIGRANT FLOW.—The term “known maritime
26 migrant flow” means the sum of the number of undocumented mi-
27 grants—

28 (A) interdicted in the waters over which the United States has
29 jurisdiction;

30 (B) identified at sea either directly or indirectly, but not inter-
31 dicted; or

32 (C) if not described in subparagraph (A) or (B), who were oth-
33 erwise reported, with a significant degree of certainty, as having
34 entered, or attempted to enter, the United States through the
35 maritime border.

36 (5) MAJOR VIOLATOR.—The term “major violator” means a person
37 or entity that has engaged in serious criminal activities at any land,
38 air, or sea port of entry, including the following:

39 (A) Possession of illicit drugs.

40 (B) Smuggling of prohibited products.

41 (C) Human smuggling.

1 (D) Possession of illegal weapons.

2 (E) Use of fraudulent documents.

3 (F) Any other offense that is serious enough to result in an ar-
4 rest.

5 (6) SITUATIONAL AWARENESS.—The term “situational awareness”
6 means knowledge and understanding of current unlawful cross-border
7 activity, including the following:

8 (A) Threats and trends concerning illicit trafficking and unlaw-
9 ful crossings.

10 (B) The ability to forecast future shifts in those threats and
11 trends.

12 (C) The ability to evaluate those threats and trends at a level
13 sufficient to create actionable plans.

14 (D) The operational capability to conduct persistent and inte-
15 grated surveillance of the international borders of the United
16 States.

17 (7) TRANSIT ZONE.—The term “transit zone” means the sea cor-
18 ridors of the western Atlantic Ocean, the Gulf of Mexico, the Caribbean
19 Sea, and the eastern Pacific Ocean through which undocumented mi-
20 grants and illicit drugs transit, either directly or indirectly, to the
21 United States.

22 (8) TURN BACK.—The term “turn back” means an unlawful border
23 crosser who, after making an unlawful entry into the United States,
24 responds to United States enforcement efforts by returning promptly
25 to the country from which the crosser entered.

26 (9) UNLAWFUL BORDER CROSSING EFFECTIVENESS RATE.—The
27 term “unlawful border crossing effectiveness rate” means the percent-
28 age that results from dividing the number of apprehensions and turn
29 backs by the sum of the number of apprehensions, estimated unde-
30 tected unlawful entries, turn backs, and got aways.

31 (10) UNLAWFUL ENTRY.—The term “unlawful entry” means an un-
32 lawful border crosser who enters the United States and is not appre-
33 hended by a border security component of the Department.

34 (b) METRICS FOR SECURING THE BORDER BETWEEN PORTS OF
35 ENTRY.—

36 (1) IN GENERAL.—Not later than 180 days after December 23,
37 2016, the Secretary shall develop metrics, informed by situational
38 awareness, to measure the effectiveness of security between ports of
39 entry. The Secretary shall annually implement the metrics developed
40 under this subsection, which shall include the following:

1 (A) Estimates, using alternative methodologies where appro-
2 priate, including recidivism data, survey data, known-flow data,
3 and technologically measured data, of the following:

4 (i) The rate of apprehension of attempted unlawful border
5 crossers.

6 (ii) The number of detected unlawful entries.

7 (iii) The number of estimated undetected unlawful entries.

8 (iv) Turn backs.

9 (v) Got aways.

10 (B) A measurement of situational awareness achieved in each
11 U.S. Border Patrol sector.

12 (C) An unlawful border crossing effectiveness rate in each U.S.
13 Border Patrol sector.

14 (D) A probability of detection rate, which compares the esti-
15 mated total unlawful border crossing attempts not detected by
16 U.S. Border Patrol to the unlawful border crossing effectiveness
17 rate under subparagraph (C), as informed by subparagraph (A).

18 (E) The number of apprehensions in each U.S. Border Patrol
19 sector.

20 (F) The number of apprehensions of unaccompanied alien chil-
21 dren, and the nationality of the children, in each U.S. Border Pa-
22 trol sector.

23 (G) The number of apprehensions of family units, and the na-
24 tionality of the family units, in each U.S. Border Patrol sector.

25 (H) An illicit drugs seizure rate for drugs seized by the U.S.
26 Border Patrol between ports of entry, which compares the ratio
27 of the amount and type of illicit drugs seized between ports of
28 entry in any fiscal year to the average of the amount and type of
29 illicit drugs seized between ports of entry in the immediately pre-
30 ceding 5 fiscal years.

31 (I) Estimates of the impact of the Consequence Delivery System
32 on the rate of recidivism of unlawful border crossers over multiple
33 fiscal years.

34 (J) An examination of each consequence under the Consequence
35 Delivery System referred to in subparagraph (I), including the fol-
36 lowing:

37 (i) Voluntary return.

38 (ii) Warrant of arrest or notice to appear.

39 (iii) Expedited removal.

40 (iv) Reinstatement of removal.

41 (v) Alien transfer exit program.

- 1 (vi) Criminal consequence program.
2 (vii) Standard prosecution.
3 (viii) Operation Against Smugglers Initiative on Safety and
4 Security.

5 (2) METRICS CONSULTATION.—To ensure that authoritative data
6 sources are utilized in the development of the metrics described in
7 paragraph (1), the Secretary shall—

8 (A) consult with the heads of the appropriate components of the
9 Department; and

10 (B) where appropriate, consult with the heads of other agencies,
11 including the Office of Refugee Resettlement of the Department
12 of Health and Human Services and the Executive Office for Immi-
13 gration Review of the Department of Justice.

14 (3) MANNER OF COLLECTION.—The data collected to inform the
15 metrics developed in accordance with paragraph (1) shall be collected
16 and reported in a consistent and standardized manner across all U.S.
17 Border Patrol sectors, informed by situational awareness.

18 (c) METRICS FOR SECURING THE BORDER AT PORTS OF ENTRY.—

19 (1) IN GENERAL.—Not later than 180 days after December 23,
20 2016, the Secretary shall develop metrics, informed by situational
21 awareness, to measure the effectiveness of security at ports of entry.
22 The Secretary shall annually implement the metrics developed under
23 this subsection, which shall include the following:

24 (A) Estimates, using alternative methodologies where appro-
25 priate, including recidivism data, survey data, and randomized sec-
26 ondary screening data, of the following:

27 (i) Total inadmissible travelers who attempt to enter or
28 successfully enter the United States at a port of entry.

29 (ii) The rate of refusals and interdictions for travelers who
30 attempt to enter or successfully enter the United States at a
31 port of entry.

32 (iii) The number of unlawful entries at a port of entry.

33 (B) The amount and type of illicit drugs seized by the Office
34 of Field Operations of U.S. Customs and Border Protection at
35 ports of entry during the previous fiscal year.

36 (C) An illicit drugs seizure rate for drugs seized by the Office
37 of Field Operations, which compares the ratio of the amount and
38 type of illicit drugs seized by the Office of Field Operations in any
39 fiscal year to the average of the amount and type of illicit drugs
40 seized by the Office of Field Operations in the immediately pre-
41 ceding 5 fiscal years.

1 (D) The number of infractions related to travelers and cargo
2 committed by major violators who are interdicted by the Office of
3 Field Operations at ports of entry, and the estimated number of
4 those infractions committed by major violators who are not so
5 interdicted.

6 (E) In consultation with the heads of the Office of National
7 Drug Control Policy and the United States Southern Command,
8 a cocaine seizure effectiveness rate, which is the percentage result-
9 ing from dividing the amount of cocaine seized by the Office of
10 Field Operations by the total estimated cocaine flow rate at ports
11 of entry along the United States land border with Mexico and
12 Canada.

13 (F) A measurement of how border security operations affect
14 crossing times, including the following:

15 (i) A wait time ratio that compares the average wait times
16 to total commercial and private vehicular traffic volumes at
17 each land port of entry.

18 (ii) An infrastructure capacity utilization rate that meas-
19 ures traffic volume against the physical and staffing capacity
20 at each land port of entry.

21 (iii) A secondary examination rate that measures the fre-
22 quency of secondary examinations at each land port of entry.

23 (iv) An enforcement rate that measures the effectiveness of
24 the secondary examinations at detecting major violators.

25 (G) A seaport scanning rate that includes the following:

26 (i) The number of all cargo containers that are considered
27 potentially high-risk, as determined by the Executive Assist-
28 ant Commissioner of the Office of Field Operations.

29 (ii) A comparison of the number of potentially high-risk
30 cargo containers scanned by the Office of Field Operations at
31 each sea port of entry during a fiscal year to the total num-
32 ber of high-risk cargo containers entering the United States
33 at each such sea port of entry during the previous fiscal year.

34 (iii) The number of potentially high-risk cargo containers
35 scanned on arrival at a United States sea port of entry.

36 (iv) The number of potentially high-risk cargo containers
37 scanned before arrival at a United States sea port of entry.

38 (2) METRICS CONSULTATION.—To ensure that authoritative data
39 sources are utilized in the development of the metrics described in
40 paragraph (1), the Secretary shall—

1 (A) consult with the heads of the appropriate components of the
2 Department; and

3 (B) where appropriate, work with heads of other appropriate
4 agencies, including the Office of Refugee Resettlement of the De-
5 partment of Health and Human Services and the Executive Office
6 for Immigration Review of the Department of Justice.

7 (3) MANNER OF COLLECTION.—The data collected to inform the
8 metrics developed in accordance with paragraph (1) shall be collected
9 and reported in a consistent and standardized manner across all United
10 States ports of entry, informed by situational awareness.

11 (d) METRICS FOR SECURING THE MARITIME BORDER.—

12 (1) IN GENERAL.—Not later than 180 days after December 23,
13 2016, the Secretary shall develop metrics, informed by situational
14 awareness, to measure the effectiveness of security in the maritime en-
15 vironment. The Secretary shall annually implement the metrics devel-
16 oped under this subsection, which shall include the following:

17 (A) Situational awareness achieved in the maritime environ-
18 ment.

19 (B) A known maritime migrant flow rate.

20 (C) An illicit drugs removal rate for drugs removed inside and
21 outside of a transit zone, which compares the amount and type of
22 illicit drugs removed, including drugs abandoned at sea, by the
23 maritime security components of the Department of Homeland Se-
24 curity in any fiscal year to the average of the amount and type
25 of illicit drugs removed by the maritime components for the imme-
26 diately preceding 5 fiscal years.

27 (D) In consultation with the heads of the Office of National
28 Drug Control Policy and the United States Southern Command,
29 a cocaine removal effectiveness rate for cocaine removed inside a
30 transit zone and outside a transit zone, which compares the
31 amount of cocaine removed by the maritime security components
32 of the Department of Homeland Security to the total documented
33 cocaine flow rate, as contained in Federal drug databases.

34 (E) A response rate, which compares the ability of the maritime
35 security components of the Department of Homeland Security to
36 respond to and resolve known maritime threats, whether inside or
37 outside a transit zone, by placing assets on-scene, to the total
38 number of events with respect to which the Department has
39 known threat information.

40 (F) An intergovernmental response rate, which compares the
41 ability of the maritime security components of the Department or

1 other United States Government entities to respond to and resolve
2 actionable maritime threats, whether inside or outside a transit
3 zone, with the number of those threats detected.

4 (2) METRICS CONSULTATION.—To ensure that authoritative data
5 sources are utilized in the development of the metrics described in
6 paragraph (1), the Secretary shall—

7 (A) consult with the heads of the appropriate components of the
8 Department; and

9 (B) where appropriate, work with the heads of other agencies,
10 including the Drug Enforcement Agency, the Department of De-
11 fense, and the Department of Justice.

12 (3) METHODS OF COLLECTION.—The data used by the Secretary
13 shall be collected and reported in a consistent and standardized manner
14 by the maritime security components of the Department, informed by
15 situational awareness.

16 (e) AIR AND MARINE SECURITY METRICS IN THE LAND DOMAIN.—

17 (1) IN GENERAL.—Not later than 180 days after December 23,
18 2016, the Secretary shall develop metrics, informed by situational
19 awareness, to measure the effectiveness of the aviation assets and oper-
20 ations of Air and Marine Operations of U.S. Customs and Border Pro-
21 tection. The Secretary shall annually implement the metrics developed
22 under this subsection, which shall include the following:

23 (A) A flight hour effectiveness rate, which compares Air and
24 Marine Operations flight hours requirements to the number of
25 flight hours flown by Air and Marine Operations.

26 (B) A funded flight hour effectiveness rate, which compares the
27 number of funded flight hours appropriated to Air and Marine Op-
28 erations to the number of actual flight hours flown by Air and Ma-
29 rine Operations.

30 (C) A readiness rate, which compares the number of aviation
31 missions flown by Air and Marine Operations to the number of
32 aviation missions cancelled by Air and Marine Operations due to
33 maintenance, operations, or other causes.

34 (D) The number of missions cancelled by Air and Marine Oper-
35 ations due to weather compared to the total planned missions.

36 (E) The number of individuals detected by Air and Marine Op-
37 erations through the use of unmanned aerial systems and manned
38 aircraft.

39 (F) The number of apprehensions assisted by Air and Marine
40 Operations through the use of unmanned aerial systems and
41 manned aircraft.

1 (G) The number and quantity of illicit drug seizures assisted by
2 Air and Marine Operations through the use of unmanned aerial
3 systems and manned aircraft.

4 (H) The number of times that actionable intelligence related to
5 border security was obtained through the use of unmanned aerial
6 systems and manned aircraft.

7 (2) METRICS CONSULTATION.—To ensure that authoritative data
8 sources are utilized in the development of the metrics described in
9 paragraph (1), the Secretary shall—

10 (A) consult with the heads of the appropriate components of the
11 Department; and

12 (B) as appropriate, work with the heads of other departments
13 and agencies, including the Department of Justice.

14 (3) MANNER OF COLLECTION.—The data collected to inform the
15 metrics developed in accordance with paragraph (1) shall be collected
16 and reported in a consistent and standardized manner by Air and Ma-
17 rine Operations, informed by situational awareness.

18 (f) DATA TRANSPARENCY.—The Secretary shall—

19 (1) in accordance with applicable privacy laws, make data relating
20 to apprehensions, inadmissible aliens, drug seizures, and other enforce-
21 ment actions available to the public, law enforcement communities, and
22 academic research communities; and

23 (2) provide the Office of Immigration Statistics of the Department
24 with unfettered access to the data referred to in paragraph (1).

25 (g) EVALUATIONS BY GOVERNMENT ACCOUNTABILITY OFFICE AND SEC-
26 RETARY.—

27 (1) METRIC REPORT.—

28 (A) MANDATORY DISCLOSURES.—The Secretary shall submit to
29 the appropriate congressional committees and the Comptroller
30 General an annual report containing the metrics required under
31 this section and the data and methodology used to develop the
32 metrics.

33 (B) PERMISSIBLE DISCLOSURES.—The Secretary, for the pur-
34 pose of validation and verification, may submit the annual report
35 described in subparagraph (A) to—

36 (i) the Center for Borders, Trade, and Immigration Re-
37 search of the Centers of Excellence network of the Depart-
38 ment;

39 (ii) the head of a national laboratory in the Department
40 laboratory network with prior expertise in border security;
41 and

- 1 (iii) a federally funded research and development center.
- 2 (2) GOVERNMENT ACCOUNTABILITY OFFICE REPORT.—Not later
3 than 270 days after receiving the first report under paragraph (1)(A)
4 and biennially thereafter for the following 10 years with respect to
5 every other report, the Comptroller General shall submit to the appro-
6 priate congressional committees a report that—
- 7 (A) analyzes the suitability and statistical validity of the data
8 and methodology contained in each report; and
- 9 (B) includes recommendations on—
- 10 (i) the feasibility of other suitable metrics that may be used
11 to measure the effectiveness of border security; and
- 12 (ii) improvements that need to be made to the metrics
13 being used to measure the effectiveness of border security.
- 14 (3) STATE OF THE BORDER REPORT.—Not later than 60 days after
15 the end of each fiscal year through fiscal year 2026, the Secretary shall
16 submit to the appropriate congressional committees a State of the Bor-
17 der report that—
- 18 (A) provides trends for each metric under this section for the
19 last 10 fiscal years, to the greatest extent possible;
- 20 (B) provides selected analysis into related aspects of illegal flow
21 rates, including undocumented migrant flows and stock estimation
22 techniques;
- 23 (C) provides selected analysis into related aspects of legal flow
24 rates; and
- 25 (D) includes any other information that the Secretary deter-
26 mines appropriate.
- 27 (4) METRICS UPDATE.—
- 28 (A) IN GENERAL.—After submitting the 10th report to the
29 Comptroller General under paragraph (1), the Secretary may re-
30 evaluate and update any of the metrics developed in accordance
31 with this section to ensure that the metrics are suitable to meas-
32 ure the effectiveness of border security.
- 33 (B) CONGRESSIONAL NOTIFICATION.—Not later than 30 days
34 before updating the metrics pursuant to subparagraph (A), the
35 Secretary shall notify the appropriate congressional committees of
36 the updates.
- 37 **§ 11116. Reports relating to border between United States**
38 **and Mexico**
- 39 (a) UNIDENTIFIED REMAINS.—
- 40 (1) ANNUAL REPORT.—Not later than 1 year after December 31,
41 2020, and annually thereafter, the Commissioner of U.S. Customs and

1 Border Protection shall submit a report to the appropriate committees
2 of Congress regarding all unidentified remains discovered, during the
3 reporting period, on or near the border between the United States and
4 Mexico, including—

5 (A) for each deceased individual—

6 (i) the cause and manner of death, if known;

7 (ii) the sex, age (at time of death), and country of origin
8 (if the information is determinable); and

9 (iii) the location of each unidentified remain;

10 (B) the total number of deceased individuals whose unidentified
11 remains were discovered by U.S. Customs and Border Protection
12 during the reporting period;

13 (C) to the extent the information is available to U.S. Customs
14 and Border Protection, the total number of deceased individuals
15 whose unidentified remains were discovered by Federal, State,
16 local or Tribal law enforcement officers, military personnel, or
17 medical examiner's offices;

18 (D) the efforts of U.S. Customs and Border Protection to en-
19 gage with nongovernmental organizations, institutions of higher
20 education, medical examiners and coroners, and law enforcement
21 agencies—

22 (i) to identify and map the locations at which migrant
23 deaths occur; and

24 (ii) to count the number of deaths that occur at those loca-
25 tions; and

26 (E) a detailed description of U.S. Customs and Border Protec-
27 tion's Missing Migrant Program, including how the program helps
28 mitigate migrant deaths while maintaining border security.

29 (2) PUBLIC DISCLOSURE.—Not later than 30 days after each report
30 required under paragraph (1) is submitted, the Commissioner of U.S.
31 Customs and Border Protection shall publish on the website of the
32 agency the information described in subparagraphs (A), (B), and (C)
33 of paragraph (1) during each reporting period.

34 (b) RESCUE BEACONS.—Not later than 1 year after December 31, 2020,
35 and annually thereafter, the Commissioner of U.S. Customs and Border
36 Protection shall submit a report to the appropriate committees of Congress
37 regarding the use of rescue beacons along the border between the United
38 States and Mexico, including, for the reporting period—

39 (1) the number of rescue beacons in each border patrol sector;

40 (2) the specific location of each rescue beacon;

1 (3) the frequency with which each rescue beacon was activated by
2 an individual in distress;

3 (4) a description of the nature of the distress that resulted in each
4 rescue beacon activation (if the information is determinable); and

5 (5) an assessment, in consultation with local stakeholders, including
6 elected officials, nongovernmental organizations, and landowners, of
7 necessary additional rescue beacons and recommendations for locations
8 for deployment to reduce migrant deaths.

9 (c) COMPTROLLER GENERAL REPORT.—Not later than 6 months after
10 the report required under subsection (a) is submitted to the appropriate
11 committees of Congress, the Comptroller General shall submit a report to
12 the same committees that describes—

13 (1) how U.S. Customs and Border Protection collects and records
14 border-crossing death data;

15 (2) the differences (if any) in U.S. Customs and Border Protection
16 border-crossing death data collection methodology across its sectors;

17 (3) how U.S. Customs and Border Protection’s data and statistical
18 analysis on trends in the numbers, locations, causes, and characteristics
19 of border-crossing deaths compare to other sources of data on these
20 deaths, including border county medical examiners and coroners and
21 the Centers for Disease Control and Prevention;

22 (4) how U.S. Customs and Border Protection measures the effective-
23 ness of its programs to mitigate migrant deaths; and

24 (5) the extent to which U.S. Customs and Border Protection engages
25 Federal, State, local, and Tribal governments, foreign diplomatic and
26 consular posts, and nongovernmental organizations—

27 (A) to accurately identify deceased individuals;

28 (B) to resolve cases involving unidentified remains;

29 (C) to resolve cases involving unidentified individuals; and

30 (D) to share information on missing individuals and unidentified
31 remains, specifically with the National Missing and Unidentified
32 Persons System (NamUs).

33 **§ 11117. Trusted traveler program**

34 The Secretary may not enter into or renew an agreement with the govern-
35 ment of a foreign country for a trusted traveler program administered by
36 U.S. Customs and Border Protection unless the Secretary certifies in writ-
37 ing that the government—

38 (1) routinely submits to INTERPOL for inclusion in INTERPOL’s
39 Stolen and Lost Travel Documents database information about lost and
40 stolen passports and travel documents of the citizens and nationals of
41 the country; or

1 (2) makes available to the United States Government the informa-
2 tion described in paragraph (1) through another means of reporting.

3 **§ 11118. Asia-Pacific Economic Cooperation Business Travel**
4 **Cards**

5 (a) DEFINITION OF TRUSTED TRAVELER PROGRAM.—In this section, the
6 term “trusted traveler program” means a voluntary program of the Depart-
7 ment that allows U.S. Customs and Border Protection to expedite clearance
8 of pre-approved, low-risk travelers arriving in the United States.

9 (b) IN GENERAL.—The Commissioner of U.S. Customs and Border Pro-
10 tection (in this section referred to as the “Commissioner”) may issue an
11 Asia-Pacific Economic Cooperation Business Travel Card (referred to in
12 this section as an “ABT Card”) to an individual described in subsection (c).

13 (c) INDIVIDUALS WHO MAY RECEIVE ABT CARD.—An individual re-
14 ferred to in subsection (b) is an individual who—

15 (1) is a citizen of the United States;

16 (2) has been approved and is in good standing in an existing inter-
17 national trusted traveler program of the Department; and

18 (3) is—

19 (A) engaged in business in the Asia-Pacific region, as deter-
20 mined by the Commissioner; or

21 (B) a United States Government official actively engaged in
22 Asia-Pacific Economic Cooperation business, as determined by the
23 Commissioner.

24 (d) INTEGRATION WITH EXISTING TRAVEL PROGRAMS.—The Commis-
25 sioner shall integrate application procedures for, and issuance, renewal, and
26 revocation of, ABT Cards with existing international trusted traveler pro-
27 grams of the Department.

28 (e) COOPERATION WITH PRIVATE ENTITIES AND NONGOVERNMENTAL
29 ORGANIZATIONS.—In carrying out this section, the Commissioner may con-
30 sult with appropriate private-sector entities and nongovernmental organiza-
31 tions, including academic institutions.

32 (f) FEE.—

33 (1) IN GENERAL.—The Commissioner shall—

34 (A) prescribe and collect a fee for the issuance and renewal of
35 ABT Cards; and

36 (B) adjust the fee to the extent the Commissioner determines
37 necessary to comply with paragraph (2).

38 (2) LIMITATION.—The Commissioner shall ensure that the total
39 amount of the fees collected under paragraph (1) during a fiscal year
40 is sufficient to offset the direct and indirect costs associated with car-
41 rying out this section during that fiscal year, including the costs associ-

1 ated with operating and maintaining the ABT Card issuance and re-
2 newal processes.

3 (3) ACCOUNT FOR COLLECTIONS.—There is in the Treasury an Asia-
4 Pacific Economic Cooperation Business Travel Card Account into
5 which the fees collected under paragraph (1) shall be deposited as off-
6 setting receipts.

7 (4) USE OF FUNDS.—Amounts deposited into the Asia-Pacific Eco-
8 nomic Cooperation Business Travel Card Account shall—

9 (A) be credited to the appropriate account of U.S. Customs and
10 Border Protection for expenses incurred in carrying out this sec-
11 tion; and

12 (B) remain available until expended.

13 (g) NOTIFICATION.—The Commissioner shall notify the Committee on
14 Homeland Security of the House of Representatives and the Committee on
15 Homeland Security and Governmental Affairs of the Senate not later than
16 60 days after the expenditures of funds to operate and provide ABT Card
17 services beyond the amounts collected under subsection (f)(1).

18 **§ 11119. Hiring members of the armed forces separating**
19 **from military service**

20 (a) EXPEDITED HIRING.—The Secretary shall consider the expedited hir-
21 ing of qualified candidates who have the ability to perform the essential
22 functions of the position of a U.S. Customs and Border Protection officer
23 and who are eligible for a veterans recruitment appointment authorized
24 under section 4214 of title 38.

25 (b) ENHANCED RECRUITING EFFORTS.—The Secretary, in consultation
26 with the Secretary of Defense, and acting through existing programs, au-
27 thorities, and agreements, where applicable, shall enhance the efforts of the
28 Department to recruit members of the armed forces who are separating
29 from military service to serve as U.S. Customs and Border Protection offi-
30 cers. The enhanced recruiting efforts shall—

31 (1) include U.S. Customs and Border Protection officer opportunities
32 in relevant job assistance efforts under the Transition Assistance Pro-
33 gram;

34 (2) place U.S. Customs and Border Protection officials or other rel-
35 evant Department officials at recruiting events and jobs fairs involving
36 members of the armed forces who are separating from military service;

37 (3) provide opportunities for local U.S. Customs and Border Protec-
38 tion field offices to partner with military bases in the region;

39 (4) include outreach efforts to educate members of the armed forces
40 with Military Occupational Specialty Codes and Officer Branches, Air
41 Force Specialty Codes, Naval Enlisted Classifications and Officer Des-

1 ignators, and Coast Guard competencies that are transferable to the re-
2 quirements, qualifications, and duties assigned to U.S. Customs and
3 Border Protection officers of available hiring opportunities to become
4 U.S. Customs and Border Protection officers;

5 (5) identify shared activities and opportunities for reciprocity related
6 to steps in hiring U.S. Customs and Border Protection officers with the
7 goal of minimizing the time required to hire qualified applicants;

8 (6) ensure the streamlined interagency transfer of relevant back-
9 ground investigations and security clearances; and

10 (7) include such other elements as may be necessary to ensure that
11 members of the armed forces who are separating from military service
12 are aware of opportunities to fill vacant U.S. Customs and Border Pro-
13 tection officer positions.

14 (c) REPORTS.—Not later than 180 days after October 16, 2015, and by
15 December 31 of each of the next 3 years, the Secretary, in consultation with
16 the Secretary of Defense, shall submit a report to the Committee on Home-
17 land Security and the Committee on Armed Services of the House of Rep-
18 resentatives and the Committee on Homeland Security and Governmental
19 Affairs and the Committee on Armed Services of the Senate that includes
20 a description and assessment of the efforts of the Department under this
21 section to hire members of the armed forces who are separating from mili-
22 tary service as U.S. Customs and Border Protection officers. The report
23 shall include—

24 (1) a detailed description of the efforts to implement subsection (b),
25 including—

26 (A) elements of the enhanced recruiting efforts and the goals
27 associated with those elements; and

28 (B) a description of how the elements and goals referred to in
29 subparagraph (A) will assist in meeting statutorily mandated
30 staffing levels and agency hiring benchmarks;

31 (2) a detailed description of the efforts that have been undertaken
32 under subsection (b);

33 (3) the estimated number of separating service members made aware
34 of U.S. Customs and Border Protection officer vacancies;

35 (4) the number of U.S. Customs and Border Protection officer va-
36 cancies filled with separating service members; and

37 (5) the number of U.S. Customs and Border Protection officer va-
38 cancies filled with separating service members under veterans recruit-
39 ment appointments authorized under section 4214 of title 38.

40 (d) RULES OF CONSTRUCTION.—Nothing in this section may be con-
41 strued—

1 (1) as superseding, altering, or amending existing Federal veterans'
2 hiring preferences or Federal hiring authorities; or

3 (2) as authorizing the appropriation of additional amounts to carry
4 out this section.

5 **§ 11120. Protecting America's food and agriculture**

6 (a) DEFINITIONS.—In this section:

7 (1) CBP.—The term “CBP” means U.S. Customs and Border Pro-
8 tection.

9 (2) COMMISSIONER.—The term “Commissioner” means Commis-
10 sioner of U.S. Customs and Border Protection.

11 (b) ADDITIONAL PERSONNEL.—

12 (1) CBP AGRICULTURE SPECIALISTS.—The Commissioner may hire,
13 train, and assign 240 new CBP Agriculture Specialists above the cur-
14 rent attrition level during every fiscal year until the total number of
15 CBP Agriculture Specialists equals and sustains the requirements iden-
16 tified each year in the Agriculture Resource Allocation Model.

17 (2) MISSION AND OPERATIONAL SUPPORT STAFF.—

18 (A) IN GENERAL.—The Commissioner may hire, train, and as-
19 sign support staff to support CBP Agriculture Specialists.

20 (B) CBP AGRICULTURE TECHNICIANS.—The Commissioner may
21 hire, train, and assign 200 new CBP Agriculture Technicians dur-
22 ing each fiscal year until the total number of CBP Agriculture
23 Technicians equals and sustains the requirements identified each
24 year in the Mission and Operation Support Resource Allocation
25 Model.

26 (3) CBP AGRICULTURE CANINE TEAMS.—The Commissioner may
27 hire, train, and assign 20 new CBP agriculture canine teams during
28 each of the first 3 fiscal years beginning after March 3, 2020.

29 (c) NUMBER OF CBP AGRICULTURE SPECIALISTS NEEDED AT EACH
30 PORT OF ENTRY.—In calculating the number of CBP Agriculture Special-
31 ists needed at each port of entry through the Agriculture Resource Alloca-
32 tion Model, the Office of Field Operations shall—

33 (1) rely on data collected regarding the inspections and other activi-
34 ties conducted at each port of entry; and

35 (2) consider volume from seasonal surges, other projected changes in
36 commercial and passenger volumes, the most current commercial fore-
37 casts, and other relevant information.

38 (d) AUTHORIZATION OF APPROPRIATIONS.—

39 (1) CBP AGRICULTURE SPECIALISTS.—There is authorized to be ap-
40 propriated to carry out subsection (b)(1) \$40,500,000 for fiscal year
41 2022.

1 (2) CBP AGRICULTURE TECHNICIANS.—There is authorized to be
2 appropriated to carry out subsection (b)(2) \$38,000,000 for fiscal year
3 2022.

4 (3) CBP AGRICULTURE CANINE TEAMS.—There is authorized to be
5 appropriated to carry out subsection (b)(3) \$12,200,000 for fiscal year
6 2022.

7 (4) TRAINING.—There is authorized to be appropriated for training
8 costs associated with new CBP personnel and canine teams hired pur-
9 suant to paragraphs (1), (2), and (3) of subsection (b) \$6,000,000 for
10 fiscal year 2022.

11 **§ 11121. Large-scale non-intrusive inspection scanning plan**

12 (a) DEFINITIONS.—In this section

13 (1) LARGE-SCALE NON-INTRUSIVE INSPECTION SYSTEM.—The term
14 “large-scale, non-intrusive inspection system” means a technology, in-
15 cluding x-ray, gamma-ray, and passive imaging systems, capable of pro-
16 ducing an image of the contents of a commercial or passenger vehicle
17 or freight rail car in 1 pass of the vehicle or car.

18 (2) SCANNING.—The term “scanning” means utilizing nonintrusive
19 imaging equipment, radiation detection equipment, or both, to capture
20 data, including images of a commercial or passenger vehicle or freight
21 rail car.

22 (b) IN GENERAL.—The Secretary shall submit a plan to the Committee
23 on Homeland Security and Governmental Affairs of the Senate and the
24 Committee on Homeland Security of the House of Representatives for in-
25 creasing to 100 percent the rate of high-throughput scanning of commercial
26 and passenger vehicles and freight rail traffic entering the United States at
27 land ports of entry and rail-border crossings along the border using large-
28 scale non-intrusive inspection systems or similar technology to enhance bor-
29 der security.

30 (c) BASELINE INFORMATION.—The plan under subsection (b) shall in-
31 clude, at a minimum, the following information regarding large-scale non-
32 intrusive inspection systems or similar technology operated by U.S. Customs
33 and Border Protection at land ports of entry and rail-border crossings as
34 of January 5, 2021:

35 (1) An inventory of large-scale non-intrusive inspection systems or
36 similar technology in use at each land port of entry.

37 (2) For each system or technology identified in the inventory under
38 paragraph (1)—

39 (A) the scanning method of the system or technology;

1 (B) the location of the system or technology at each land port
2 of entry that specifies whether in use in pre-primary, primary, or
3 secondary inspection area, or some combination of the areas;

4 (C) the percentage of commercial and passenger vehicles and
5 freight rail traffic scanned by the system or technology;

6 (D) seizure data directly attributed to scanned commercial and
7 passenger vehicles and freight rail traffic; and

8 (E) the number of personnel required to operate each system or
9 technology.

10 (3) Information regarding the continued use of other technology and
11 tactics used for scanning, such as canines and human intelligence in
12 conjunction with large scale, nonintrusive inspection systems.

13 (d)ELEMENTS.—The plan under subsection (b) shall include the following
14 information:

15 (1) Benchmarks for achieving incremental progress towards 100 per-
16 cent high-throughput scanning by January 5, 2027, of commercial and
17 passenger vehicles and freight rail traffic entering the United States at
18 land ports of entry and rail-border crossings along the border with cor-
19 responding projected incremental improvements in scanning rates by
20 fiscal year and rationales for the specified timeframes for each land
21 port of entry.

22 (2) Estimated costs, together with an acquisition plan, for achieving
23 the 100 percent high-throughput scanning rate within the timeframes
24 specified in paragraph (1), including acquisition, operations, and main-
25 tenance costs for large-scale, nonintrusive inspection systems or similar
26 technology, and associated costs for any necessary infrastructure en-
27 hancements or configuration changes at each port of entry. The acqui-
28 sition plan shall promote, to the extent practicable, opportunities for
29 entities that qualify as small business concerns (as defined under sec-
30 tion 3(a) of the Small Business Act (15 U.S.C. 632(a)).

31 (3) Any projected impacts, as identified by the Commissioner of U.S.
32 Customs and Border Protection, on the total number of commercial
33 and passenger vehicles and freight rail traffic entering at land ports
34 of entry and rail-border crossings where the systems are in use, and
35 average wait times at peak and non-peak travel times, by lane type if
36 applicable, as scanning rates are increased.

37 (4) Any projected impacts, as identified by the Commissioner of U.S.
38 Customs and Border Protection, on land ports of entry and rail-border
39 crossings border security operations as a result of implementation ac-
40 tions, including any changes to the number of U.S. Customs and Bor-
41 der Protection officers or their duties and assignments.

1 (e)ANNUAL REPORT.—Not later than 1 year after the submission of the
2 plan under subsection (b), and biennially thereafter for the following 6
3 years, the Secretary of Homeland Security shall submit a report to the
4 Committee on Homeland Security and Governmental Affairs of the Senate
5 and the Committee on Homeland Security of the House of Representatives
6 that describes the progress implementing the plan and includes—

7 (1) an inventory of large-scale, nonintrusive inspection systems or
8 similar technology operated by U.S. Customs and Border Protection at
9 each land port of entry;

10 (2) for each system or technology identified in the inventory required
11 under paragraph (1)—

12 (A) the scanning method of the system or technology;

13 (B) the location of the system or technology at each land port
14 of entry that specifies whether in use in pre-primary, primary, or
15 secondary inspection area, or some combination of the areas;

16 (C) the percentage of commercial and passenger vehicles and
17 freight rail traffic scanned by the system or technology; and

18 (D) seizure data directly attributed to scanned commercial and
19 passenger vehicles and freight rail traffic;

20 (3) the total number of commercial and passenger vehicles and
21 freight rail traffic entering at each land port of entry at which each
22 system or technology is in use, and information on average wait times
23 at peak and non-peak travel times, by lane type if applicable;

24 (4) a description of the progress towards reaching the benchmarks
25 referred to in subsection (d)(1), and an explanation if any of the bench-
26 marks are not achieved as planned;

27 (5) a comparison of actual costs (including information on any
28 awards of associated contracts) to estimated costs set forth in sub-
29 section (d)(2);

30 (6) any realized impacts, as identified by the Commissioner of U.S.
31 Customs and Border Protection, on land ports of entry and rail-border
32 crossings operations as a result of implementation actions, including
33 any changes to the number of U.S. Customs and Border Protection of-
34 ficers or their duties and assignments;

35 (7) any proposed changes to the plan and an explanation for the
36 changes, including changes made in response to any Department re-
37 search and development findings or changes in terrorist or
38 transnational criminal organizations tactics, techniques, or procedures;
39 and

40 (8) any challenges to implementing the plan or meeting the bench-
41 marks, and plans to mitigate the challenges.

Part B—Customs Functions

§ 11131. Definition of customs revenue function

In this subchapter, the term “customs revenue function” means the following:

(1) Assessing and collecting customs duties (including antidumping and countervailing duties and duties imposed under safeguard provisions), excise taxes, fees, and penalties due on imported merchandise, including classifying and valuing merchandise for purposes of assessment.

(2) Processing and denial of entry of persons, baggage, cargo, and mail, with respect to the assessment and collection of import duties.

(3) Detecting and apprehending persons engaged in fraudulent practices designed to circumvent the customs laws of the United States.

(4) Enforcing section 337 of the Tariff Act of 1930 (19 U.S.C. 1337) and provisions relating to import quotas and the marking of imported merchandise, and providing Customs Recordations for copyrights, patents, and trademarks.

(5) Collecting accurate import data for compilation of international trade statistics.

(6) Enforcing reciprocal trade agreements.

(7) Functions performed by the following personnel, and associated support staff, of U. S. Customs and Border Protection on January 23, 2003:

(A) Import Specialists.

(B) Entry Specialists.

(C) Drawback Specialists.

(D) National Import Specialists.

(E) Fines and Penalties Specialists.

(F) Attorneys of the Office of Regulations and Rulings.

(G) Customs Auditors.

(H) International Trade Specialists.

(I) Financial Systems Specialists.

(8) Functions performed by the following offices, with respect to any function described in any of paragraphs (1) through (7), and associated support staff, of the United States Customs Service on January 23, 2003, and of U.S. Customs and Border Protection on February 23, 2016:

(A) Office of Information and Technology.

(B) Office of Laboratory Services.

(C) Office of the Chief Counsel.

- 1 (D) Office of Congressional Affairs.
- 2 (E) Office of International Affairs.
- 3 (F) Office of Training and Development.

4 **§ 11132. Retention of customs revenue functions by Sec-**
5 **retary of the Treasury**

6 (a) RETENTION OF CUSTOMS REVENUE FUNCTIONS BY SECRETARY OF
7 THE TREASURY.—

8 (1) RETENTION OF AUTHORITY.—Notwithstanding section
9 11101(b)(1) of this title, authority relating to customs revenue func-
10 tions that was vested in the Secretary of the Treasury by law before
11 January 24, 2003, under those provisions of law set forth in paragraph
12 (2) shall not be transferred to the Secretary by reason of the Homeland
13 Security Act of 2002 (Public Law 107–296, 116 Stat. 2135) and, on
14 and after January 24, 2003, the Secretary of the Treasury may dele-
15 gate that authority to the Secretary at the discretion of the Secretary
16 of the Treasury. The Secretary of the Treasury shall consult with the
17 Secretary regarding the exercise of authority not delegated to the Sec-
18 retary.

19 (2) STATUTES.—The provisions of law referred to in paragraph (1)
20 are the following:

21 (A) Section 249 of the Revised Statutes of the United States
22 (19 U.S.C. 3).

23 (B) Section 2 of the Act of March 4, 1923 (19 U.S.C. 6).

24 (C) Section 13031 of the Consolidated Omnibus Budget Rec-
25 onciliation Act of 1985 (19 U.S.C. 58e).

26 (D) Section 251 of the Revised Statutes of the United States
27 (19 U.S.C. 66).

28 (E) Section 1 of the Act of June 26, 1930 (19 U.S.C. 68).

29 (F) The Act of June 18, 1934 (known as the Foreign Trade
30 Zones Act) (19 U.S.C. 81a et seq.).

31 (G) Section 1 of the Act of March 2, 1911 (19 U.S.C. 198).

32 (H) The Tariff Act of 1930 (19 U.S.C. 1202 et seq.).

33 (I) The Trade Act of 1974 (19 U.S.C. 2101 et seq.).

34 (J) The Trade Agreements Act of 1979 (19 U.S.C. 2501 et
35 seq.).

36 (K) The Caribbean Basin Economic Recovery Act (19 U.S.C.
37 2701 et seq.).

38 (L) The Andean Trade Preference Act (19 U.S.C. 3201 et seq.).

39 (M) The North American Free Trade Agreement Implementa-
40 tion Act (19 U.S.C. 3311 et seq.).

1 (N) The Uruguay Round Agreements Act (19 U.S.C. 3501 et
2 seq.).

3 (O) The African Growth and Opportunity Act (19 U.S.C. 3701
4 et seq.).

5 (P) Any other provision of law vesting customs revenue func-
6 tions in the Secretary of the Treasury.

7 (b) MAINTENANCE OF CUSTOMS REVENUE FUNCTIONS.—

8 (1) MAINTENANCE OF FUNCTIONS.—Notwithstanding this subtitle,
9 the Secretary may not consolidate, discontinue, or diminish those func-
10 tions described in paragraph (2) performed by U.S. Customs and Bor-
11 der Protection on or after January 24, 2003, reduce the staffing level,
12 or reduce the resources attributable to the functions, and the Secretary
13 shall ensure that an appropriate management structure is implemented
14 to carry out the functions.

15 (2) FUNCTIONS.—The functions referred to in paragraph (1) are
16 those functions performed by the following personnel, and associated
17 support staff, of U. S. Customs and Border Protection on January 23,
18 2003:

19 (A) Import Specialists.

20 (B) Entry Specialists.

21 (C) Drawback Specialists.

22 (D) National Import Specialists.

23 (E) Fines and Penalties Specialists.

24 (F) Attorneys of the Office of Regulations and Rulings.

25 (G) Customs Auditors.

26 (H) International Trade Specialists.

27 (I) Financial Systems Specialists.

28 (c) NEW PERSONNEL.—The Secretary of the Treasury may appoint up
29 to 20 new personnel to work with personnel of the Department in per-
30 forming customs revenue functions.

31 **§ 11133. Preservation of customs funds**

32 Notwithstanding this subtitle, no funds collected under section 13031(a)
33 (1) through (8) of the Consolidated Omnibus Budget Reconciliation Act of
34 1985 (19 U.S.C. 58e(a)(1) through (8)) may be transferred for use by an-
35 other agency or office in the Department.

36 **Part C—Drug Interdiction**

37 **§ 11141. Methamphetamine and methamphetamine pre- 38 cursor chemicals**

39 (a) DEFINITION OF METHAMPHETAMINE PRECURSOR CHEMICALS.—In
40 this section, the term “methamphetamine precursor chemicals” means the
41 chemicals ephedrine, pseudoephedrine, or phenylpropanolamine, including

1 each of the salts, optical isomers, and salts of optical isomers of the chemi-
2 cals.

3 (b) COMPLIANCE WITH PERFORMANCE PLAN REQUIREMENTS.—As part
4 of the annual performance plan required in the budget submission of U.S.
5 Customs and Border Protection under section 1115 of title 31, the Commis-
6 sioner of U.S. Customs and Border Protection (in this section referred to
7 as the “Commissioner”) shall establish performance indicators relating to
8 the seizure of methamphetamine and methamphetamine precursor chemicals
9 in order to evaluate the performance goals of U.S. Customs and Border
10 Protection with respect to the interdiction of illegal drugs entering the
11 United States.

12 (c) STUDY AND REPORT RELATING TO METHAMPHETAMINE AND METH-
13 AMPHETAMINE PRECURSOR CHEMICALS.—

14 (1) ANALYSIS.—The Commissioner shall, on an ongoing basis, ana-
15 lyze the movement of methamphetamine and methamphetamine pre-
16 cursor chemicals into the United States. In conducting the analysis, the
17 Commissioner shall—

18 (A) consider the entry of methamphetamine and methamphet-
19 amine precursor chemicals through ports of entry, between ports
20 of entry, through international mails, and through international
21 courier services;

22 (B) examine the export procedures of each foreign country
23 where the shipments of methamphetamine and methamphetamine
24 precursor chemicals originate and determine if changes in the
25 country’s customs overtime provisions would alleviate the export of
26 methamphetamine and methamphetamine precursor chemicals;
27 and

28 (C) identify emerging trends in smuggling techniques and strat-
29 egies.

30 (2) REPORT.—Not later than September 30 of each odd-numbered
31 year, the Commissioner, in consultation with the Attorney General,
32 United States Immigration and Customs Enforcement, the United
33 States Drug Enforcement Administration, and the United States De-
34 partment of State, shall submit a report to the Committee on Finance
35 of the Senate, the Committee on Foreign Relations of the Senate, the
36 Committee on the Judiciary of the Senate, the Committee on Ways and
37 Means of the House of Representatives, the Committee on Foreign Af-
38 fairs of the House of Representatives, and the Committee on the Judi-
39 ciary of the House of Representatives that includes—

40 (A) a comprehensive summary of the analysis described in para-
41 graph (1); and

1 (B) a description of how U.S. Customs and Border Protection
2 utilized the analysis described in paragraph (1) to target ship-
3 ments presenting a high risk for smuggling or circumvention of
4 the Combat Methamphetamine Epidemic Act of 2005 (Public Law
5 109–177, title VII, 120 Stat. 256).

6 (3) AVAILABILITY OF ANALYSIS.—The Commissioner shall ensure
7 that the analysis described in paragraph (1) is made available in a
8 timely manner to the Secretary of State to facilitate the Secretary in
9 fulfilling the Secretary’s reporting requirements in section 722 of the
10 Combat Methamphetamine Epidemic Act of 2005 (Public Law 109–
11 177, title VII, 120 Stat. 268).

12 **§ 11142. Protection against potential synthetic opioid expo-**
13 **sure**

14 (a) ISSUANCE OF POLICY.—The Commissioner of U.S. Customs and Bor-
15 der Protection (in this section referred to as the “Commissioner”) shall
16 issue a policy that specifies effective protocols and procedures—

17 (1) for the safe handling of potential synthetic opioids, including
18 fentanyl, by U.S. Customs and Border Protection officers, agents, other
19 personnel, and canines; and

20 (2) to reduce the risk of injury or death resulting from accidental
21 exposure and enhance post-exposure management.

22 (b) TRAINING.—

23 (1) IN GENERAL.— Together with the issuance of the policy de-
24 scribed in subsection (a), the Commissioner shall require mandatory
25 and recurrent training on the following:

26 (A) The potential risk of opioid exposure and safe handling pro-
27 cedures for potential synthetic opioids, including precautionary
28 measures such as the use of personal protective equipment during
29 the handling of potential synthetic opioids.

30 (B) How to access and administer opioid receptor antagonists,
31 including naloxone, post-exposure to potential synthetic opioids.

32 (C) How to use containment devices to prevent potential syn-
33 thetic opioid exposure.

34 (2) INTEGRATION WITH OTHER TRAINING.— The training described
35 in paragraph (1) may be integrated into existing training undersection
36 11102(d) of this title for U.S. Customs and Border Protection officers,
37 agents, and other personnel.

38 (c) PERSONAL PROTECTIVE EQUIPMENT, CONTAINMENT DEVICES, AND
39 OPIOID RECEPTOR ANTAGONISTS.— Together with the issuance of the pol-
40 icy described in subsection (a), the Commissioner shall ensure the avail-
41 ability of personal protective equipment and opioid receptor antagonists, in-

1 cluding naloxone and containment devices, to all U.S. Customs and Border
2 Protection officers, agents, other personnel, and canines at risk of accidental
3 exposure to synthetic opioids.

4 (d) OVERSIGHT.—To ensure the effectiveness of the policy described in
5 subsection (a)—

6 (1) the Commissioner shall regularly monitor the efficacy of the im-
7 plementation of the policy and adjust protocols and procedures, as nec-
8 essary; and

9 (2) the Inspector General of the Department shall audit compliance
10 with the requirements of this section not less than once during the 3-
11 year period after December 27, 2020.

12 (e) APPLICABILITY TO OTHER COMPONENTS.—If the Secretary deter-
13 mines that other officers, agents, other personnel, or canines of a component
14 of the Department other than U.S. Customs and Border Protection are at
15 risk of potential synthetic opioid exposure in the course of their duties, the
16 head of the component shall carry out the responsibilities under this section
17 in the same manner and to the same manner as the Commissioner carries
18 out the responsibilities.

19 **§ 11143. Reports, evaluations, and research regarding drug**
20 **interdiction at and between ports of entry**

21 (a) DETECTION OF NARCOTICS AT VARIOUS PURITY LEVELS.—The Com-
22 missioner of U.S. Customs and Border Protection shall—

23 (1) implement a strategy to ensure deployed chemical screening de-
24 vices are able to identify, in an operational environment, narcotics at
25 purity levels less than or equal to 10 percent, or provide ports of entry
26 with an alternate method for identifying narcotics at lower purity lev-
27 els; and

28 (2) require testing of any new chemical screening devices to under-
29 stand the abilities and limitations of the devices relating to identifying
30 narcotics at various purity levels before CBP commits to the acquisi-
31 tion of the devices.

32 (b) DEVELOPMENT OF CENTRALIZED SPECTRAL DATABASE FOR CHEM-
33 ICAL SCREENING DEVICES.—The Secretary shall implement a plan for the
34 long-term development of a centralized spectral database for chemical
35 screening devices. The plan shall address the following:

36 (1) How newly identified spectra will be collected, stored, and dis-
37 tributed to the devices in their operational environment, including at
38 ports of entry.

39 (2) Identification of parties responsible for updates and maintenance
40 of the database.

1 (c) RESEARCH ON ADDITIONAL TECHNOLOGIES TO DETECT
2 FENTANYL.—Not later than December 23, 2023, the Secretary, in consulta-
3 tion with the Attorney General, the Secretary of Health and Human Serv-
4 ices, and the Director of the Office of National Drug Control Policy, shall
5 research additional technological solutions to—

6 (1) target and detect illicit fentanyl, fentanyl analogs, and precursor
7 chemicals, including low-purity fentanyl, especially in counterfeit
8 pressed tablets, and illicit pill press molds; and

9 (2) enhance detection of the counterfeit pressed tablets through non-
10 intrusive, noninvasive, and other advanced screening technologies.

11 (d) EVALUATION OF CURRENT TECHNOLOGIES AND STRATEGIES IN IL-
12 LICIT DRUG INTERDICTION AND PROCUREMENT DECISIONS.—

13 (1) IN GENERAL.—The Secretary, in consultation with the Attorney
14 General, the Secretary of Health and Human Services, and the Direc-
15 tor of the Office of National Drug Control Policy, shall establish a pro-
16 gram to collect available data and develop metrics to measure how tech-
17 nologies and strategies used by the Department, U.S. Customs and
18 Border Protection, U.S. Immigration and Customs Enforcement, and
19 other relevant Federal agencies have helped detect trafficked illicit
20 fentanyl, fentanyl analogs, and precursor chemicals or deter illicit
21 fentanyl, fentanyl analogs, and precursor chemicals from being traf-
22 ficked into the United States at and between land, air, and sea ports
23 of entry.

24 (2) CONSIDERATIONS.—The data and metrics program established
25 pursuant to paragraph (1) may consider

26 (A) the rate of detection of illicit fentanyl, fentanyl analogs, and
27 precursor chemicals at land, air, and sea ports of entry;

28 (B) investigations and intelligence sharing into the origins of il-
29 licit fentanyl, fentanyl analogs, and precursor chemicals in the
30 United States; and

31 (C) other data or metric the Secretary considers appropriate.

32 (3) UPDATES.—The Secretary, as appropriate and in the coordina-
33 tion with the officials referred to in paragraph (1), may update the
34 data and metrics programs established pursuant to paragraph (1).

35 (4) REPORTS.—

36 (A) SECRETARY.— Not later than December 23, 2023, and bi-
37 ennially thereafter, the Secretary, in consultation with the Attor-
38 ney General, the Secretary of Health and Human Services, and
39 the Director of the Office of National Drug Control Policy, shall,
40 based on the data collected and metrics developed pursuant to the
41 program established pursuant to paragraph (1), submit to the

1 Committee on Homeland Security, the Committee on Energy and
2 Commerce, the Committee on Science, Space, and Technology, and
3 the Committee on the Judiciary of the House of Representatives
4 and the Committee on Homeland Security and Governmental Af-
5 fairs, the Committee on Commerce, Science, and Transportation,
6 and the Committee on the Judiciary of the Senate a report that—

7 (i) examines and analyzes current technologies, including
8 pilot technologies, deployed at land, air, and sea ports of
9 entry to assess how well the technologies detect, deter, and
10 address illicit fentanyl, fentanyl analogs, and precursor chemi-
11 cals; and

12 (ii) examines and analyzes current technologies, including
13 pilot technologies, deployed between land ports of entry to as-
14 sess how well and accurately the technologies detect, deter,
15 and address illicit fentanyl, fentanyl analogs, and precursor
16 chemicals.

17 (B) GOVERNMENT ACCOUNTABILITY OFFICE.—Not later
18 than 1 year after the submission of each of the first 3 reports re-
19 quired under subparagraph (A), the Comptroller General shall
20 submit to the Committee on Homeland Security, the Committee
21 on Energy and Commerce, the Committee on Science, Space, and
22 Technology, and the Committee on the Judiciary of the House of
23 Representatives and the Committee on Homeland Security and
24 Governmental Affairs, the Committee on Commerce, Science, and
25 Transportation, and the Committee on the Judiciary of the Senate
26 a report that evaluates and as appropriate makes recommenda-
27 tions to improve the collection of data under the program estab-
28 lished pursuant to paragraph (1) and metrics used in the subse-
29 quent reports required under that paragraph.

30 **Subchapter III—Immigration Enforcement** 31 **Functions**

32 **§ 11151. Transfer of functions**

33 The Secretary succeeds to the functions, personnel, assets, and liabilities
34 of the following programs of the Commissioner of Immigration and Natu-
35 ralization:

- 36 (1) The Border Patrol program.
- 37 (2) The detention and removal program.
- 38 (3) The intelligence program.
- 39 (4) The investigations program.
- 40 (5) The inspections program.

1 **§ 11152. Responsibilities of U.S. Immigration and Customs**
2 **Enforcement officials**

3 (a) DIRECTOR OF IMMIGRATION AND CUSTOMS ENFORCEMENT.—

4 (1) FUNCTIONS.—The Director of Immigration and Customs En-
5 forcement—

6 (A) shall establish the policies for performing functions—

7 (i) transferred to the Secretary by section 11151 of this
8 title and delegated to the Director of Immigration and Cus-
9 toms Enforcement by the Secretary; or

10 (ii) otherwise vested in the Director of Immigration and
11 Customs Enforcement by law;

12 (B) shall oversee the administration of the policies; and

13 (C) shall advise the Secretary with respect to a policy or oper-
14 ation of U.S. Immigration and Customs Enforcement that may af-
15 fect U.S. Citizenship and Immigration Services established under
16 subchapter IV of this chapter, including potentially conflicting
17 policies or operations.

18 (2) PROGRAM TO COLLECT INFORMATION RELATING TO FOREIGN
19 STUDENTS.—The Director of Immigration and Customs Enforcement
20 is responsible for administering the program to collect information re-
21 lating to nonimmigrant foreign students and other exchange program
22 participants described in section 641 of the Illegal Immigration Reform
23 and Immigrant Responsibility Act of 1996 (8 U.S.C. 1372), including
24 the Student and Exchange Visitor Information System established
25 under that section, and shall use the information to carry out the en-
26 forcement functions of U.S. Immigration and Customs Enforcement.

27 (3) MANAGERIAL ROTATION PROGRAM.—The Director of Immigra-
28 tion and Customs Enforcement shall design and implement a manage-
29 rial rotation program under which employees of U.S. Immigration and
30 Customs Enforcement holding positions involving supervisory or mana-
31 gerial responsibility and classified, in accordance with chapter 51 of
32 title 5, as a GS-14 or above, shall—

33 (A) gain some experience in all the major functions performed
34 by U.S. Immigration and Customs Enforcement; and

35 (B) work in at least one local office of U.S. Immigration and
36 Customs Enforcement.

37 (b) CHIEF OF POLICY AND STRATEGY.—

38 (1) IN GENERAL.—There is a Chief of Policy and Strategy for U.S.
39 Immigration and Customs Enforcement.

1 (2) FUNCTIONS.—In consultation with U.S. Immigration and Customs Enforcement personnel in local offices, the Chief of Policy and Strategy is responsible for—

2 (A) making policy recommendations and performing policy research and analysis on immigration enforcement issues; and

3 (B) coordinating immigration policy issues with the Chief of Policy and Strategy for U.S. Citizenship and Immigration Services, as appropriate.

4 (c) LEGAL ADVISOR.—There is a principal legal advisor to the Assistant Secretary of Immigration and Customs Enforcement. The legal advisor shall provide specialized legal advice to the Assistant Secretary and shall represent U.S. Immigration and Customs Enforcement in all exclusion, deportation, and removal proceedings before the Executive Office for Immigration Review.

5 **§ 11153. Professional responsibility and quality review**

6 The Secretary is responsible for—

7 (1) conducting investigations of noncriminal allegations of misconduct, corruption, and fraud involving an employee of U. S. Immigration and Customs Enforcement that are not subject to investigation by the Inspector General for the Department;

8 (2) inspecting the operations of U. S. Immigration and Customs Enforcement and providing assessments of the quality of the operations of U. S. Immigration and Customs Enforcement as a whole and each of its components; and

9 (3) providing an analysis of the management of U.S. Immigration and Customs Enforcement.

10 **§ 11154. Annual report on cross-border tunnels**

11 (a) DEFINITION OF CONGRESSIONAL COMMITTEES.—In this section, the term “congressional committees” means—

12 (1) the Committee on Homeland Security and Governmental Affairs of the Senate;

13 (2) the Committee on the Judiciary of the Senate;

14 (3) the Committee on Appropriations of the Senate;

15 (4) the Committee on Homeland Security of the House of Representatives;

16 (5) the Committee on the Judiciary of the House of Representatives; and

17 (6) the Committee on Appropriations of the House of Representatives.

18 (b) CONTENT.—The Secretary shall submit an annual report to the congressional committees that includes a description of—

1 (1) the cross-border tunnels along the border between Mexico and
2 the United States discovered during the preceding fiscal year; and

3 (2) the needs of the Department to effectively prevent, investigate,
4 and prosecute border tunnel construction along the border between
5 Mexico and the United States.

6 **§ 11155. Illicit cross-border tunnel defense**

7 (a) COUNTER ILLICIT CROSS-BORDER TUNNEL OPERATIONS STRATEGIC
8 PLAN.—

9 (1) IN GENERAL.—Not later than 180 days after December 23,
10 2022, the Commissioner of U.S. Customs and Border Protection, in co-
11 ordination with the Under Secretary for Science and Technology, and,
12 as appropriate, other officials of the Department, shall develop an illicit
13 cross-border tunnel operations strategic plan (in this section referred
14 to as the “strategic plan”) to address the following:

15 (A) Risk-based criteria to be used to prioritize the identification,
16 breach, assessment, and remediation of illicit cross-border tunnels.

17 (B) Promote the use of innovative technologies to identify,
18 breach, assess, and remediate illicit cross-border tunnels in a man-
19 ner that, among other considerations, reduces the impact of those
20 activities on surrounding communities.

21 (C) Processes to share relevant illicit cross-border tunnel loca-
22 tions, operations, and technical information.

23 (D) Indicators of specific types of illicit cross-border tunnels
24 found in each U.S. Border Patrol sector identified through oper-
25 ations to be periodically disseminated to U.S. Border Patrol sector
26 chiefs to education field personnel.

27 (E) A counter illicit cross-border tunnel operations resource
28 needs assessment that includes consideration of the following:

29 (i) Technology needs.

30 (ii) Staffing needs including the following:

31 (I) A position description for counter illicit cross-bor-
32 der tunnel operations personnel.

33 (II) Any specialized skills required of the personnel.

34 (III) The number of the full time personnel
35 disaggregated by U.S. Border Patrol sector.

36 (2) Report to congress on strategic plan.—Not later than 1 year
37 after the development of the strategic plan, the Commissioner of U.S.
38 Customs and Border Protection shall submit to the Committee on
39 Homeland Security of the House of Representatives and the Committee
40 on Homeland Security and Governmental Affairs of the Senate a report
41 on the implementation of the strategic plan.

1 (b) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be ap-
2 propriated to the Commissioner of U.S. Customs and Border Protection
3 \$1,000,000 for each of fiscal years 2023 and 2024 to carry out.—

4 (1) the development of the strategic plan; and

5 (2) remediation operations of illicit cross-border tunnels in accord-
6 ance with the strategic plan to the maximum extent practicable.

7 **Subchapter IV—Citizenship and** 8 **Immigration Services**

9 **§ 11171. Transfer of functions to Director of U.S. Citizenship** 10 **and Immigration Services**

11 The Director of U.S. Citizenship and Immigration Services succeeds to
12 the following functions of the Commissioner of Immigration and Naturaliza-
13 tion, and all personnel, infrastructure, and funding provided to the Commis-
14 sioner in support of the functions immediately before March 1, 2003:

15 (1) Adjudications of immigrant visa petitions.

16 (2) Adjudications of naturalization petitions.

17 (3) Adjudications of asylum and refugee applications.

18 (4) Adjudications performed at service centers.

19 (5) All other adjudications performed by the Immigration and Natu-
20 ralization Service immediately before March 1, 2003.

21 **§ 11172. Responsibilities of U.S. Citizenship and Immigra-** 22 **tion Services officials**

23 (a) DIRECTOR.—

24 (1) FUNCTIONS.—The Director of U.S. Citizenship and Immigration
25 Services—

26 (A) shall establish the policies for performing the functions
27 transferred to the Director by section 11171 of this title or the
28 Homeland Security Act of 2002 (Public Law 107–296, 116 Stat.
29 2135) or otherwise vested in the Director by law;

30 (B) shall oversee the administration of the policies;

31 (C) shall advise the Deputy Secretary of Homeland Security
32 with respect to a policy or operation of U.S. Citizenship and Immi-
33 gration Services that may affect U.S. Immigration and Customs
34 Enforcement, including potentially conflicting policies or oper-
35 ations;

36 (D) shall establish national immigration services policies and
37 priorities;

38 (E) shall meet regularly with the Ombudsman described in sec-
39 tion 11173 of this title to correct serious service problems identi-
40 fied by the Ombudsman; and

1 (F) shall establish procedures requiring a formal response to
2 recommendations submitted in the Ombudsman's annual report to
3 Congress within 3 months after its submission to Congress.

4 (2) MANAGERIAL ROTATION PROGRAM.—The Director of U.S. Citi-
5 zenship and Immigration Services shall design and implement a mana-
6 gerial rotation program under which employees of U.S. Citizenship and
7 Immigration Services holding positions involving supervisory or mana-
8 gerial responsibility and classified, in accordance with chapter 51 of
9 title 5, as a GS-14 or above, shall—

10 (A) gain some experience in all the major functions performed
11 by U.S. Citizenship and Immigration Services; and

12 (B) work in at least one field office and one service center of
13 U.S. Citizenship and Immigration Services.

14 (3) PILOT INITIATIVES FOR BACKLOG ELIMINATION.—The Director
15 of U.S. Citizenship and Immigration Services may implement innova-
16 tive pilot initiatives to eliminate a remaining backlog in the processing
17 of immigration benefit applications, and to prevent a backlog in the
18 processing of applications from recurring, under section 204(a) of the
19 Immigration Services and Infrastructure Improvements Act of 2000 (8
20 U.S.C. 1573(a)). Initiatives may include measures such as increasing
21 personnel, transferring personnel to focus on areas with the largest po-
22 tential for backlog, and streamlining paperwork.

23 (b) CHIEF OF POLICY AND STRATEGY.—

24 (1) IN GENERAL.—There is a Chief of Policy and Strategy for U.S.
25 Citizenship and Immigration Services.

26 (2) FUNCTIONS.—In consultation with U.S. Citizenship and Immi-
27 gration Services personnel in field offices, the Chief of Policy and
28 Strategy is responsible for—

29 (A) making policy recommendations and performing policy re-
30 search and analysis on immigration services issues; and

31 (B) coordinating immigration policy issues with the Chief of
32 Policy and Strategy for U.S. Immigration and Customs Enforce-
33 ment.

34 (c) LEGAL ADVISOR.—

35 (1) IN GENERAL.—There is a principal legal advisor to the Director
36 of U.S. Citizenship and Immigration Services.

37 (2) FUNCTIONS.—The legal advisor is responsible for—

38 (A) providing specialized legal advice, opinions, determinations,
39 regulations, and other assistance to the Director of U.S. Citi-
40 zenship and Immigration Services with respect to legal matters affect-
41 ing U.S. Citizenship and Immigration Services; and

1 (B) representing U.S. Citizenship and Immigration Services in
2 visa petition appeal proceedings before the Executive Office for
3 Immigration Review.

4 (d) BUDGET OFFICER.—

5 (1) IN GENERAL.—There is a Budget Officer for U.S. Citizenship
6 and Immigration Services.

7 (2) FUNCTIONS.—The Budget Officer is responsible for—

8 (A) formulating and executing the budget of U.S. Citizenship
9 and Immigration Services;

10 (B) managing the finances of U.S. Citizenship and Immigration
11 Services; and

12 (C) collecting all payments, fines, and other debts for U.S. Citi-
13 zenship and Immigration Services.

14 (e) CHIEF OF OFFICE OF CITIZENSHIP.—

15 (1) IN GENERAL.—There is a Chief of the Office of Citizenship for
16 U.S. Citizenship and Immigration Services.

17 (2) FUNCTIONS.—The Chief of the Office of Citizenship for U.S.
18 Citizenship and Immigration Services is responsible for promoting in-
19 struction and training on citizenship responsibilities for aliens inter-
20 ested in becoming naturalized citizens of the United States, including
21 the development of educational materials.

22 **§ 11173. Citizenship and Immigration Services Ombudsman**

23 (a) IN GENERAL.—There is in the Department a Citizenship and Immi-
24 gration Services Ombudsman (in this section referred to as the “Ombuds-
25 man”). The Ombudsman shall report directly to the Deputy Secretary of
26 Homeland Security. The Ombudsman shall have a background in customer
27 service as well as immigration law.

28 (b) FUNCTIONS.—The Ombudsman—

29 (1) shall assist individuals and employers in resolving problems with
30 U.S. Citizenship and Immigration Services;

31 (2) shall identify areas in which individuals and employers have
32 problems in dealing with U.S. Citizenship and Immigration Services;
33 and

34 (3) to the extent possible, shall propose changes in the administrative
35 practices of U.S. Citizenship and Immigration Services to mitigate
36 problems identified under paragraph (2).

37 (c) ANNUAL REPORT.—

38 (1) OBJECTIVES.—Not later than June 30 each year, the Ombuds-
39 man shall report to the Committees on the Judiciary of the House of
40 Representatives and the Senate on the objectives of the Office of the
41 Ombudsman for the fiscal year beginning in that year. The report shall

1 contain full and substantive analysis, in addition to statistical informa-
2 tion, and—

3 (A) shall identify the recommendations the Office of the Om-
4 budsman has made on improving the services and responsiveness
5 of U.S. Citizenship and Immigration Services;

6 (B) shall contain a summary of the most pervasive and serious
7 problems encountered by individuals and employers, including a
8 description of the nature of the problems;

9 (C) shall contain an inventory of the items described in sub-
10 paragraphs (A) and (B) for which action has been taken and the
11 result of the action;

12 (D) shall contain an inventory of the items described in sub-
13 paragraphs (A) and (B) for which action remains to be completed
14 and the period during which each item has remained on the inven-
15 tory;

16 (E) shall contain an inventory of the items described in sub-
17 paragraphs (A) and (B) for which no action has been taken, the
18 period during which each item has remained on the inventory, and
19 the reasons for the inaction, and shall identify any official of U.S.
20 Citizenship and Immigration Services who is responsible for the
21 inaction;

22 (F) shall contain recommendations for administrative action ap-
23 propriate to resolve problems encountered by individuals and em-
24 ployers, including problems created by excessive backlogs in the
25 adjudication and processing of immigration benefit petitions and
26 applications; and

27 (G) shall include other information the Ombudsman may deem
28 advisable.

29 (2) REPORT TO BE SUBMITTED DIRECTLY TO COMMITTEES.—Each
30 report required under this subsection shall be provided directly to the
31 committees described in paragraph (1) without prior comment or
32 amendment from the Secretary, the Deputy Secretary of Homeland Se-
33 curity, the Director of U.S. Citizenship and Immigration Services, or
34 another officer or employee of the Department or the Office of Manage-
35 ment and Budget.

36 (d) OTHER RESPONSIBILITIES.—The Ombudsman—

37 (1) shall monitor the coverage and geographic allocation of local of-
38 fices of the Ombudsman;

39 (2) shall develop guidance to be distributed to all officers and em-
40 ployees of U.S. Citizenship and Immigration Services outlining the cri-
41 teria for referral of inquiries to local offices of the Ombudsman;

1 (3) shall ensure that the local telephone number for each local office
2 of the Ombudsman is published and available to individuals and em-
3 ployers served by the office; and

4 (4) shall meet regularly with the Director of U.S. Citizenship and
5 Immigration Services to identify serious service problems and to
6 present recommendations for administrative action appropriate to re-
7 solve problems encountered by individuals and employers.

8 (e) PERSONNEL ACTIONS.—

9 (1) IN GENERAL.—The Ombudsman has the responsibility and au-
10 thority—

11 (A) to appoint local ombudsmen and make available at least one
12 ombudsman for each State; and

13 (B) to evaluate and take personnel actions (including dismissal)
14 with respect to an employee of a local office of the Ombudsman.

15 (2) CONSULTATION.—The Ombudsman may consult with the appro-
16 priate supervisory personnel of U.S. Citizenship and Immigration Serv-
17 ices in carrying out the Ombudsman's responsibilities under this sub-
18 section.

19 (f) RESPONSIBILITIES OF DIRECTOR OF U.S. CITIZENSHIP AND IMMIGRA-
20 TION SERVICES.—The Director of U.S. Citizenship and Immigration Serv-
21 ices shall establish procedures requiring a formal response to all rec-
22 ommendations submitted to the Director by the Ombudsman within 3
23 months after submission.

24 (g) OPERATION OF LOCAL OFFICES.—

25 (1) IN GENERAL.—Each local ombudsman—

26 (A) shall report to the Ombudsman or the delegate of the Om-
27 budsman;

28 (B) may consult with the appropriate supervisory personnel of
29 U.S. Citizenship and Immigration Services regarding the daily op-
30 eration of the local office of the Ombudsman;

31 (C) shall, at the initial meeting with an individual or employer
32 seeking the assistance of the local office, notify the individual or
33 employer that the local offices of the Ombudsman operate inde-
34 pendently of any other component of the Department and report
35 directly to Congress through the Ombudsman; and

36 (D) at the local ombudsman's discretion, may determine not to
37 disclose to U.S. Citizenship and Immigration Services contact
38 with, or information provided by, the individual or employer.

39 (2) MAINTENANCE OF INDEPENDENT COMMUNICATIONS.—Each local
40 office of the Ombudsman shall maintain a phone, facsimile, and other
41 means of electronic communication access, and a post office address,

1 that is separate from those maintained by U.S. Citizenship and Immi-
2 gration Services, or any component of U.S. Citizenship and Immigra-
3 tion Services.

4 **§ 11174. Professional responsibility and quality review**

5 (a) IN GENERAL.—The Director of U.S. Citizenship and Immigration
6 Services is responsible for—

7 (1) conducting investigations of noncriminal allegations of mis-
8 conduct, corruption, and fraud involving an employee of U.S. Citizen-
9 ship and Immigration Services that are not subject to investigation by
10 the Inspector General for the Department;

11 (2) inspecting the operations of U.S. Citizenship and Immigration
12 Services and providing assessments of the quality of the operations of
13 U.S. Citizenship and Immigration Services as a whole and each of its
14 components; and

15 (3) providing an analysis of the management of U.S. Citizenship and
16 Immigration Services.

17 (b) SPECIAL CONSIDERATIONS.—In providing assessments under sub-
18 section (a)(2) with respect to a decision of U.S. Citizenship and Immigra-
19 tion Services, or any of its components, consideration shall be given to—

20 (1) the accuracy of the findings of fact and conclusions of law used
21 in rendering the decision;

22 (2) fraud or misrepresentation associated with the decision; and

23 (3) the efficiency with which the decision was rendered.

24 **§ 11175. Employee discipline**

25 Notwithstanding another law, the Director of U.S. Citizenship and Immi-
26 gration Services may impose disciplinary action, including termination of
27 employment, pursuant to policies and procedures applicable to employees of
28 the Federal Bureau of Investigation, on an employee of U.S. Citizenship
29 and Immigration Services who willfully deceives Congress or agency leader-
30 ship on any matter.

31 **§ 11176. Transition**

32 (a) REFERENCES.—With respect to a function transferred by this sub-
33 chapter to, and exercised on or after March 1, 2003, by, the Director of
34 U.S. Citizenship and Immigration Services, a reference in any other Federal
35 law, Executive order, rule, regulation, delegation of authority, or document
36 of or pertaining to a component of government from which the function is
37 transferred—

38 (1) to the head of the component is deemed to refer to the Director
39 of U.S. Citizenship and Immigration Services; or

40 (2) to the component is deemed to refer to U.S. Citizenship and Im-
41 migration Services.

1 (b) EXERCISE OF AUTHORITIES.—Except as otherwise provided by law,
2 a Federal official to whom a function is transferred by this subchapter may,
3 for purposes of performing the function, exercise all authorities under any
4 other provision of law that were available with respect to the performance
5 of that function to the official responsible for the performance of the func-
6 tion immediately before March 1, 2003.

7 **§ 11177. Application of Internet-based technologies**

8 (a) ESTABLISHMENT OF TRACKING SYSTEM.—The Secretary, in consulta-
9 tion with the Technology Advisory Committee established under subsection
10 (c), shall establish an Internet-based system that will permit a person, em-
11 ployer, immigrant, or nonimmigrant who has filings with the Secretary for
12 a benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et
13 seq.), access to online information about the processing status of the filing
14 involved.

15 (b) FEASIBILITY STUDY FOR ONLINE FILING AND IMPROVED PROC-
16 ESSING.—

17 (1) ONLINE FILING.—The Secretary, in consultation with the Tech-
18 nology Advisory Committee established under subsection (c), shall con-
19 duct a feasibility study on the online filing of the filings described in
20 subsection (a). The study shall include a review of computerization and
21 technology of U.S. Immigration and Customs Enforcement relating to
22 immigration services and the processing of filings relating to immigrant
23 services. The study shall also include an estimate of the time frame and
24 cost and shall consider other factors in implementing the filing system,
25 including the feasibility of fee payment online.

26 (2) REPORT.—A report on the study under this subsection shall be
27 submitted to the Committees on the Judiciary of the House of Rep-
28 resentatives and the Senate not later than January 24, 2004.

29 (c) TECHNOLOGY ADVISORY COMMITTEE.—

30 (1) ESTABLISHMENT.—The Secretary shall establish the Technology
31 Advisory Committee to assist the Secretary in—

- 32 (A) establishing the tracking system under subsection (a); and
33 (B) conducting the study under subsection (b).

34 (2) CONSULTATION.—The Technology Advisory Committee shall be
35 established after consultation with the Committees on the Judiciary of
36 the House of Representatives and the Senate.

37 (3) COMPOSITION.—The Technology Advisory Committee shall be
38 composed of representatives from high technology companies capable of
39 establishing and implementing the tracking system described in sub-
40 section (a) in an expeditious manner, and representatives of persons

1 who may use the tracking system described in subsection (a) and the
2 online filing system described in subsection (b)(1).

3 **Subchapter V—General Immigration** 4 **Provisions**

5 **§ 11191. Director of Shared Services**

6 (a) IN GENERAL.—There is in the Office of the Deputy Secretary of
7 Homeland Security a Director of Shared Services.

8 (b) FUNCTIONS.—The Director of Shared Services is responsible for the
9 coordination of resources for U.S. Immigration and Customs Enforcement
10 and U.S. Citizenship and Immigration Services, including—

11 (1) information resources management, including computer data-
12 bases and information technology;

13 (2) records and file management; and

14 (3) forms management.

15 **§ 11192. Separation of funding**

16 (a) IN GENERAL.—There are in the Treasury separate accounts for ap-
17 propriated funds and other deposits available for U.S. Citizenship and Im-
18 migration Services and U.S. Immigration and Customs Enforcement.

19 (b) SEPARATE BUDGETS.—To ensure that U.S. Citizenship and Immigra-
20 tion Services and U.S. Immigration and Customs Enforcement are funded
21 to the extent necessary to fully carry out their respective functions, the Di-
22 rector of the Office of Management and Budget shall separate the budget
23 requests for each entity.

24 (c) FEES.—Fees imposed for a particular service, application, or benefit
25 shall be deposited in the account established under subsection (a) that is
26 for whichever of U.S. Immigration and Customs Enforcement or U.S. Citi-
27 zenship and Immigration Services has jurisdiction over the function to
28 which the fee relates.

29 (d) FEES NOT TRANSFERABLE.—A fee may not be transferred between
30 U.S. Citizenship and Immigration Services and U.S. Immigration and Cus-
31 toms Enforcement for purposes not authorized by section 286 of the Immi-
32 gration and Nationality Act (8 U.S.C. 1356).

33 **§ 11193. Annual immigration functions report**

34 (a) ANNUAL REPORT.—The Secretary shall submit a report annually to
35 the President, to the Committee on the Judiciary and the Committee on
36 Oversight and Government Reform of the House of Representatives, and to
37 the Committee on the Judiciary and the Committee on Homeland Security
38 and Governmental Affairs of the Senate, on the impact the transfers made
39 by Subtitle F of Title IV of the Homeland Security Act of 2002 (Public
40 Law 107–296, 116 Stat. 2205) have had on immigration functions.

1 (b) CONTENT.—The report shall address the following with respect to the
2 period covered by the report:

3 (1) The aggregate number of all immigration applications and peti-
4 tions received, and processed, by the Department.

5 (2) Region-by-region statistics on the aggregate number of immigra-
6 tion applications and petitions filed by an alien (or filed on behalf of
7 an alien) and denied, disaggregated by category of denial and applica-
8 tion or petition type.

9 (3) The quantity of backlogged immigration applications and peti-
10 tions that have been processed, the aggregate number awaiting proc-
11 essing, and a detailed plan for eliminating the backlog.

12 (4) The average processing period for immigration applications and
13 petitions, disaggregated by application or petition type.

14 (5) The number and types of immigration-related grievances filed
15 with an official of the Department of Justice, and if those grievances
16 were resolved.

17 (6) Plans to address grievances and improve immigration services.

18 (7) Whether immigration-related fees were used consistent with legal
19 requirements regarding their use.

20 (8) Whether immigration-related questions conveyed by customers to
21 the Department (whether conveyed in person, by telephone, or by
22 means of the Internet) were answered effectively and efficiently.

23 **Subchapter VI—U.S. Customs and Border** 24 **Protection Public-Private Partnerships**

25 **§ 11201. Definitions**

26 In this subchapter:

27 (1) DONOR.—The term “donor” means an entity that is proposing
28 to make a donation under this title (except chapters 113 and 409).

29 (2) ENTITY.—The term “entity” means—

30 (A) a person;

31 (B) a partnership, corporation, trust, estate, cooperative, asso-
32 ciation, or other organized group of persons;

33 (C) the Federal Government or a State or local government (in-
34 cluding a subdivision, agency, or instrumentality of the Federal
35 Government or a State or local government); or

36 (D) another private person or governmental entity.

37 **§ 11202. Fee agreements for certain services at ports of** 38 **entry**

39 (a) IN GENERAL.—Notwithstanding section 13031(e) of the Consolidated
40 Omnibus Budget Reconciliation Act of 1985 (19 U.S.C. 58c(e)) and section
41 451 of the Tariff Act of 1930 (19 U.S.C. 1451), the Commissioner of U.S.

1 Customs and Border Protection, on request of any entity, may enter into
2 a fee agreement with the entity under which—

3 (1) U. S. Customs and Border Protection shall provide services de-
4 scribed in subsection (b) at a United States port of entry or any other
5 facility at which U.S. Customs and Border Protection provides the
6 services;

7 (2) the entity shall remit to U.S. Customs and Border Protection a
8 fee imposed under subsection (h) in an amount equal to the full costs
9 that are incurred or will be incurred in providing the services; and

10 (3) if space is provided by the entity, each facility at which U.S.
11 Customs and Border Protection services are performed shall be main-
12 tained and equipped by the entity, without cost to the Federal Govern-
13 ment, in accordance with U.S. Customs and Border Protection speci-
14 fications.

15 (b) SERVICES DESCRIBED.—The services referred to in subsection (a) are
16 activities of an employee or Office of Field Operations contractor of U.S.
17 Customs and Border Protection (except employees of U.S. Border Patrol,
18 as established under section 10306(e) of this title) pertaining to, or in sup-
19 port of, customs, agricultural processing, border security, or immigration in-
20 spection-related matters at a port of entry or other facility at which U.S.
21 Customs and Border Protection provides or will provide the services.

22 (c) MODIFICATION OF PRIOR AGREEMENTS.—The Commissioner of U.S.
23 Customs and Border Protection, at the request of an entity that has pre-
24 viously entered into an agreement with U.S. Customs and Border Protection
25 for the reimbursement of fees in effect on December 16, 2016, may modify
26 the agreement to implement provisions of this section.

27 (d) LIMITATIONS.—

28 (1) IMPACTS OF SERVICES.—The Commissioner of U.S. Customs and
29 Border Protection—

30 (A) may enter into fee agreements under this section only for
31 services that—

32 (i) will increase or enhance the operational capacity of U.S.
33 Customs and Border Protection based on available staffing
34 and workload; and

35 (ii) will not shift the cost of services funded in an appro-
36 priations Act, or provided from an account in the Treasury
37 derived by the collection of fees, to entities under this title
38 (except chapters 113 and 409); and

39 (B) may not enter into a fee agreement under this section if the
40 agreement would unduly and permanently impact services funded

1 in an appropriations Act, or provided from an account in the
2 Treasury, derived by the collection of fees.

3 (2) NO LIMIT.—There shall be no limit to the number of fee agree-
4 ments that the Commissioner of U.S. Customs and Border Protection
5 may enter into under this section.

6 (e) AIR PORTS OF ENTRY.—

7 (1) IN GENERAL.—Except as otherwise provided in this subsection,
8 a fee agreement for U.S. Customs and Border Protection services at
9 an air port of entry may only provide for the payment of overtime costs
10 of U.S. Customs and Border Protection officers and salaries and ex-
11 penses of U.S. Customs and Border Protection employees to support
12 U.S. Customs and Border Protection officers in performing services de-
13 scribed in subsection (b).

14 (2) SMALL AIRPORTS.—Notwithstanding paragraph (1), U.S. Cus-
15 toms and Border Protection may receive reimbursement in addition to
16 overtime costs if the fee agreement is for services at an air port of
17 entry that has fewer than 100,000 arriving international passengers
18 annually.

19 (3) COVERED SERVICES.—In addition to costs described in para-
20 graph (1), a fee agreement for U.S. Customs and Border Protection
21 services at an air port of entry referred to in paragraph (2) may pro-
22 vide for the reimbursement of—

23 (A) salaries and expenses of not more than 5 fulltime equivalent
24 U.S. Customs and Border Protection officers beyond the number
25 of officers assigned to the port of entry on the date on which the
26 fee agreement was signed;

27 (B) salaries and expenses of employees of U.S. Customs and
28 Border Protection, other than the officers referred to in subpara-
29 graph (A), to support U.S. Customs and Border Protection offi-
30 cers in performing law enforcement functions; and

31 (C) other costs incurred by U.S. Customs and Border Protec-
32 tion relating to services described in subparagraph (B), such as
33 temporary placement or permanent relocation of employees, in-
34 cluding incentive pay for relocation, as appropriate.

35 (f) PORT OF ENTRY SIZE NOT A FACTOR.—The Commissioner of U.S.
36 Customs and Border Protection shall ensure that each fee agreement pro-
37 posal is given equal consideration regardless of the size of the port of entry.

38 (g) DENIED APPLICATION.—

39 (1) IN GENERAL.—If the Commissioner of U.S. Customs and Border
40 Protection denies a proposal for a fee agreement under this section, the

1 Commissioner shall provide the entity submitting the proposal with the
2 reason for the denial unless—

- 3 (A) the reason for the denial is law enforcement sensitive; or
4 (B) withholding the reason for the denial is in the national secu-
5 rity interests of the United States.

6 (2) JUDICIAL REVIEW.—Decisions of the Commissioner of U.S. Cus-
7 toms and Border Protection under paragraph (1) are in the discretion
8 of the Commissioner of U.S. Customs and Border Protection and are
9 not subject to judicial review.

10 (h) FEE.—

11 (1) IN GENERAL.—The amount of the fee to be charged under an
12 agreement authorized under subsection (a) shall be paid by each entity
13 requesting U.S. Customs and Border Protection services, and shall be
14 for the full cost of providing the services, including the salaries and ex-
15 penses of employees and contractors of U.S. Customs and Border Pro-
16 tection, to provide the services and other costs incurred by U.S. Cus-
17 toms and Border Protection relating to the services, such as temporary
18 or permanent relocation of the employees and contractors.

19 (2) TIMING.—The Commissioner of U.S. Customs and Border Pro-
20 tection may require that the fee referred to in paragraph (1) be paid
21 by each entity that has entered into a fee agreement under subsection
22 (a) with U.S. Customs and Border Protection in advance of the per-
23 formance of U.S. Customs and Border Protection services.

24 (3) OVERSIGHT.—The Commissioner of U.S. Customs and Border
25 Protection shall develop a process to oversee the services for which fees
26 are charged pursuant to an agreement under subsection (a), includ-
27 ing—

- 28 (A) a determination and report on the full costs of providing the
29 services, and a process for increasing the fees, as necessary;
30 (B) the establishment of a periodic remittance schedule to re-
31 plenish appropriations, accounts, or funds, as necessary; and
32 (C) the identification of costs paid by the fees.

33 (i) DEPOSIT OF FUNDS.—

34 (1) ACCOUNT.—Funds collected pursuant to an agreement entered
35 into pursuant to subsection (a)—

- 36 (A) shall be deposited as offsetting collections;
37 (B) shall remain available until expended without fiscal year
38 limitation; and
39 (C) shall be credited to the applicable appropriation, account, or
40 fund for the amount paid out of the appropriation, account, or
41 fund for any expenses incurred or to be incurred by U.S. Customs

1 and Border Protection in providing U.S. Customs and Border Pro-
2 tection services under the agreement and for any other costs in-
3 curred or to be incurred by U.S. Customs and Border Protection
4 relating to the services.

5 (2) RETURN OF UNUSED FUNDS.—The Commissioner of U.S. Cus-
6 toms and Border Protection shall return any unused funds collected
7 and deposited in the account described in paragraph (1) if a fee agree-
8 ment entered into pursuant to subsection (a) is terminated for any rea-
9 son or the terms of the fee agreement change by mutual agreement to
10 cause a reduction of U.S. Customs and Border Protection services. No
11 interest shall be owed on the return of the unused funds.

12 (j) TERMINATION.—

13 (1) IN GENERAL.—The Commissioner of U.S. Customs and Border
14 Protection shall terminate the services provided pursuant to a fee
15 agreement entered into under subsection (a) with an entity that, after
16 receiving notice from the Commissioner of U.S. Customs and Border
17 Protection that a fee under subsection (h) is due, fails to pay the fee
18 in a timely manner. If the services are terminated, all costs incurred
19 by U.S. Customs and Border Protection that have not been paid shall
20 become immediately due and payable. Interest on unpaid fees shall ac-
21 crue based on the rate and amount established under sections 6621
22 and 6622 of the Internal Revenue Code of 1986 (26 U.S.C. 6621,
23 6622).

24 (2) PENALTY.—An entity that, after notice and demand for payment
25 of a fee under subsection (h), fails to pay the fee in a timely manner
26 shall be liable for a penalty or liquidated damage equal to 2 times the
27 amount of the fee. The amount collected under this paragraph shall be
28 deposited into the appropriate account specified under subsection (i)
29 and shall be available as described in subsection (i).

30 (3) TERMINATION BY THE ENTITY.—An entity that has previously
31 entered into an agreement with U.S. Customs and Border Protection
32 for the reimbursement of fees in effect on December 16, 2016, or
33 under this section, may request that the agreement be amended to pro-
34 vide for termination on advance notice, length, and terms that are ne-
35 gotiated between the entity and U.S. Customs and Border Protection.

36 (k) ANNUAL REPORT.—The Commissioner of U.S. Customs and Border
37 Protection shall—

38 (1) submit an annual report identifying the activities undertaken and
39 the agreements entered into pursuant to this section to—

40 (A) the Committee on Appropriations of the Senate;

41 (B) the Committee on Finance of the Senate;

1 (C) the Committee on Homeland Security and Governmental Af-
2 fairs of the Senate;

3 (D) the Committee on the Judiciary of the Senate;

4 (E) the Committee on Appropriations of the House of Rep-
5 resentatives;

6 (F) the Committee on Homeland Security of the House of Rep-
7 resentatives;

8 (G) the Committee on the Judiciary of the House of Represent-
9 atives; and

10 (H) the Committee on Ways and Means of the House of Rep-
11 resentatives; and

12 (2) not later than 15 days before entering into a fee agreement, no-
13 tify the members of Congress who represent the State or congressional
14 district in which the affected port of entry or facility is located of the
15 agreement.

16 (l) RULE OF CONSTRUCTION.—Nothing in this section may be construed
17 as imposing on U.S. Customs and Border Protection any responsibilities,
18 duties, or authorities relating to real property.

19 **§ 11203. Port of entry donation authority**

20 (a) PERSONAL PROPERTY, MONEY, OR NONPERSONAL SERVICES.—

21 (1) IN GENERAL.—The Commissioner of U.S. Customs and Border
22 Protection, in consultation with the Administrator of General Services,
23 may enter into an agreement with an entity to accept a donation of
24 personal property, money, or nonpersonal services for the uses de-
25 scribed in paragraph (3) only with respect to the following locations at
26 which U.S. Customs and Border Protection performs or will be per-
27 forming inspection services:

28 (A) A new or existing sea or air port of entry.

29 (B) An existing Federal Government-owned or -leased land port
30 of entry.

31 (C) A new Federal Government-owned or -leased land port of
32 entry if—

33 (i) the fair market value of the donation is \$75,000,000 or
34 less; and

35 (ii) the fair market value of donations with respect to the
36 land port of entry total \$75,000,000 or less over the pre-
37 ceding 5 years.

38 (2) LIMITATION ON MONETARY DONATIONS.—A monetary donation
39 accepted pursuant to this subsection may not be used to pay the sala-
40 ries of U.S. Customs and Border Protection employees performing in-
41 spection services.

1 (3) USES.—Donations accepted pursuant to this subsection may be
2 used for activities of the Office of Field Operations, set forth in sub-
3 paragraphs (A) through (F) of section 10306(g)(3) of this title, that
4 are related to a new or existing sea or air port of entry or a new or
5 existing Federal Government-owned or -leased land port of entry de-
6 scribed in paragraph (1), including expenses relating to—

7 (A) furniture, fixtures, equipment, or technology, including the
8 installation or deployment of those items; and

9 (B) the operation and maintenance of the furniture, fixtures,
10 equipment, or technology.

11 (b) REAL PROPERTY OR MONEY.—

12 (1) IN GENERAL.—Subject to paragraph (3), the Commissioner of
13 U.S. Customs and Border Protection, and the Administrator of General
14 Services, as applicable, may enter into an agreement with an entity to
15 accept a donation of real property or money for uses described in para-
16 graph (2) only with respect to the following locations at which U.S.
17 Customs and Border Protection performs or will be performing inspec-
18 tion services:

19 (A) A new or existing sea or air port of entry.

20 (B) An existing Federal Government-owned land port of entry.

21 (C) A new Federal Government-owned land port of entry if—

22 (i) the fair market value of the donation is \$75,000,000 or
23 less; and

24 (ii) the fair market value with respect to the land port of
25 entry total \$75,000,000 or less over the preceding 5 years.

26 (2) USES.—Donations accepted pursuant to this subsection may be
27 used for activities of the Office of Field Operations set forth in section
28 10306(g) of this title that are related to the construction, alteration,
29 operation, or maintenance of a new or existing sea or air port of entry
30 or a new or existing Federal Government-owned land port of entry de-
31 scribed in paragraph (1), including expenses related to—

32 (A) land acquisition, design, construction, repair, or alteration;
33 and

34 (B) operation and maintenance of the port of entry facility.

35 (3) LIMITATION ON REAL PROPERTY DONATIONS.—A donation of
36 real property under this subsection at an existing land port of entry
37 owned by the General Services Administration may only be accepted by
38 the Administrator of General Services.

39 (4) SUNSET.—

40 (A) IN GENERAL.—The authority to enter into an agreement
41 under this subsection shall terminate on December 31, 2026.

1 (B) RULE OF CONSTRUCTION.—The termination date referred
2 to in subparagraph (A) shall not apply to a proposal accepted for
3 consideration by U.S. Customs and Border Protection or the Gen-
4 eral Services Administration pursuant to this section or a prior
5 pilot program prior to December 31, 2026.

6 (c) GENERAL PROVISIONS.—

7 (1) DURATION.—An agreement entered into under subsection (a) or
8 (b) (and in the case of subsection (b), in accordance with paragraph
9 (4) of subsection (b)) may last as long as required to meet the terms
10 of the agreement.

11 (2) CRITERIA.—In carrying out an agreement entered into under
12 subsection (a) or (b), the Commissioner of U.S. Customs and Border
13 Protection, in consultation with the Administrator of General Services,
14 shall establish criteria regarding—

15 (A) the selection and evaluation of donors;

16 (B) the identification of roles and responsibilities between U.S.
17 Customs and Border Protection, the General Services Administra-
18 tion, and donors;

19 (C) the identification, allocation, and management of explicit
20 and implicit risks of partnering between the Federal Government
21 and donors;

22 (D) decision-making and dispute resolution processes; and

23 (E) processes for U.S. Customs and Border Protection, and the
24 General Services Administration, as applicable, to terminate agree-
25 ments if selected donors are not meeting the terms of the agree-
26 ment, including the security standards established by U.S. Cus-
27 toms and Border Protection.

28 (3) EVALUATION PROCEDURES.—

29 (A) IN GENERAL.—The Commissioner of U.S. Customs and
30 Border Protection, in consultation with the Administrator of Gen-
31 eral Services, as applicable, shall—

32 (i) establish criteria for evaluating a proposal to enter into
33 an agreement under subsection (a) or (b); and

34 (ii) make the criteria publicly available.

35 (B) CONSIDERATIONS.—Criteria established pursuant to sub-
36 paragraph (A) shall consider—

37 (i) the impact of a proposal referred to in subparagraph
38 (A) on the land, sea, or air port of entry at issue and other
39 ports of entry or similar facilities or other infrastructure near
40 the location of the proposed donation;

- 1 (ii) the proposal’s potential to increase trade and travel ef-
2 ficiency through added capacity;
- 3 (iii) the proposal’s potential to enhance the security of the
4 port of entry at issue;
- 5 (iv) the impact of the proposal on reducing wait times at
6 the port of entry or facility and other ports of entry on the
7 same border;
- 8 (v) for a donation under subsection (b)—
9 (I) whether the donation satisfies the requirements of
10 the proposal or whether additional real property would
11 be required; and
12 (II) how the donation was acquired, including if emi-
13 nent domain was used;
- 14 (vi) the funding available to complete the intended use of
15 the donation;
- 16 (vii) the costs of maintaining and operating the donation;
- 17 (viii) the impact of the proposal on U.S. Customs and Bor-
18 der Protection staffing requirements; and
- 19 (ix) other factors that the Commissioner of U.S. Customs
20 and Border Protection or the Administrator of General Serv-
21 ices determines to be relevant.

22 (C) DETERMINATION AND NOTIFICATION.—

- 23 (i) INCOMPLETE PROPOSALS.—
24 (I) IN GENERAL.—Not later than 60 days after receiv-
25 ing the proposals for a donation agreement from an enti-
26 ty, the Commissioner of U.S. Customs and Border Pro-
27 tection shall notify the entity as to whether the proposal
28 is complete or incomplete.
- 29 (II) RESUBMISSION.—If the Commissioner of U.S.
30 Customs and Border Protection determines that a pro-
31 posal is incomplete, the Commissioner shall—
32 (aa) notify the appropriate entity and provide the
33 entity with a description of all information or mate-
34 rial that is needed to complete review of the pro-
35 posal; and
36 (bb) allow the entity to resubmit the proposal
37 with additional information and material described
38 in item (aa) to complete the proposal.
- 39 (ii) COMPLETE PROPOSAL.—Not later than 180 days after
40 receiving a completed proposal to enter into an agreement
41 under subsection (a) or (b), the Commissioner of U.S. Cus-

1 toms and Border Protection, with the concurrence of the Ad-
2 ministrator of General Services, as applicable, shall—

3 (I) determine whether to approve or deny the proposal;

4 and

5 (II) notify the entity that submitted the proposal of
6 the determination.

7 (4) SUPPLEMENTAL FUNDING.—Except as required under section
8 3307 of title 40, real property donations to the Administrator of Gen-
9 eral Services made pursuant to subsection (b) at a GSA-owned land
10 port of entry may be used in addition to any other funding for the port
11 of entry, including appropriated funds, property, or services.

12 (5) RETURN OF DONATIONS.—The Commissioner of U.S. Customs
13 and Border Protection, or the Administrator of General Services, as
14 applicable, may return a donation made pursuant to subsection (a) or
15 (b). No interest shall be owed to the donor with respect to any donation
16 provided under subsection (a) or (b) that is returned pursuant to this
17 subsection.

18 (6) PROHIBITION ON CERTAIN FUNDING.—

19 (A) IN GENERAL.—Except as provided in subsections (a) and
20 (b) regarding the acceptance of donations, the Commissioner of
21 U.S. Customs and Border Protection and the Administrator of
22 General Services, as applicable, may not, with respect to an agree-
23 ment entered into under subsection (a) or (b), obligate or expend
24 amounts in excess of amounts that have been appropriated pursu-
25 ant to any appropriations Act for purposes specified in subsection
26 (a) or (b) or otherwise made available for those purposes.

27 (B) CERTIFICATION REQUIREMENT.—Before accepting any do-
28 nations pursuant to an agreement under subsection (a) or (b), the
29 Commissioner of U.S. Customs and Border Protection shall certify
30 to the congressional committees set forth in paragraph (7) that—

31 (i) the donation will not be used for the construction of a
32 detention facility or a border fence or wall; or

33 (ii) the donor will be notified in the Donations Acceptance
34 Agreement that the donor shall be financially responsible for
35 all costs and operating expenses related to the operation,
36 maintenance, and repair of the donated real property until
37 such time as U.S. Customs and Border Protection provides
38 the donor written notice otherwise.

39 (7) REPORTS BY COMMISSIONER OF U.S. CUSTOMS AND BORDER
40 PROTECTION AND ADMINISTRATOR OF GENERAL SERVICES.—The Com-
41 missioner of U.S. Customs and Border Protection, in collaboration with

1 the Administrator of General Services, as applicable, shall submit an
2 annual report identifying the activities undertaken and agreements en-
3 tered into pursuant to subsections (a) and (b) to—

- 4 (A) the Committee on Appropriations of the Senate;
5 (B) the Committee on Environment and Public Works of the
6 Senate;
7 (C) the Committee on Finance of the Senate;
8 (D) the Committee on Homeland Security and Governmental
9 Affairs of the Senate;
10 (E) the Committee on the Judiciary of the Senate;
11 (F) the Committee on Appropriations of the House of Rep-
12 resentatives;
13 (G) the Committee on Homeland Security of the House of Rep-
14 resentatives;
15 (H) the Committee on the Judiciary of the House of Represent-
16 atives;
17 (I) the Committee on Transportation and Infrastructure of the
18 House of Representatives; and
19 (J) the Committee on Ways and Means of the House of Rep-
20 resentatives.

21 (d) REPORT BY COMPTROLLER GENERAL.—The Comptroller General
22 shall submit a biennial report to the congressional committees referred to
23 in subsection (c)(7) that evaluates—

- 24 (1) fee agreements entered into pursuant to section 11202 of this
25 title;
26 (2) donation agreements entered into pursuant to subsections (a)
27 and (b); and
28 (3) the fees and donations received by U. S. Customs and Border
29 Protection pursuant to the agreements.

30 (e) JUDICIAL REVIEW.—Decisions of the Commissioner of U.S. Customs
31 and Border Protection and the Administrator of General Services under this
32 section regarding the acceptance of real or personal property are in the dis-
33 cretion of the Commissioner of U.S. Customs and Border Protection and
34 the Administrator of General Services, and are not subject to judicial re-
35 view.

36 (f) RULE OF CONSTRUCTION.—Except as otherwise provided in this sec-
37 tion, nothing in this section may be construed as affecting in any manner
38 the responsibilities, duties, or authorities of U.S. Customs and Border Pro-
39 tection or the General Services Administration.

1 **§ 11204. Current and proposed agreements**

2 Nothing in this subchapter or in section 4 of the Cross-Border Trade En-
3 hancement Act of 2016 (Public Law 114–279, 130 Stat. 1422) may be con-
4 strued as affecting—

5 (1) any agreement entered into pursuant to section 560 of the De-
6 partment of Homeland Security Appropriations Act, 2013 (Public Law
7 113–6, 127 Stat. 378) or section 559 of the Department of Homeland
8 Security Appropriations Act, 2014 (Public Law 113–76, 128 Stat. 279)
9 as in existence on December 15, 2016, and the agreement shall con-
10 continue to have full force and effect on and after December 15, 2016;
11 or

12 (2) a proposal accepted for consideration by U.S. Customs and Bor-
13 der Protection pursuant to section 559 of the Department of Homeland
14 Security Appropriations Act, 2014 (Public Law 113–76, 128 Stat. 279)
15 as in existence on December 15, 2016.

16 **Subchapter VII—Miscellaneous Provisions**

17 **§ 11211. Coordination of information and information tech-**
18 **nology**

19 (a) DEFINITION OF AFFECTED AGENCY.—In this section, the term “af-
20 fected agency” means—

21 (1) the Department;

22 (2) the Department of Agriculture;

23 (3) the Department of Health and Human Services; and

24 (4) any other department or agency determined to be appropriate by
25 the Secretary.

26 (b) COORDINATION.—The Secretary, in coordination with the Secretary of
27 Agriculture, the Secretary of Health and Human Services, and the head of
28 each other department or agency determined to be appropriate by the Sec-
29 retary, shall ensure that appropriate information (as determined by the Sec-
30 retary) concerning inspections of articles that are imported or entered into
31 the United States, and are inspected or regulated by one or more affected
32 agencies, is timely and efficiently exchanged between the affected agencies.

33 **§ 11212. Visa issuance**

34 (a) DEFINITION OF CONSULAR OFFICER.—In this section, the term “con-
35 sular officer” has the meaning given the term under section 101(a) of the
36 Immigration and Nationality Act (8 U.S.C. 1101(a)).

37 (b) IN GENERAL.—Notwithstanding section 104(a) of the Immigration
38 and Nationality Act (8 U.S.C. 1104(a)) or any other law, and except as pro-
39 vided in subsection (c) of this section, the Secretary—

40 (1) shall be vested exclusively with all authorities to issue regulations
41 with respect to, to administer, and to enforce the Immigration and Na-

1 tionality Act (8 U.S.C. 1101 et seq.), and of all other immigration and
2 nationality laws, relating to the functions of consular officers of the
3 United States in connection with the granting or refusal of visas, and
4 shall have the authority to refuse visas in accordance with law and to
5 develop programs of homeland security training for consular officers (in
6 addition to consular training provided by the Secretary of State), which
7 authorities shall be exercised through the Secretary of State, except
8 that the Secretary shall not have authority to alter or reverse the deci-
9 sion of a consular officer to refuse a visa to an alien; and

10 (2) shall have authority to confer or impose upon an officer or em-
11 ployee of the United States, with the consent of the head of the execu-
12 tive agency under whose jurisdiction the officer or employee is serving,
13 any of the functions specified in paragraph (1).

14 (c) AUTHORITY OF THE SECRETARY OF STATE.—

15 (1) IN GENERAL.—Notwithstanding subsection (b), the Secretary of
16 State may direct a consular officer to refuse a visa to an alien if the
17 Secretary of State deems the refusal necessary or advisable in the for-
18 eign policy or security interests of the United States.

19 (2) CONSTRUCTION REGARDING AUTHORITY.—Nothing in this sec-
20 tion, consistent with the Secretary of Homeland Security’s authority to
21 refuse visas in accordance with law, shall be construed as affecting the
22 authorities of the Secretary of State under the following provisions of
23 law:

24 (A) Section 101(a)(15)(A) of the Immigration and Nationality
25 Act (8 U.S.C. 1101(a)(15)(A)).

26 (B) Section 204(d)(2) of the Immigration and Nationality Act
27 (8 U.S.C. 1154(d)(2)) (as it will take effect upon the entry into
28 force of the Convention on Protection of Children and Cooperation
29 in Respect to Inter-Country adoption).

30 (C) Section 212(a)(3)(B)(i)(IV)(bb) of the Immigration and Na-
31 tionality Act (8 U.S.C. 1182(a)(3)(B)(i)(IV)(bb)).

32 (D) Section 212(a)(3)(B)(i)(VI) of the Immigration and Nation-
33 ality Act (8 U.S.C. 1182(a)(3)(B)(i)(VI)).

34 (E) Section 212(a)(3)(B)(vi)(II) of the Immigration and Na-
35 tionality Act (8 U.S.C. 1182(a)(3)(B)(vi)(II)).

36 (F) Section 212(a)(3)(C) of the Immigration and Nationality
37 Act (8 U.S.C. 1182(a)(3)(C)).

38 (G) Section 212(a)(10)(C) of the Immigration and Nationality
39 Act (8 U.S.C. 1182(a)(10)(C)).

40 (H) Section 212(f) of the Immigration and Nationality Act (8
41 U.S.C. 1182(f)).

1 (I) Section 801 of the Admiral James W. Nance and Meg Dono-
2 van Foreign Relations Authorization Act, Fiscal Years 2000 and
3 2001 (8 U.S.C. 1182e).

4 (J) Section 219(a) of the Immigration and Nationality Act (8
5 U.S.C. 1189(a)).

6 (K) Section 237(a)(4)(C) of the Immigration and Nationality
7 Act (8 U.S.C. 1227(a)(4)(C)).

8 (L) Section 51 of the State Department Basic Authorities Act
9 of 1956 (22 U.S.C. 2723).

10 (M) Section 401 of the Cuban Liberty and Democratic Soli-
11 darity (LIBERTAD) Act of 1996 (22 U.S.C. 6091).

12 (N) Section 103(f) of the Chemical Weapons Convention Imple-
13 mentation Act of 1998 (22 U.S.C. 6713(f)).

14 (O) Section 616 of the Departments of Commerce, Justice, and
15 State, the Judiciary, and Related Agencies Appropriations Act,
16 1999 (section 101(b) of division A of the Omnibus Consolidated
17 and Emergency Supplemental Appropriations Act, 1999, Public
18 Law 105–277, 112 Stat. 2681–114).

19 (P) Section 568 of the Foreign Operations, Export Financing,
20 and Related Programs Appropriations Act, 2002 (Public Law
21 107–115, 115 Stat. 2166).

22 (d) CONSULAR OFFICERS AND CHIEFS OF MISSIONS.—

23 (1) IN GENERAL.—Nothing in this section may be construed to alter
24 or affect—

25 (A) the employment status of consular officers as employees of
26 the Department of State; or

27 (B) the authority of a chief of mission under section 207 of the
28 Foreign Service Act of 1980 (22 U.S.C. 3927).

29 (2) CONSTRUCTION REGARDING DELEGATION OF AUTHORITY.—

30 Nothing in this section shall be construed to affect any delegation of
31 authority to the Secretary of State by the President pursuant to any
32 proclamation issued under section 212(f) of the Immigration and Na-
33 tionality Act (8 U.S.C. 1182(f)), consistent with the Secretary of
34 Homeland Security’s authority to refuse visas in accordance with law.

35 (e) ASSIGNMENT OF DEPARTMENT EMPLOYEES TO DIPLOMATIC AND
36 CONSULAR POSTS.—

37 (1) IN GENERAL.—The Secretary may assign employees of the De-
38 partment to each diplomatic and consular post at which visas are
39 issued, unless the Secretary determines that an assignment at a par-
40 ticular post would not promote homeland security.

41 (2) FUNCTIONS.—Employees assigned under paragraph (1) shall—

1 (A) provide expert advice and training to consular officers re-
2 garding specific security threats relating to the adjudication of in-
3 dividual visa applications or classes of applications;

4 (B) review applications, either on the initiative of the employee
5 of the Department or upon request by a consular officer or other
6 person charged with adjudicating applications; and

7 (C) conduct investigations with respect to consular matters
8 under the jurisdiction of the Secretary.

9 (3) EVALUATION OF CONSULAR OFFICERS.—The Secretary of State
10 shall evaluate, in consultation with the Secretary, as considered appro-
11 priate by the Secretary, the performance of consular officers with re-
12 spect to the processing and adjudication of applications for visas in ac-
13 cordance with performance standards developed by the Secretary for
14 these procedures.

15 (4) REPORT.—The Secretary shall, on an annual basis, submit a re-
16 port to Congress that describes the basis for each determination under
17 paragraph (1) that the assignment of an employee of the Department
18 at a particular diplomatic post would not promote homeland security.

19 (5) PERMANENT ASSIGNMENT; PARTICIPATION IN TERRORIST LOOK-
20 OUT COMMITTEE.—When appropriate, employees of the Department as-
21 signed to perform functions described in paragraph (2) may be as-
22 signed permanently to overseas diplomatic or consular posts with coun-
23 try-specific or regional responsibility. If the Secretary so directs, an
24 employee, when present at an overseas post, shall participate in the ter-
25 rorist lookout committee established under section 304 of the Enhanced
26 Border Security and Visa Entry Reform Act of 2002 (8 U.S.C. 1733).

27 (6) TRAINING AND HIRING.—

28 (A) IN GENERAL.—The Secretary shall ensure, to the extent
29 possible, that employees of the Department assigned to perform
30 functions under paragraph (2) and, as appropriate, consular offi-
31 cers, shall be provided the necessary training to enable them to
32 carry out the functions, including training in foreign languages,
33 interview techniques, and fraud detection techniques, in conditions
34 in the particular country where each employee is assigned, and in
35 other appropriate areas of study.

36 (B) USE OF CENTER.—The Secretary may use the George P.
37 Shultz National Foreign Affairs Training Center, on a reimburs-
38 able basis, to obtain the training described in subparagraph (A).

39 (f) NO CREATION OF PRIVATE RIGHT OF ACTION.—Nothing in this sec-
40 tion shall be construed to create or authorize a private right of action to

1 challenge a decision of a consular officer or other United States official or
2 employee to grant or deny a visa.

3 (g) VISA ISSUANCE PROGRAM FOR SAUDI ARABIA.—On-site personnel of
4 the Department shall review all visa applications for Saudi Arabia prior to
5 adjudication.

6 **§ 11213. Information on visa denials required to be entered**
7 **into electronic data system**

8 (a) IN GENERAL.—Whenever a consular officer of the United States de-
9 nies a visa to an applicant, the consular officer shall enter the fact and the
10 basis of the denial and the name of the applicant into the interoperable elec-
11 tronic data system implemented under section 202(a) of the Enhanced Bor-
12 der Security and Visa Entry Reform Act of 2002 (8 U.S.C. 1722(a)).

13 (b) PROHIBITION.—In the case of an alien with respect to whom a visa
14 has been denied under subsection (a)—

15 (1) no subsequent visa may be issued to the alien unless the consular
16 officer considering the alien’s visa application has reviewed the infor-
17 mation concerning the alien placed in the interoperable electronic data
18 system, has indicated on the alien’s application that the information
19 has been reviewed, and has stated for the record why the visa is being
20 issued or a waiver of visa ineligibility recommended in spite of that in-
21 formation; and

22 (2) the alien may not be admitted to the United States without a
23 visa issued in accordance with the procedures described in paragraph
24 (1).

25 **§ 11214. Purpose and responsibilities of Office of Cargo Se-**
26 **curity Policy**

27 (a) PURPOSES.—The Office of Cargo Security Policy—

28 (1) coordinates all Department policies relating to cargo security;
29 and

30 (2) consults with stakeholders and coordinates with other Federal
31 agencies in the establishment of standards and regulations and the pro-
32 motion of best practices.

33 (b) RESPONSIBILITIES OF DIRECTOR.—The Director of the Office of
34 Cargo Security Policy—

35 (1) advises the Assistant Secretary for Policy in the development of
36 Department-wide policies regarding cargo security;

37 (2) coordinates all policies relating to cargo security among the agen-
38 cies and offices within the Department relating to cargo security; and

39 (3) coordinates the cargo security policies of the Department with
40 the policies of other executive agencies.

1 (c) RELATIONSHIP WITH COAST GUARD.—Nothing in this section shall be
2 construed to affect—

3 (1) the authorities, functions, or capabilities of the Coast Guard to
4 perform its missions; or

5 (2) the requirement under section 10312 of this title that those au-
6 thorities, functions, and capabilities be maintained intact.

7 **§ 11215. Purpose, composition, and operation of Border En-**
8 **forcement Security Task Force**

9 (a) PURPOSE.—The purpose of the Border Enforcement Security Task
10 Force (in this section referred to as “BEST”) is to establish units to en-
11 hance border security by addressing and reducing border security threats
12 and violence by—

13 (1) facilitating collaboration among Federal, State, local, tribal, and
14 foreign law enforcement agencies to execute coordinated activities in
15 furtherance of border security, and homeland security; and

16 (2) enhancing information sharing, including the dissemination of
17 homeland security information among these agencies.

18 (b) COMPOSITION AND ESTABLISHMENT OF UNITS.—

19 (1) COMPOSITION.—BEST units may be comprised of personnel
20 from—

21 (A) U.S. Immigration and Customs Enforcement;

22 (B) U.S. Customs and Border Protection;

23 (C) the Coast Guard;

24 (D) other Department personnel, as appropriate;

25 (E) other Federal agencies, as appropriate;

26 (F) appropriate State law enforcement agencies;

27 (G) foreign law enforcement agencies, as appropriate;

28 (H) local law enforcement agencies from affected border cities
29 and communities; and

30 (I) appropriate tribal law enforcement agencies.

31 (2) ESTABLISHMENT.—The Secretary may establish BEST units in
32 jurisdictions in which the units can contribute to BEST missions, as
33 appropriate. Before establishing a BEST unit, the Secretary shall con-
34 sider—

35 (A) whether the area in which the BEST unit would be estab-
36 lished is significantly impacted by cross-border threats;

37 (B) the availability of Federal, State, local, tribal, and foreign
38 law enforcement resources to participate in the BEST unit;

39 (C) the extent to which border security threats are having a sig-
40 nificant harmful impact in the jurisdiction in which the BEST

1 unit is to be established, and in other jurisdictions in the country;
2 and

3 (D) whether or not an Integrated Border Enforcement Team al-
4 ready exists in the area in which the BEST unit would be estab-
5 lished.

6 (3) DUPLICATION OF EFFORTS.—In determining whether to establish
7 a new BEST unit or to expand an existing BEST unit in a given juris-
8 diction, the Secretary shall ensure that the BEST unit under consider-
9 ation does not duplicate the efforts of other existing interagency task
10 forces or centers within that jurisdiction.

11 (c) OPERATION.—After determining the jurisdictions in which to establish
12 BEST units under subsection (b)(2), and in order to provide Federal assist-
13 ance to the jurisdictions, the Secretary may—

14 (1) direct the assignment of Federal personnel to BEST, subject to
15 the approval of the head of the department or agency that employs
16 such personnel; and

17 (2) take other actions to assist Federal, State, local, and tribal enti-
18 ties to participate in BEST, including providing financial assistance, as
19 appropriate, for operational, administrative, salary reimbursement, and
20 technological costs associated with the participation of Federal, State,
21 local, and tribal law enforcement agencies in BEST

22 (d) REPORT.—Not later than June 6, 2017, and 2018, the Secretary
23 shall submit a report to Congress that describes the effectiveness of BEST
24 in enhancing border security and reducing the drug trafficking, arms smug-
25 gling, illegal alien trafficking and smuggling, violence, and kidnapping along
26 and across the international borders of the United States, as measured by
27 crime statistics, including violent deaths, incidents of violence, and drug-re-
28 lated arrests.

29 **§ 11216. Cyber Crimes Center**

30 (a) IN GENERAL.—

31 (1) ESTABLISHMENT.—The Secretary shall operate, in U.S. Immig-
32 ration and Customs Enforcement, Homeland Security Investigations,
33 a Cyber Crimes Center (in this section referred to as the “Center”).

34 (2) PURPOSE.—The Center shall provide investigative assistance,
35 training, and equipment to support domestic and international inves-
36 tigations of cyber-related crimes by the Department.

37 (b) CHILD EXPLOITATION INVESTIGATIONS UNIT

38 (1) IN GENERAL.—The Secretary shall operate, in the Center, a
39 Child Exploitation Investigations Unit (in this subsection referred to as
40 the “CEIU”).

41 (2) FUNCTIONS.—The CEIU—

1 (A) shall coordinate all U.S. Immigration and Customs Enforce-
2 ment child exploitation initiatives, including investigations into—
3 (i) child exploitation;
4 (ii) child pornography;
5 (iii) child victim identification;
6 (iv) traveling child sex offenders; and
7 (v) forced child labor, including the sexual exploitation of
8 minors;

9 (B) shall, among other things, focus on—
10 (i) child exploitation prevention;
11 (ii) investigative capacity building;
12 (iii) enforcement operations; and
13 (iv) training for Federal, State, local, tribal, and foreign
14 law enforcement agency personnel, on request;

15 (C) shall provide training, technical expertise, support, or co-
16 ordination of child exploitation investigations, as needed, to co-
17 operating law enforcement agencies and personnel, which shall in-
18 clude participating in training for Homeland Security Investiga-
19 tions personnel conducted by Internet Crimes Against Children
20 Task Force;

21 (D) shall provide psychological support and counseling services
22 for U.S. Immigration and Customs Enforcement personnel en-
23 gaged in child exploitation prevention initiatives, including making
24 available other existing services to assist employees who are ex-
25 posed to child exploitation material during investigations;

26 (E) may collaborate with the Department of Defense and the
27 National Association to Protect Children for the purpose of the re-
28 cruiting, training, equipping and hiring of wounded, ill, and in-
29 jured veterans and transitioning service members, through the
30 Human Exploitation Rescue Operative (HERO) Child-Rescue
31 Corps Program; and

32 (F) shall collaborate with other governmental, nongovernmental,
33 and nonprofit entities approved by the Secretary for the sponsor-
34 ship of, and participation in, outreach and training activities.

35 (3) DATA COLLECTION.—The CEIU shall collect and maintain data
36 concerning—

37 (A) the total number of suspects identified by U.S. Immigration
38 and Customs Enforcement;

39 (B) the number of arrests by U.S. Immigration and Customs
40 Enforcement in child exploitation investigations, disaggregated by
41 type, including—

1 (i) the number of child victims identified through investiga-
2 tions carried out by U.S. Immigration and Customs Enforce-
3 ment; and

4 (ii) the number of suspects arrested who were in positions
5 of trust or authority over children;

6 (C) the number of child exploitation cases opened for investiga-
7 tion by U.S. Immigration and Customs Enforcement; and

8 (D) the number of child exploitation cases resulting in a Fed-
9 eral, State, foreign, or military prosecution.

10 (4) AVAILABILITY OF DATA TO CONGRESS.—In addition to submit-
11 ting the reports required under paragraph (7), the CEIU shall make
12 the data collected and maintained under paragraph (3) available to the
13 committees of Congress described in paragraph (7).

14 (5) COOPERATIVE AGREEMENTS.—The CEIU may enter into cooper-
15 ative agreements to accomplish the functions set forth in paragraphs
16 (2) and (3).

17 (6) ACCEPTANCE OF GIFTS.—

18 (A) IN GENERAL.—The Secretary may accept money and in-
19 kind donations from the Virtual Global Taskforce, national labora-
20 tories, Federal agencies, not-for-profit organizations, and edu-
21 cational institutions to create and expand public awareness cam-
22 paigns in support of the functions of the CEIU.

23 (B) EXEMPTION FROM FEDERAL ACQUISITION REGULATION.—
24 Gifts authorized under subparagraph (A) are not subject to the
25 Federal Acquisition Regulation for competition when the services
26 provided by the entities referred to in subparagraph (A) are do-
27 nated or of minimal cost to the Department.

28 (7) REPORTS.—Not later than May 29, 2017, 2018, 2019, and
29 2020, the CEIU shall—

30 (A) submit a report containing a summary of the data collected
31 pursuant to paragraph (3) during the previous year to—

32 (i) the Committee on Homeland Security and Govern-
33 mental Affairs of the Senate;

34 (ii) the Committee on the Judiciary of the Senate;

35 (iii) the Committee on Appropriations of the Senate;

36 (iv) the Committee on Homeland Security of the House of
37 Representatives;

38 (v) the Committee on the Judiciary of the House of Rep-
39 resentatives; and

40 (vi) the Committee on Appropriations of the House of Rep-
41 resentatives; and

1 (B) make a copy of each report submitted under subparagraph
2 (A) publicly available on the website of the Department.

3 (e) COMPUTER FORENSICS UNIT.—

4 (1) IN GENERAL.—The Secretary shall operate, in the Center, a
5 Computer Forensics Unit (in this subsection referred to as the
6 “CFU”).

7 (2) FUNCTIONS.—The CFU—

8 (A) shall provide training and technical support in digital
9 forensics and administer the Digital Forensics and Document and
10 Media Exploitation program to—

11 (i) U.S. Immigration and Customs Enforcement personnel;
12 and

13 (ii) Federal, State, local, tribal, military, and foreign law
14 enforcement agency personnel engaged in the investigation of
15 crimes within their respective jurisdictions, on request and
16 subject to the availability of funds;

17 (B) shall provide computer hardware, software, and forensic li-
18 censes for all computer forensics personnel in U.S. Immigration
19 and Customs Enforcement;

20 (C) shall participate in research and development in the area of
21 digital forensics and emerging technologies, in coordination with
22 appropriate components of the Department; and

23 (D) may collaborate with the Department of Defense, the Na-
24 tional Association to Protect Children, and other governmental en-
25 tities for the purpose of recruiting, training, equipping, and hiring
26 wounded, ill, and injured veterans and transitioning service mem-
27 bers, through the Human Exploitation Rescue Operative (HERO)
28 Child-Rescue Corps Program.

29 (3) COOPERATIVE AGREEMENTS.—The CFU may enter into coopera-
30 tive agreements to accomplish the functions set forth in paragraph (2).

31 (4) ACCEPTANCE OF GIFTS.—

32 (A) IN GENERAL.—The Secretary may accept money and in-
33 kind donations from the Virtual Global Task Force, national lab-
34 oratories, Federal agencies, not-for-profit organizations, and edu-
35 cational institutions to create and expand public awareness cam-
36 paigns in support of the functions of the CFU.

37 (B) EXEMPTION FROM FEDERAL ACQUISITION REGULATION.—
38 Gifts authorized under subparagraph (A) are not subject to the
39 Federal Acquisition Regulation for competition when the services
40 provided by the entities referred to in subparagraph (A) are do-
41 nated or of minimal cost to the Department.

1 (d) CYBER CRIMES UNIT.—

2 (1) IN GENERAL.—The Secretary shall operate, in the Center, a
3 Cyber Crimes Unit (in this subsection referred to as the “CCU”).

4 (2) FUNCTIONS.—The CCU—

5 (A) shall oversee the cyber security strategy and cyber-related
6 operations and programs for U.S. Immigration and Customs En-
7 forcement;

8 (B) shall enhance U.S. Immigration and Customs Enforce-
9 ment’s ability to combat criminal enterprises operating on or
10 through the Internet, with specific focus in the areas of—

11 (i) cyber economic crime;

12 (ii) digital theft of intellectual property;

13 (iii) illicit e-commerce (including hidden marketplaces);

14 (iv) Internet-facilitated proliferation of arms and strategic
15 technology; and

16 (v) cyber-enabled smuggling and money laundering;

17 (C) shall provide training and technical support in cyber inves-
18 tigation to—

19 (i) U.S. Immigration and Customs Enforcement personnel;

20 and

21 (ii) Federal, State, local, tribal, military, and foreign law
22 enforcement agency personnel engaged in the investigation of
23 crimes within their respective jurisdictions, on request and
24 subject to the availability of funds;

25 (D) shall participate in research and development in the area
26 of cyber investigations, in coordination with appropriate compo-
27 nents of the Department; and

28 (E) may recruit participants of the Human Exploitation Rescue
29 Operative (HERO) Child-Rescue Corps Program for investigative
30 and forensic positions in support of the functions of the CCU.

31 (3) COOPERATIVE AGREEMENTS.—The CCU may enter into coopera-
32 tive agreements to accomplish the functions set forth in paragraph (2).

33 (e) HUMAN EXPLOITATION RESCUE OPERATIVE CHILD-RESCUE CORPS
34 PROGRAM.—

35 (1) ESTABLISHMENT.—

36 (A) IN GENERAL.—There is in the Center a Human Exploi-
37 tation Rescue Operative Child-Rescue Corps Program (in this sub-
38 section referred to as the “HERO Child-Rescue Corps Program”),
39 which shall be a Department-wide program, in collaboration with
40 the Department of Defense and the National Association to Pro-
41 tect Children.

1 (B) PRIVATE-SECTOR COLLABORATION.—As part of the HERO
2 Child-Rescue Corps Program, the National Association to Protect
3 Children shall provide logistical support for program participants.

4 (2) PURPOSE.—The purpose of the HERO Child-Rescue Corps Pro-
5 gram shall be to recruit, train, equip, and employ members of the
6 Armed Forces on active duty and wounded, ill, and injured veterans
7 to combat and prevent child exploitation, through serving in investiga-
8 tive, intelligence, analyst, inspection, and forensic positions or in any
9 other positions determined appropriate by the employing agency.

10 (3) FUNCTIONS.—The HERO Child-Rescue Corps Program shall—

11 (A) provide, recruit, train, and equip participants of the HERO
12 Child-Rescue Corps Program in the areas of digital forensics, in-
13 vestigation, analysis, intelligence, and victim identification, as de-
14 termined by the Center and the needs of the Department; and

15 (B) ensure that during the internship period, participants in the
16 HERO Child-Rescue Corps Program are assigned to investigate
17 and analyze—

18 (i) child exploitation;

19 (ii) child pornography;

20 (iii) unidentified child victims;

21 (iv) human trafficking;

22 (v) traveling child sex offenders; and

23 (vi) forced child labor, including the sexual exploitation of
24 minors.

25 (f) PAID INTERNSHIP AND HIRING PROGRAM.—

26 (1) IN GENERAL.—The Secretary shall establish a paid internship
27 and hiring program for the purpose of placing participants of the
28 HERO Child-Rescue Corps Program (in this subsection referred to as
29 “participants”) into paid internship positions, for the subsequent ap-
30 pointment of the participants to permanent positions, as described in
31 the guidelines promulgated under paragraph (3).

32 (2) INTERNSHIP POSITIONS.—Under the paid internship and hiring
33 program required to be established under paragraph (1), the Secretary
34 shall assign or detail participants to positions in United States Immi-
35 gration and Customs Enforcement or any other Federal agency in ac-
36 cordance with the guidelines promulgated under paragraph (3).

37 (3) PLACEMENT.—

38 (A) IN GENERAL.—The Secretary shall promulgate guidelines
39 for assigning or detailing participants to positions in United
40 States Immigration and Customs Enforcement and other Federal
41 agencies, which shall include requirements for internship duties

1 and agreements regarding the subsequent appointment of the par-
2 ticipants to permanent positions.

3 (B) PREFERENCE.—The Secretary shall give a preference to
4 Homeland Security Investigations in assignments or details under
5 the guidelines promulgated under subparagraph (A).

6 (4) TERM OF INTERNSHIP.—An appointment to an internship posi-
7 tion under this subsection shall be for a term not to exceed 12 months.

8 (5) RATE AND TERM OF PAY.—After completion of initial group
9 training and on beginning work at an assigned office, a participant ap-
10 pointed to an internship position under this subsection who is not re-
11 ceiving monthly basic pay as a member of the Armed Forces on active
12 duty shall receive compensation at a rate that is—

13 (A) not less than the minimum rate of basic pay payable for a
14 position at level GS–5 of the General Schedule; and

15 (B) not more than the maximum rate of basic pay payable for
16 a position at level GS–7 of the General Schedule.

17 (6) ELIGIBILITY.—In establishing the paid internship and hiring
18 program required under paragraph (1), the Secretary shall ensure that
19 the eligibility requirements for participation in the internship program
20 are the same as the eligibility requirements for participation in the
21 HERO Child-Rescue Corps Program.

22 (7) HERO CHILD-RESCUE CORPS HIRING.—The Secretary shall es-
23 tablish in Homeland Security Investigations positions, which shall be
24 in addition to positions in existence on December 21, 2018, for the hir-
25 ing and permanent employment of graduates of the paid internship
26 program required to be established under paragraph (1).

27 (g) AUTHORIZATION OF APPROPRIATIONS.—

28 (1) IN GENERAL.—There are authorized to be appropriated to the
29 Secretary such sums as are necessary to carry out this section.

30 (2) ALLOCATION.—Of the amounts made available pursuant to para-
31 graph (1) in each of fiscal years 2023 through 2027, not more than
32 \$10,000,000 shall be used to carry out subsection (e) and not less than
33 \$2,000,000 shall be used to carry out subsection (f).

34 **§ 11217. Human trafficking**

35 (a) CENTER FOR COUNTERING HUMAN TRAFFICKING.—

36 (1) IN GENERAL.—

37 (A) ESTABLISHMENT.—The Secretary shall operate, within U.S.
38 Immigration and Customs Enforcement’s Homeland Security In-
39 vestigations, the Center for Countering Human Trafficking (re-
40 ferred to in this section as “CCHT”).

1 (B) PURPOSE.—The purpose of CCHT shall be to serve at the
2 forefront of the Department’s unified global efforts to counter
3 human trafficking through law enforcement operations and victim
4 protection, prevention, and awareness programs.

5 (C) ADMINISTRATION.—Homeland Security Investigations
6 shall—

7 (i) maintain a concept of operations that identifies CCHT
8 participants, funding, core functions, and personnel; and

9 (ii) update the concept of operations, as needed, to accom-
10 modate its mission and the threats to the mission.

11 (D) PERSONNEL.—

12 (i) DIRECTOR.—The Secretary shall appoint a CCHT Di-
13 rector, who shall—

14 (I) be a member of the Senior Executive Service; and

15 (II) serve as the Department’s representative on
16 human trafficking.

17 (ii) MINIMUM CORE PERSONNEL REQUIREMENTS.—Subject
18 to appropriations, the Secretary shall ensure that CCHT is
19 staffed with at least 45 employees in order to maintain con-
20 tinuity of effort, subject matter expertise, and necessary sup-
21 port to the Department, including—

22 (I) employees who are responsible for the Continued
23 Presence Program and other victim protection duties;

24 (II) employees who are responsible for training, in-
25 cluding curriculum development, and public awareness
26 and education;

27 (III) employees who are responsible for stakeholder
28 engagement, Federal interagency coordination, multilat-
29 eral partnerships, and policy;

30 (IV) employees who are responsible for public rela-
31 tions, human resources, evaluation, data analysis and re-
32 porting, and information technology;

33 (V) special agents and criminal analysts necessary to
34 accomplish its mission of combating human trafficking
35 and the importation of goods produced with forced labor;
36 and

37 (VI) managers.

38 (2) OPERATIONS UNIT.—The CCHT Director shall operate, in
39 CCHT, an Operations Unit, that shall, at a minimum—

40 (A) support criminal investigations of human trafficking (in-
41 cluding sex trafficking and forced labor)—

1 (i) by developing, tracking, and coordinating leads; and

2 (ii) by providing subject matter expertise;

3 (B) augment the enforcement of the prohibition on the importa-
4 tion of goods produced with forced labor through civil and criminal
5 authorities;

6 (C) coordinate a Department-wide effort to conduct procure-
7 ment audits and enforcement actions, including suspension and de-
8 barment, to mitigate the risk of human trafficking throughout De-
9 partment acquisitions and contracts; and

10 (D) support all CCHT enforcement efforts with intelligence by
11 conducting lead development, lead validation, case support, stra-
12 tegic analysis, and data analytics.

13 (3) PROTECTION AND AWARENESS PROGRAMS UNIT.—The CCHT
14 Director shall operate, in CCHT, an Operations Unit, that shall—

15 (A) incorporate a victim-centered approach throughout Depart-
16 ment policies, training, and practices;

17 (B) operate a comprehensive Continued Presence program;

18 (C) conduct, review, and assist with Department human traf-
19 ficking training, screening, and identification tools and efforts;

20 (D) operate the Blue Campaign’s nationwide public awareness
21 effort and any other awareness efforts needed to encourage victim
22 identification and reporting to law enforcement and to prevent
23 human trafficking; and

24 (E) coordinate external engagement, including training and
25 events, regarding human trafficking with critical partners, includ-
26 ing survivors, nongovernmental organizations, corporations, multi-
27 lateral entities, law enforcement agencies, and other interested
28 parties.

29 (4) Investigation of labor trafficking.—

30 (A) IN GENERAL.—Not later than January 5, 2025, the Sec-
31 retary shall establish a team of not fewer than 10 agents in CCHT
32 to be assigned to exclusively investigate labor trafficking.

33 (B) AUTHORIZATION OF APPROPRIATIONS.—There is authorized
34 to be appropriated to carry out subparagraph (A) \$2,000,000 for
35 each of fiscal years 2023 through 2027, to remain available until
36 expended.

37 (b) BLUE CAMPAIGN.—

38 (1) DEFINITION OF HUMAN TRAFFICKING.—In this subsection, the
39 term “human trafficking” means an act or practice described in para-
40 graph (11) or (12) of section 103 of the Trafficking Victims Protection
41 Act of 2000 (22 U.S.C. 7102(11), (12)).

1 (2) ESTABLISHMENT.—There is in CCHT a program that shall be
2 known as the “Blue Campaign”. The Blue Campaign shall be headed
3 by a Director, who shall be appointed by the Secretary.

4 (3) PURPOSE.—The purpose of the Blue Campaign shall be to unify
5 and coordinate Department efforts to address human trafficking.

6 (4) RESPONSIBILITIES.—The Secretary, working through the Direc-
7 tor, shall, in accordance with paragraph (5)—

8 (A) issue Department-wide guidance to appropriate Department
9 personnel;

10 (B) develop training programs for the personnel;

11 (C) coordinate departmental efforts, including training for the
12 personnel; and

13 (D) provide guidance and training on trauma-informed practices
14 to ensure that human trafficking victims are afforded prompt ac-
15 cess to victim support service providers, in addition to the assist-
16 ance required under section 107 of the Trafficking Victims Protec-
17 tion Act of 2000 (22 U.S.C. 7105), to address their immediate
18 and long-term needs.

19 (5) GUIDANCE AND TRAINING.—The Blue Campaign shall provide
20 guidance and training to Department personnel and other Federal,
21 State, tribal, and law enforcement personnel, as appropriate, regard-
22 ing—

23 (A) programs to help identify instances of human trafficking;

24 (B) the types of information that should be collected and re-
25 corded in information technology systems utilized by the Depart-
26 ment to help identify individuals suspected or convicted of human
27 trafficking;

28 (C) systematic and routine information sharing in the Depart-
29 ment and among Federal, State, tribal, and local law enforcement
30 agencies regarding—

31 (i) individuals suspected or convicted of human trafficking;

32 and

33 (ii) patterns and practices of human trafficking;

34 (D) techniques to identify suspected victims of trafficking along
35 the United States border and at airport security checkpoints;

36 (E) methods to be used by the Transportation Security Admin-
37 istration and personnel from other appropriate agencies to train
38 employees of the Transportation Security Administration to—

39 (i) identify suspected victims of trafficking; and

1 (ii) serve as a liaison and resource regarding human traf-
2 ficking prevention to appropriate State, local, and private-sec-
3 tor aviation workers and the traveling public;

4 (F) the development and utilization, in consultation with the
5 Blue Campaign Advisory Board established pursuant to paragraph
6 (7), of resources, such as indicator cards, fact sheets, pamphlets,
7 posters, brochures, and radio and television campaigns to—

8 (i) educate partners and stakeholders; and

9 (ii) increase public awareness of human trafficking;

10 (G) the leveraging of partnerships with State and local govern-
11 mental, nongovernmental, and private-sector organizations to raise
12 public awareness of human trafficking; and

13 (H) any other activities the Secretary determines necessary to
14 carry out the Blue Campaign.

15 (6) WEB-BASED TRAINING PROGRAMS.—To enhance training oppor-
16 tunities, the Director of the Blue Campaign shall develop web-based
17 interactive training videos that utilize a learning management system
18 to provide online training opportunities. During the 10-year period be-
19 ginning on the date that is 90 days after December 27, 2021, the
20 training opportunities shall be made available to the following individ-
21 uals:

22 (A) Federal, State, local, Tribal, and territorial law enforcement
23 officers.

24 (B) Non-Federal correction system personnel.

25 (C) Such other individuals as the Director determines appro-
26 priate.

27 (7) BLUE CAMPAIGN ADVISORY BOARD.—

28 (A) IN GENERAL.—There is in the Department a Blue Cam-
29 paign Advisory Board, which shall be comprised of representatives
30 assigned by the Secretary from—

31 (i) the Office for Civil Rights and Civil Liberties of the De-
32 partment;

33 (ii) the Privacy Office of the Department; and

34 (iii) not fewer than 4 other separate components or offices
35 of the Department.

36 (B) CHARTER.—The Secretary may issue a charter for the Blue
37 Campaign Advisory Board. The charter shall specify the following:

38 (i) The Board's mission and goals and the scope of its ac-
39 tivities.

40 (ii) The duties of the Board's representatives.

41 (iii) The frequency of the Board's meetings.

1 (C) CONSULTATION.—The Director shall consult the Blue Cam-
2 paign Advisory Board and, as appropriate, experts from other
3 components and offices of the CCHT regarding the following:

4 (i) Recruitment tactics used by human traffickers to inform
5 the development of training and materials by the Blue Cam-
6 paign.

7 (ii) The development of effective awareness tools for dis-
8 tribution to Federal and non-Federal officials to identify and
9 prevent instances of human trafficking.

10 (iii) Identification of additional persons or entities that
11 may be uniquely positioned to recognize signs of human traf-
12 ficking and the development of materials for those persons.

13 (8) CONSULTATION.—With regard to the development of programs
14 under the Blue Campaign and the implementation of the programs, the
15 Director may consult with State, local, Tribal, and territorial agencies,
16 non-governmental organizations, private sector organizations, and ex-
17 perts.

18 (e) TRANSFER OF FUNCTIONS AND RESOURCES.—

19 (1) AUTHORIZATION.—Not later than 180 days after December 27,
20 2022, the Secretary may transfer the functions and resources of any
21 component, directorate, or other office of the Department related to
22 combating human trafficking to the CCHT.

23 (2) NOTIFICATION.—Not later than 30 days before executing any
24 transfer authorized under paragraph (1), the Secretary shall notify the
25 Committee on Homeland Security and Governmental Affairs of the
26 Senate and the Committee on Homeland Security of the House of Rep-
27 resentatives of the planned transfer.

28 (d) INFORMATION SHARING TO FACILITATE REPORTS AND ANALYSIS.—
29 Each subagency of the Department shall share with CCHT—

30 (1) any information needed by CCHT to develop the strategy and
31 proposal required under section 4(a) of the Countering Human Traf-
32 ficking Act of 2021 (Public Law 117–322 136 Stat. 4435);and

33 (2) any additional data analysis to help CCHT better understand the
34 issues surrounding human trafficking.

35 (e) REPORTS TO CONGRESS.—

36 (1) IDENTIFYING NEEDED LEGISLATION.—Not later than December
37 27, 2023, the CCHT Director shall submit a report to Congress that
38 identifies any legislation that is needed to facilitate the Department’s
39 mission to end human trafficking.

- 11360. Review of fire prevention codes.
 - 11361. Fire safety effectiveness statements.
 - 11362. Annual conference.
 - 11363. Public safety awards.
 - 11364. Public access to information.
 - 11365. Assistance to Consumer Product Safety Commission.
 - 11366. Arson prevention, detection, and control.
 - 11367. Arson prevention grants.
 - 11368. Review of existing response information.
 - 11369. Working group.
 - 11370. Annual revision of recommendations.
 - 11371. Listings of places of public accommodation.
 - 11372. Dissemination of fire prevention and control information.
 - 11373. Fire prevention and control guidelines for places of public accommodation.
 - 11374. Prohibiting Federal funding of conferences held at non-certified places of public accommodation.
 - 11375. Fire safety systems in federally assisted buildings.
 - 11376. CPR training.
 - 11377. Firefighter assistance.
 - 11378. Staffing for adequate fire and emergency response.
 - 11379. Training for administration, and oversight and monitoring, of grants programs.
 - 11380. Surplus and excess Federal equipment.
 - 11381. Cooperative agreements with Federal facilities.
 - 11382. Burn research.
 - 11383. Removal of civil liability barriers that discourage the donation of fire equipment to volunteer fire companies.
 - 11384. Encouraging adoption of standards for firefighter health and safety.
 - 11385. Investigation authorities.
 - 11386. Administrative provisions.
 - 11387. Reports to Congress and the President.
 - 11388. Authorization of appropriations.
- Subchapter III—Global Catastrophic Risk Management**
- 11401. Definitions.
 - 11402. Assessment of global catastrophic risk.
 - 11403. Report.
 - 11404. Enhanced catastrophic incident annex.
 - 11405. Rules of construction.

Subchapter I—General

§ 11301. Definitions

In this subchapter:

(1) ADMINISTRATOR.—the term “Administrator” means the Administrator of the Agency.

(2) AGENCY.—The term “Agency” means the Federal Emergency Management Agency.

(3) CATASTROPHIC INCIDENT.—The term “catastrophic incident” means a natural disaster, act of terrorism, or other man-made disaster that results in extraordinary levels of casualties or damage or disruption severely affecting the population (including mass evacuations), infrastructure, environment, economy, national morale, or government functions in an area.

(4) CREDENTIALLED; CREDENTIALING.—The terms “credentialed” and “credentialing” mean having provided, or providing, respectively, documentation that identifies personnel and authenticates and verifies the qualifications of the personnel by ensuring that the personnel pos-

1 sess a minimum common level of training, experience, physical and
2 medical fitness, and capability appropriate for a particular position in
3 accordance with standards created under section 11310 of this title.

4 (5) FEDERAL COORDINATING OFFICER.—The term “Federal coordi-
5 nating officer” means a Federal coordinating officer as described in
6 section 302 of the Robert T. Stafford Disaster Relief and Emergency
7 Assistance Act (42 U.S.C. 5143).

8 (6) INTEROPERABLE COMMUNICATIONS.—The term “interoperable
9 communications” has the meaning given that term in section 10912(a)
10 of this title.

11 (7) NATIONAL INCIDENT MANAGEMENT SYSTEM.—The term “Na-
12 tional Incident Management System” means a system to enable effec-
13 tive, efficient, and collaborative incident management.

14 (8) NATIONAL RESPONSE PLAN.—The term “National Response
15 Plan” means the National Response Plan or a successor plan prepared
16 under section 11303(a)(6) of this title.

17 (9) NUCLEAR INCIDENT RESPONSE TEAM.—The term “Nuclear Inci-
18 dent Response Team” means a resource that includes—

19 (A) those entities of the Department of Energy that perform
20 nuclear or radiological emergency support functions (including ac-
21 cident response, search response, advisory, and technical oper-
22 ations functions), radiation exposure functions at the medical as-
23 sistance facility known as the Radiation Emergency Assistance
24 Center/Training Site (REAC/TS), radiological assistance func-
25 tions, and related functions; and

26 (B) those entities of the Environmental Protection Agency that
27 perform such support functions (including radiological emergency
28 response functions) and related functions.

29 (10) REGIONAL ADMINISTRATOR.—The term “Regional Adminis-
30 trator” means a Regional Administrator appointed under section 11307
31 of this title.

32 (11) REGIONAL OFFICE.—The term “Regional Office” means a Re-
33 gional Office established under section 11307 of this title.

34 (12) RESOURCES.—The term “resources” means personnel and
35 major items of equipment, supplies, and facilities available or poten-
36 tially available for responding to a natural disaster, act of terrorism,
37 or other man-made disaster.

38 (13) SURGE CAPACITY.—The term “surge capacity” means the abil-
39 ity to rapidly and substantially increase the provision of search and res-
40 cue capabilities, food, water, medicine, shelter and housing, medical
41 care, evacuation capacity, staffing (including disaster assistance em-

1 ployees), and other resources necessary to save lives and protect prop-
2 erty during a catastrophic incident.

3 (14) TRIBAL GOVERNMENT.—The term “tribal government” means
4 the government of an entity described in section 10101(13)(B) of this
5 title.

6 (15) TYPED; TYPING.—The terms “typed” and “typing” mean hav-
7 ing evaluated, or evaluating, respectively, a resource in accordance with
8 standards created under section 11310 of this title.

9 **§ 11302. Federal Emergency Management Agency**

10 (a) MISSION.—

11 (1) PRIMARY MISSION.—The primary mission of the Agency is to re-
12 duce the loss of life and property and protect the Nation from all haz-
13 ards, including natural disasters, acts of terrorism, and other man-
14 made disasters, by leading and supporting the Nation in a risk-based,
15 comprehensive emergency management system of preparedness, protec-
16 tion, response, recovery, and mitigation.

17 (2) SPECIFIC ACTIVITIES.—In support of the primary mission of the
18 Agency, the Administrator shall—

19 (A) lead the Nation’s efforts to prepare for, protect against, re-
20 spond to, recover from, and mitigate against the risk of natural
21 disasters, acts of terrorism, and other man-made disasters, includ-
22 ing catastrophic incidents;

23 (B) partner with State, local, and tribal governments and emer-
24 gency response providers, with other Federal agencies, with the
25 private sector, and with nongovernmental organizations to build a
26 national system of emergency management that can effectively and
27 efficiently utilize the full measure of the Nation’s resources to re-
28 spond to natural disasters, acts of terrorism, and other man-made
29 disasters, including catastrophic incidents;

30 (C) develop a Federal response capability that, when necessary
31 and appropriate, can act effectively and rapidly to deliver assist-
32 ance essential to saving lives or protecting or preserving property
33 or public health and safety in a natural disaster, act of terrorism,
34 or other man-made disaster;

35 (D) integrate the Agency’s emergency preparedness, protection,
36 response, recovery, and mitigation responsibilities to confront ef-
37 fectively the challenges of a natural disaster, act of terrorism, or
38 other man-made disaster;

39 (E) develop and maintain robust Regional Offices that will work
40 with State, local, and tribal governments, emergency response pro-

1 viders, and other appropriate entities to identify and address re-
2 gional priorities;

3 (F) under the leadership of the Secretary, coordinate with the
4 Commandant of the Coast Guard, the Commissioner of U.S. Cus-
5 toms and Border Protection, the Director of Immigration and
6 Customs Enforcement, the National Operations Center, and other
7 agencies and offices in the Department to take full advantage of
8 the substantial range of resources in the Department;

9 (G) provide funding, training, exercises, technical assistance,
10 planning, and other assistance to build tribal, local, State, re-
11 gional, and national capabilities (including communications capa-
12 bilities) necessary to respond to a natural disaster, act of ter-
13 rorism, or other man-made disaster; and

14 (H) develop and coordinate the implementation of a risk-based,
15 all-hazards strategy for preparedness that builds those common
16 capabilities necessary to respond to natural disasters, acts of ter-
17 rorism, and other man-made disasters while also building the
18 unique capabilities necessary to respond to specific types of inci-
19 dents that pose the greatest risk to our Nation.

20 (I) identify, integrate, and implement the needs of children, in-
21 cluding children within under-served communities, into activities to
22 prepare for, protect against, respond to, recover from, and miti-
23 gate against the risk of natural disasters, acts of terrorism, and
24 other disasters, including catastrophic incidents, including by ap-
25 pointing a technical expert, who may consult with relevant outside
26 organizations and experts, as necessary, to coordinate the integra-
27 tion, as necessary.

28 (b) ADMINISTRATOR.—

29 (1) REPORTING.—The Administrator shall report to the Secretary,
30 without being required to report through another official of the Depart-
31 ment.

32 (2) PRINCIPAL ADVISOR ON EMERGENCY MANAGEMENT.—

33 (A) IN GENERAL.—The Administrator is the principal advisor to
34 the President, the Homeland Security Council, and the Secretary
35 for all matters relating to emergency management in the United
36 States.

37 (B) ADVICE AND RECOMMENDATIONS.—

38 (i) RANGE OF OPTIONS.—In presenting advice with respect
39 to a matter to the President, the Homeland Security Council,
40 or the Secretary, the Administrator shall, as the Adminis-
41 trator considers appropriate, inform the President, the Home-

1 land Security Council, or the Secretary, as the case may be,
2 of the range of emergency preparedness, protection, response,
3 recovery, and mitigation options with respect to that matter.

4 (ii) ADVICE ON A PARTICULAR MATTER.—The Adminis-
5 trator, as the principal advisor on emergency management,
6 shall provide advice to the President, the Homeland Security
7 Council, or the Secretary on a particular matter when the
8 President, the Homeland Security Council, or the Secretary
9 requests advice.

10 (iii) RECOMMENDATIONS.—After informing the Secretary,
11 the Administrator may make recommendations to Congress
12 relating to emergency management the Administrator con-
13 sidered appropriate.

14 (3) CABINET STATUS.—

15 (A) IN GENERAL.—The President may designate the Adminis-
16 trator to serve as a member of the Cabinet in the event of natural
17 disasters, acts of terrorism, or other man-made disasters.

18 (B) RETENTION OF AUTHORITY.—Nothing in this paragraph
19 shall be construed as affecting the authority of the Secretary
20 under this subtitle.

21 **§ 11303. Authority and responsibilities**

22 (a) IN GENERAL.—The Administrator shall provide Federal leadership
23 necessary to prepare for, protect against, respond to, recover from, or miti-
24 gate against a natural disaster, act of terrorism, or other man-made dis-
25 aster, including—

26 (1) helping to ensure the effectiveness of emergency response pro-
27 viders to terrorist attacks, major disasters, and other emergencies;

28 (2) with respect to the Nuclear Incident Response Team (regardless
29 of whether it is operating as an organizational unit of the Department
30 pursuant to this subchapter)—

31 (A) establishing standards and certifying when those standards
32 have been met;

33 (B) conducting joint and other exercises, and training and eval-
34 uating performance; and

35 (C) providing funds to the Department of Energy and the Envi-
36 ronmental Protection Agency, as appropriate, for homeland secu-
37 rity planning, exercises and training, and equipment;

38 (3) providing the Federal Government's response to terrorist attacks
39 and major disasters, including—

40 (A) managing the response;

1 (B) directing the Domestic Emergency Support Team and
2 (when operating as an organizational unit of the Department pur-
3 suant to this subchapter) the Nuclear Incident Response Team;

4 (C) overseeing the Metropolitan Medical Response System; and

5 (D) coordinating other Federal response resources, including re-
6 quiring deployment of the Strategic National Stockpile, in the
7 event of a terrorist attack or major disaster;

8 (4) aiding the recovery from terrorist attacks and major disasters;

9 (5) building a comprehensive national incident management system
10 with Federal, State, and local government personnel, agencies, and au-
11 thorities, to respond to attacks and disasters;

12 (6) consolidating existing Federal Government emergency response
13 plans into a single, coordinated national response plan;

14 (7) helping ensure the acquisition of operable and interoperable com-
15 munications capabilities by Federal, State, local, and tribal govern-
16 ments and emergency response providers;

17 (8) assisting the President in carrying out the functions under the
18 Robert T. Stafford Disaster Relief and Emergency Assistance Act (42
19 U.S.C. 5121 et seq.) and carrying out all functions and authorities
20 given to the Administrator under that Act;

21 (9) carrying out the mission of the Agency to reduce the loss of life
22 and property and protect the Nation from all hazards by leading and
23 supporting the Nation in a risk-based, comprehensive emergency man-
24 agement system of—

25 (A) mitigation, by taking sustained actions to reduce or elimi-
26 nate long-term risks to people and property from hazards and
27 their effects;

28 (B) preparedness, by planning, training, and building the emer-
29 gency management profession to prepare effectively for, mitigate
30 against, respond to, and recover from a hazard;

31 (C) response, by conducting emergency operations to save lives
32 and property through positioning emergency equipment, personnel,
33 and supplies, through evacuating potential victims, through pro-
34 viding food, water, shelter, and medical care to those in need, and
35 through restoring critical public services; and

36 (D) recovery, by rebuilding communities so individuals, busi-
37 nesses, and governments can function on their own, return to nor-
38 mal life, and protect against future hazards;

39 (10) increasing efficiencies, by coordinating efforts relating to pre-
40 paredness, protection, response, recovery, and mitigation;

1 (11) helping to ensure the effectiveness of emergency response pro-
2 viders in responding to a natural disaster, act of terrorism, or other
3 man-made disaster;

4 (12) supervising grant programs administered by the Agency;

5 (13) administering and ensuring the implementation of the National
6 Response Plan, including coordinating and ensuring the readiness of
7 each emergency support function under the National Response Plan;

8 (14) coordinating with the National Advisory Council established
9 under section 11308 of this title;

10 (15) preparing and implementing the plans and programs of the
11 Federal Government for—

12 (A) continuity of operations;

13 (B) continuity of government; and

14 (C) continuity of plans;

15 (16) minimizing, to the extent practicable, overlapping planning and
16 reporting requirements applicable to State, local, and tribal govern-
17 ments and the private sector;

18 (17) maintaining and operating within the Agency the National Re-
19 sponse Coordination Center or its successor;

20 (18) developing a national emergency management system that is ca-
21 pable of preparing for, protecting against, responding to, recovering
22 from, and mitigating against catastrophic incidents;

23 (19) assisting the President in carrying out the functions under the
24 national preparedness goal and the national preparedness system and
25 carrying out all functions and authorities of the Administrator under
26 the national preparedness system;

27 (20) carrying out all authorities of the Federal Emergency Manage-
28 ment Agency and the Directorate of Preparedness of the Department
29 as transferred under section 11305 of this title; and

30 (21) otherwise carrying out the mission of the Agency as described
31 in section 11302(a) of this title.

32 (b) ALL-HAZARDS APPROACH.—In carrying out the responsibilities under
33 this section, the Administrator shall coordinate the implementation of a
34 risk-based, all-hazards strategy that builds those common capabilities nec-
35 essary to prepare for, protect against, respond to, recover from, or mitigate
36 against natural disasters, acts of terrorism, and other man-made disasters,
37 while also building the unique capabilities necessary to prepare for, protect
38 against, respond to, recover from, or mitigate against the risks of specific
39 types of incidents that pose the greatest risk to the Nation.

1 **§ 11304. Preparedness programs**

2 The Administrator is responsible for the radiological emergency prepared-
3 ness program and the chemical stockpile emergency preparedness program.

4 **§ 11305. Functions transferred**

5 (a) IN GENERAL.—Except as provided in subsection (b), there are trans-
6 ferred to the Agency the following:

7 (1) All functions of the Agency, including existing responsibilities for
8 emergency alert systems and continuity of operations and continuity of
9 government plans and programs as constituted on June 1, 2006, in-
10 cluding all of its personnel, assets, components, authorities, grant pro-
11 grams, and liabilities, and including the functions of the former Under
12 Secretary for Federal Emergency Management relating to the Agency.

13 (2) The former Directorate of Preparedness, as constituted on June
14 1, 2006, including all of its functions, personnel, assets, components,
15 authorities, grant programs, and liabilities, and including the functions
16 of the Under Secretary for Preparedness relating to the Directorate.

17 (b) EXCEPTIONS.—The following in the former Directorate of Prepared-
18 ness shall not be transferred:

19 (1) The Office of Infrastructure Protection.

20 (2) The National Communications System.

21 (3) The National Cybersecurity Division.

22 (4) The functions, personnel, assets, components, authorities, and li-
23 abilities of each component described under paragraphs (1) through
24 (3).

25 **§ 11306. Preserving the Federal Emergency Management**
26 **Agency**

27 (a) REORGANIZATION.—Section 10341(b) of this title shall not apply to
28 the Agency, including any function or organizational unit of the Agency.

29 (b) PROHIBITION ON CHANGES TO MISSIONS.—

30 (1) IN GENERAL.—The Secretary may not substantially or signifi-
31 cantly reduce, including through a Joint Task Force established under
32 section 11708 of this title, the authorities, responsibilities, or functions
33 of the Agency or the capability of the Agency to perform those authori-
34 ties, responsibilities, or functions, except as otherwise specifically pro-
35 vided in an Act enacted after October 4, 2006.

36 (2) CERTAIN TRANSFERS PROHIBITED.—No asset, function, or mis-
37 sion of the Agency may be diverted to the principal and continuing use
38 of another organization, unit, or entity of the Department, including
39 a Joint Task Force established under section 11708 of this title, except
40 for details or assignments that do not reduce the capability of the
41 Agency to perform its missions.

1 (c) REPROGRAMMING AND TRANSFER OF FUNDS.—In reprogramming or
2 transferring funds, the Secretary shall comply with applicable provisions of
3 any Act making appropriations for the Department for any fiscal year relat-
4 ing to the reprogramming or transfer of funds.

5 **§ 11307. Regional Offices**

6 (a) IN GENERAL.—There are in the Agency 10 regional offices, as identi-
7 fied by the Administrator.

8 (b) MANAGEMENT OF REGIONAL OFFICES.—

9 (1) REGIONAL ADMINISTRATOR.—Each Regional Office shall be
10 headed by a Regional Administrator, who shall be appointed by the Ad-
11 ministrator, after consulting with State, local, and tribal government
12 officials in the region. Each Regional Administrator shall report di-
13 rectly to the Administrator and be in the Senior Executive Service.

14 (2) QUALIFICATIONS.—

15 (A) IN GENERAL.—Each Regional Administrator shall be ap-
16 pointed from among individuals who have a demonstrated ability
17 in and knowledge of emergency management and homeland secu-
18 rity.

19 (B) CONSIDERATIONS.—In selecting a Regional Administrator
20 for a Regional Office, the Administrator shall consider the famili-
21 arity of an individual with the geographical area and demographic
22 characteristics of the population served by the Regional Office.

23 (c) RESPONSIBILITIES.—

24 (1) IN GENERAL.—The Regional Administrator shall work in part-
25 nership with State, local, and tribal governments, emergency managers,
26 emergency response providers, medical providers, the private sector,
27 nongovernmental organizations, multijurisdictional councils of govern-
28 ments, and regional planning commissions and organizations in the
29 geographical area served by the Regional Office to carry out the re-
30 sponsibilities of a Regional Administrator under this section.

31 (2) SPECIFIC RESPONSIBILITIES.—The responsibilities of a Regional
32 Administrator include—

33 (A) ensuring effective, coordinated, and integrated regional pre-
34 paredness, protection, response, recovery, and mitigation activities
35 and programs for natural disasters, acts of terrorism, and other
36 man-made disasters (including planning, training, exercises, and
37 professional development);

38 (B) assisting in the development of regional capabilities needed
39 for a national catastrophic response system;

40 (C) coordinating the establishment of effective regional operable
41 and interoperable emergency communications capabilities;

1 (D) staffing and overseeing one or more strike teams within the
2 region under subsection (f), to serve as the focal point of the Fed-
3 eral Government's initial response efforts for natural disasters,
4 acts of terrorism, and other man-made disasters within that re-
5 gion, and otherwise building Federal response capabilities to re-
6 spond to natural disasters, acts of terrorism, and other man-made
7 disasters within that region;

8 (E) designating an individual responsible for the development of
9 strategic and operational regional plans in support of the National
10 Response Plan;

11 (F) fostering the development of mutual aid and other coopera-
12 tive agreements;

13 (G) identifying critical gaps in regional capabilities to respond
14 to populations with special needs;

15 (H) maintaining and operating a Regional Response Coordina-
16 tion Center or its successor;

17 (I) coordinating with the private sector to help ensure private-
18 sector preparedness for natural disasters, acts of terrorism, and
19 other man-made disasters;

20 (J) assisting State, local, and tribal governments, where appro-
21 priate, to pre-identify and evaluate suitable sites where a multi-
22 jurisdictional incident command system may quickly be established
23 and operated from, if the need for a system arises; and

24 (K) performing any other duties relating to these responsibilities
25 that the Administrator may require.

26 (3) TRAINING AND EXERCISE REQUIREMENTS.—

27 (A) TRAINING.—The Administrator shall require each Regional
28 Administrator to undergo specific training periodically to com-
29 plement the qualifications of the Regional Administrator. The
30 training, as appropriate, shall include training with respect to the
31 National Incident Management System, the National Response
32 Plan, and other subjects determined by the Administrator.

33 (B) EXERCISES.—The Administrator shall require each Re-
34 gional Administrator to participate as appropriate in regional and
35 national exercises.

36 (d) AREA OFFICES.—

37 (1) IN GENERAL.—There is an Area Office for the Pacific and an
38 Area Office for the Caribbean, as components in the appropriate Re-
39 gional Offices.

40 (2) ALASKA.—The Administrator shall establish an Area Office in
41 Alaska, as a component in the appropriate Regional Office.

1 (e) REGIONAL ADVISORY COUNCIL.—

2 (1) ESTABLISHMENT.—Each Regional Administrator shall establish
3 a Regional Advisory Council.

4 (2) NOMINATIONS.—A State, local, or tribal government located in
5 the geographic area served by the Regional Office may nominate offi-
6 cials, including Adjutants General and emergency managers, to serve
7 as members of the Regional Advisory Council for that region.

8 (3) RESPONSIBILITIES.—Each Regional Advisory Council shall—

9 (A) advise the Regional Administrator on emergency manage-
10 ment issues specific to that region;

11 (B) identify geographic, demographic, or other characteristics
12 peculiar to a State, local, or tribal government within the region
13 that might make preparedness, protection, response, recovery, or
14 mitigation more complicated or difficult; and

15 (C) advise the Regional Administrator of weaknesses or defi-
16 ciencies in preparedness, protection, response, recovery, and miti-
17 gation for a State, local, and tribal government within the region
18 of which the Regional Advisory Council is aware.

19 (f) REGIONAL OFFICE STRIKE TEAMS.—

20 (1) IN GENERAL.—In coordination with other relevant Federal agen-
21 cies, each Regional Administrator shall oversee multi-agency strike
22 teams authorized under section 303 of the Robert T. Stafford Disaster
23 Relief and Emergency Assistance Act (42 U.S.C. 5144) that shall con-
24 sist of—

25 (A) a designated Federal coordinating officer;

26 (B) personnel trained in incident management;

27 (C) public affairs, response and recovery, and communications
28 support personnel;

29 (D) a defense coordinating officer;

30 (E) liaisons to other Federal agencies;

31 (F) other personnel the Administrator or Regional Adminis-
32 trator determines appropriate; and

33 (G) individuals from the agencies with primary responsibility for
34 each of the emergency support functions in the National Response
35 Plan.

36 (2) OTHER DUTIES TO BE CONSISTENT.—The duties of an individual
37 assigned to a Regional Office strike team from another relevant agency
38 when the individual is not functioning as a member of the strike team
39 shall be consistent with the emergency preparedness activities of the
40 agency that employs the individual.

1 (3) LOCATION OF MEMBERS.—The members of each Regional Office
2 strike team, including representatives from agencies other than the De-
3 partment, shall be based primarily within the region that corresponds
4 to that strike team.

5 (4) COORDINATION.—Each Regional Office strike team shall coordi-
6 nate the training and exercises of that strike team with the State, local,
7 and tribal governments and private-sector and nongovernmental entities
8 that the strike team shall support when a natural disaster, act of ter-
9 rorism, or other man-made disaster occurs.

10 (5) PREPAREDNESS.—Each Regional Office strike team shall be
11 trained as a unit on a regular basis and equipped and staffed to be
12 well prepared to respond to natural disasters, acts of terrorism, and
13 other man-made disasters, including catastrophic incidents.

14 (6) AUTHORITIES.—If the Administrator determines that statutory
15 authority is inadequate for the preparedness and deployment of individ-
16 uals in strike teams under this subsection, the Administrator shall re-
17 port to Congress regarding the additional statutory authorities that the
18 Administrator determines are necessary.

19 **§ 11308. National Advisory Council**

20 (a) ESTABLISHMENT.—There is in the Department the National Advisory
21 Council, established as an advisory body under section 10391(a) of this title
22 to ensure effective and ongoing coordination of Federal preparedness, pro-
23 tection, response, recovery, and mitigation for natural disasters, acts of ter-
24 rorism, and other man-made disasters.

25 (b) RESPONSIBILITIES.—

26 (1) IN GENERAL.—The National Advisory Council shall advise the
27 Administrator on all aspects of emergency management. The National
28 Advisory Council shall incorporate State, local, and tribal government
29 and private-sector input in the development and revision of the national
30 preparedness goal, the national preparedness system, the National Inci-
31 dent Management System, the National Response Plan, and other re-
32 lated plans and strategies.

33 (2) CONSULTATION ON GRANTS.—To ensure input from and coordi-
34 nation with State, local, and tribal governments and emergency re-
35 sponse providers, the Administrator shall regularly consult and work
36 with the National Advisory Council on the administration and assess-
37 ment of grant programs administered by the Department, including
38 with respect to the development of program guidance and the develop-
39 ment and evaluation of risk-assessment methodologies, as appropriate.

40 (c) MEMBERSHIP.—

1 (1) IN GENERAL.—The members of the National Advisory Council
2 shall be appointed by the Administrator, and shall, to the extent prac-
3 ticable, represent a geographic (including urban and rural) and sub-
4 stantive cross section of officials, emergency managers, and emergency
5 response providers from State, local, and tribal governments, the pri-
6 vate sector, and nongovernmental organizations, including as appro-
7 priate—

8 (A) members selected from the emergency management field
9 and emergency response providers, including fire service, law en-
10 forcement, hazardous materials response, emergency medical serv-
11 ices, and emergency management personnel, or organizations rep-
12 resenting these individuals;

13 (B) health scientists, emergency and inpatient medical pro-
14 viders, and public health professionals;

15 (C) experts from Federal, State, local, and tribal governments,
16 and the private sector, representing standards-setting and accred-
17 iting organizations, including representatives from the voluntary
18 consensus codes and standards development community, particu-
19 larly those with expertise in the emergency preparedness and re-
20 sponse field;

21 (D) State, local, and tribal government officials with expertise
22 in preparedness, protection, response, recovery, and mitigation, in-
23 cluding Adjutants General;

24 (E) elected State, local, and tribal government executives;

25 (F) experts in public- and private-sector infrastructure protec-
26 tion, cybersecurity, and communications;

27 (G) representatives of individuals with disabilities and other
28 populations with special needs; and

29 (H) other individuals the Administrator determines to be appro-
30 priate.

31 (2) COORDINATION WITH DEPARTMENTS OF HEALTH AND HUMAN
32 SERVICES AND TRANSPORTATION.—In the selection of members of the
33 National Advisory Council who are health or emergency medical serv-
34 ices professionals, the Administrator shall work with the Secretary of
35 Health and Human Services and the Secretary of Transportation.

36 (3) EX OFFICIO MEMBERS.—The Administrator shall designate one
37 or more officers of the Federal Government to serve as ex officio mem-
38 bers of the National Advisory Council.

39 (4) TERM OF OFFICE.—The term of office of each member of the
40 National Advisory Council shall be 3 years.

41 (d) RESPONSE SUBCOMMITTEE.—

1 (1) ESTABLISHMENT.—The Administrator shall establish the Rail-
2 road Emergency Services Preparedness, Operational Needs, and Safety
3 Evaluation Subcommittee (in this subsection referred to as the “RE-
4 SPONSE Subcommittee”).

5 (2) MEMBERSHIP.—Notwithstanding subsection (c), the RE-
6 SPONSE Subcommittee is composed of the following:

7 (A) the Deputy Administrator, Protection and National Pre-
8 paredness of the Federal Emergency Management Agency, or des-
9 ignee.

10 (B) The Chief Safety Officer of the Pipeline and Hazardous
11 Materials Safety Administration, or designee.

12 (C) The Associate Administrator for Hazardous Materials Safe-
13 ty of the Pipeline and Hazardous Materials Safety Administration,
14 or designee.

15 (D) The Assistant Director for Emergency Communications, or
16 designee.

17 (E) The Director of the Office of Railroad, Pipeline and Haz-
18 ardous Materials Investigations of the National Transportation
19 Safety Board, or designee.

20 (F) The Chief Safety Officer and Associate Administrator for
21 Railroad Safety of the Federal Railroad Administration, or des-
22 ignee.

23 (G) The Assistant Administrator for Security Policy and Indus-
24 try Engagement of the Transportation Security Administration, or
25 designee.

26 (H) The Assistant Commandant for Response Policy of the
27 Coast Guard, or designee.

28 (I) The Assistant Administrator for the Office of Solid Waste
29 and Emergency Response of the Environmental Protection Agen-
30 cy, or designee.

31 (J) Such other qualified individuals as the co-chairpersons shall
32 jointly appoint as soon as practicable from among the following:

33 (i) Members of the National Advisory Council who have the
34 requisite technical knowledge and expertise to address rail
35 emergency response issues, including members for the fol-
36 lowing disciplines:

37 (I) Emergency management and emergency response
38 providers, including fire service, law enforcement, haz-
39 ardous materials response, and emergency medical serv-
40 ices.

41 (II) State, local, and tribal government officials.

1 (ii) Individuals who have the requisite technical knowledge
2 and expertise to serve on the RESPONSE Subcommittee, in-
3 cluding at least 1 representative from each of the following:

4 (I) The rail industry.

5 (II) Rail labor.

6 (III) Persons that offer oil for transportation by rail.

7 (IV) The communications industry.

8 (V) Emergency response providers, including individ-
9 uals nominated by national organizations representing
10 State and local governments and emergency responders.

11 (VI) Emergency response training providers.

12 (VII) Representatives from tribal organizations.

13 (VIII) Technical experts.

14 (IX) Vendors, developers, and manufacturers of sys-
15 tems, facilities, equipment, and capabilities for emer-
16 gency responder services.

17 (iii) Representatives of such other stakeholders and inter-
18 ested and affected parties as the co-chairpersons consider ap-
19 propriate.

20 (3) CO-CHAIRPERSONS.—The members described in subparagraphs
21 (A) and (B) of paragraph (2) shall serve as the co-chairpersons of the
22 RESPONSE Subcommittee.

23 (4) CONSULTATION WITH NONMEMBERS.—The RESPONSE Sub-
24 committee and the program offices for emergency responder training
25 and resources shall consult with other relevant agencies and groups, in-
26 cluding entities engaged in federally funded research and academic in-
27 stitutions engaged in relevant work and research, that are not rep-
28 resented on the RESPONSE Subcommittee to consider new and devel-
29 oping technologies and methods that may be beneficial to preparedness
30 and response to rail hazardous materials incidents.

31 (5) RECOMMENDATIONS.—The RESPONSE Subcommittee shall de-
32 velop recommendations, as appropriate, for improving emergency re-
33 sponder training and resource allocation for hazardous materials inci-
34 dents involving railroads after evaluating the following topics:

35 (A) The quality and application of training for State and local
36 emergency responders relating to rail hazardous materials inci-
37 dents, including training for emergency responders serving small
38 communities near railroads, including the following:

39 (i) Ease of access to relevant training for State and local
40 emergency responders, including an analysis of—

41 (I) the number of individual being trained;

- 1 (II) the number of individuals who are applying;
- 2 (III) whether current demand is being met;
- 3 (IV) current challenges; and
- 4 (V) projected needs.
- 5 (ii) Modernization of training course content relating to rail
- 6 hazardous materials incidents, with a particular focus on fluc-
- 7 tuations in oil shipments by rail, including regular and ongo-
- 8 ing evaluation of course opportunities, adaptation to emerging
- 9 trends, agency and private-sector outreach, effectiveness, and
- 10 ease of access for State and local emergency responders.
- 11 (iii) Identification of overlap in training content and identi-
- 12 fication of opportunities to develop complementary courses
- 13 and materials among governmental and nongovernmental en-
- 14 tities.
- 15 (iv) Online training platforms, train-the-trainer, and mobile
- 16 training options.
- 17 (B) The availability and effectiveness of Federal, State, local,
- 18 and nongovernmental funding levels related to training emergency
- 19 responders for rail hazardous materials incidents, including emer-
- 20 gency responders serving small communities near railroads, includ-
- 21 ing—
- 22 (i) identifying overlap in resource allocation;
- 23 (ii) identifying cost-saving measures that can be imple-
- 24 mented to increase training opportunities;
- 25 (iii) leveraging government funding with nongovernmental
- 26 funding to enhance training opportunities and fill existing
- 27 training gaps;
- 28 (iv) adapting priority settings for agency funding alloca-
- 29 tions in response to emerging trends;
- 30 (v) identifying historic levels of funding across Federal
- 31 agencies for rail hazardous materials incident response and
- 32 training, including funding provided by the private sector to
- 33 public entities or in conjunction with Federal programs; and
- 34 (vi) identifying current funding resources across agencies.
- 35 (C) The strategy for integrating commodity flow studies, map-
- 36 ping, and rail and hazardous materials databases for State and
- 37 local emergency responders and for increasing the rate of access
- 38 to the individual responder in existing or emerging communica-
- 39 tions technology.
- 40 (6) REPORT.—

1 (A) IN GENERAL.—Not later than December 16, 2017, the RE-
2 SPONSE Subcommittee shall submit a report to the National Ad-
3 visory Council that—

4 (i) includes the recommendations developed under para-
5 graph (5);

6 (ii) specifies the time frames for implementing the rec-
7 ommendations that do not require congressional action; and

8 (iii) identifies the recommendations that do require con-
9 gressional action.

10 (B) REVIEW.—Not later than 30 days after receiving the report
11 under subparagraph (A), the National Advisory Council shall
12 begin a review of the report. The National Advisory Council may
13 ask for additional clarification, changes, or other information from
14 the RESPONSE Subcommittee to assist in the approval of the
15 recommendations.

16 (C) RECOMMENDATIONS.—Once the National Advisory Council
17 approves the recommendations of the RESPONSE Subcommittee,
18 the National Advisory Council shall submit the report to—

19 (i) the co-chairpersons of the RESPONSE Subcommittee;

20 (ii) the head of each other agency represented on the RE-
21 SPONSE Subcommittee;

22 (iii) the Committee on Homeland Security and Govern-
23 mental Affairs of the Senate;

24 (iv) the Committee on Commerce, Science, and Transpor-
25 tation of the Senate;

26 (v) the Committee on Homeland Security of the House of
27 Representatives; and

28 (vi) the Committee on Transportation and Infrastructure of
29 the House of Representatives.

30 (7) INTERIM ACTIVITY.—

31 (A) UPDATES AND OVERSIGHT.—After the submission of the re-
32 port by the National Advisory Council under paragraph (6), the
33 Administrator shall—

34 (i) provide annual updates to the congressional committees
35 referred to in paragraph (6)(C) regarding the status of the
36 implementation of the recommendations developed under
37 paragraph (5); and

38 (ii) coordinate the implementation of the recommendations
39 described in paragraph (5)(A)(i), as appropriate.

1 (B) SUNSET.—The requirements of subparagraph (A) shall ter-
2minate on the date that is 2 years after the date of the submission
3of the report required under paragraph (6)(A).

4 (8) TERMINATION.—The RESPONSE Subcommittee shall terminate
5not later than 90 days after the submission of the report required
6under paragraph (6))(C).

7 (e) APPLICABILITY OF CHAPTER 10 OF TITLE 5.—

8 (1) IN GENERAL.—Notwithstanding section 10391(a) of this title
9and subject to paragraph (2), chapter 10 of title 5, including sub-
10sections (a), (b), and (d) of section 1009 of title 5, and section 552b(e)
11of title 5, apply to the National Advisory Council.

12 (2) TERMINATION.—Section 1013(a)(2) of title 5 does not apply to
13the National Advisory Council.

14 **§ 11309. National Integration Center**

15 (a) IN GENERAL.—There is in the Agency the National Integration Cen-
16ter.

17 (b) RESPONSIBILITIES.—

18 (1) IN GENERAL.—The Administrator, through the National Integra-
19tion Center, and in consultation with other Federal departments and
20agencies and the National Advisory Council, shall ensure ongoing man-
21agement and maintenance of the National Incident Management Sys-
22tem, the National Response Plan, and a successor to the system or
23plan.

24 (2) REVIEW AND REVISION OF SYSTEM AND PLAN.—The National
25Integration Center shall periodically review, and revise as appropriate,
26the National Incident Management System and the National Response
27Plan, including—

28 (A) establishing, in consultation with the Director of the Cor-
29poration for National and Community Service, a process to better
30use volunteers and donations;

31 (B) improving the use of Federal, State, local, and tribal re-
32sources and ensuring the effective use of emergency response pro-
33viders at emergency scenes; and

34 (C) revising the Catastrophic Incident Annex, finalizing and re-
35leasing the Catastrophic Incident Supplement to the National Re-
36sponse Plan, and ensuring that both effectively address response
37requirements in the event of a catastrophic incident.

38 (c) INCIDENT MANAGEMENT.—

39 (1) IN GENERAL.—

40 (A) NATIONAL RESPONSE PLAN.—The Administrator shall en-
41sure that the National Response Plan provides for a clear chain

1 of command to lead and coordinate the Federal response to a nat-
2 ural disaster, act of terrorism, or other man-made disaster.

3 (B) ADMINISTRATOR.—The chain of the command specified in
4 the National Response Plan shall provide for a role for—

5 (i) the Administrator consistent with the role of the Admin-
6 istrator as the principal emergency management advisor to
7 the President, the Homeland Security Council, and the Sec-
8 retary under section 11302(b)(2) of this title and the respon-
9 sibility of the Administrator under the Post-Katrina Emer-
10 gency Management Reform Act of 2006 (Public Law 109-
11 295, 120 Stat. 1394), and the amendments made by that
12 Act, relating to natural disasters, acts of terrorism, and other
13 man-made disasters; and

14 (ii) the Federal Coordinating Officer consistent with the re-
15 sponsibilities under section 302(b) of the Robert T. Stafford
16 Disaster Relief and Emergency Assistance Act (42 U.S.C.
17 5143(b)).

18 (2) PRINCIPAL FEDERAL OFFICIAL OR DIRECTOR OF A JOINT TASK
19 FORCE.—The Principal Federal Official (or the successor to the Offi-
20 cial) or a Director of a Joint Task Force established under section
21 11708 of this title shall not—

22 (A) direct or replace the incident command structure established
23 at the incident; or

24 (B) have directive authority over the Senior Federal Law En-
25 forcement Official, Federal Coordinating Officer, or other Federal
26 and State officials.

27 **§ 11310. Credentialing and typing**

28 (a) IN GENERAL.—The Administrator shall enter into a memorandum of
29 understanding with the administrators of the Emergency Management As-
30 sistance Compact, State, local, and tribal governments, and organizations
31 that represent emergency response providers, to collaborate on developing
32 standards for deployment capabilities, including for credentialing and typing
33 of incident management personnel, emergency response providers, and other
34 personnel (including temporary personnel) and resources likely needed to re-
35 spond to natural disasters, acts of terrorism, and other man-made disasters.

36 (b) DISTRIBUTION.—

37 (1) IN GENERAL.—The Administrator shall provide the standards de-
38 veloped under subsection (a), including detailed written guidance, to—

39 (A) each Federal agency that has responsibilities under the Na-
40 tional Response Plan to aid that agency with credentialing and
41 typing incident management personnel, emergency response pro-

1 Homeland Security Presidential Directive–7, or a successor to the Di-
2 rective, shall establish a formal relationship, including an agreement re-
3 garding information sharing, between the elements of the agency or de-
4 partment and the National Infrastructure Simulation and Analysis
5 Center, through the Department.

6 (3) PURPOSE.—The purpose of the relationship under paragraph (2)
7 is to permit each Federal agency and department described in para-
8 graph (2) to take full advantage of the capabilities of the National In-
9 frastructure Simulation and Analysis Center (particularly vulnerability
10 and consequence analysis), consistent with its work load capacity and
11 priorities, for real-time response to reported and projected natural dis-
12 asters, acts of terrorism, and other man-made disasters.

13 (4) RECIPIENT OF CERTAIN SUPPORT.—Modeling, simulation, and
14 analysis provided under this subsection shall be provided to relevant
15 Federal agencies and departments, including Federal agencies and de-
16 partments with critical infrastructure responsibilities under Homeland
17 Security Presidential Directive–7, or a successor to the Directive.

18 **§ 11312. Evacuation plans and exercises**

19 (a) IN GENERAL.—Notwithstanding another law, and subject to sub-
20 section (d), grants made to States or local or tribal governments by the De-
21 partment through the State Homeland Security Grant Program or the
22 Urban Area Security Initiative may be used to—

23 (1) establish programs for the development and maintenance of mass
24 evacuation plans under subsection (b) in the event of a natural dis-
25 aster, act of terrorism, or other man-made disaster;

26 (2) prepare for the execution of the plans, including the development
27 of evacuation routes and the purchase and stockpiling of necessary sup-
28 plies and shelters; and

29 (3) conduct exercises of the plans.

30 (b) PLAN DEVELOPMENT.—In developing the mass evacuation plans au-
31 thorized under subsection (a), each State, local, or tribal government shall,
32 to the maximum extent practicable—

33 (1) establish incident command and decision-making processes;

34 (2) ensure that State, local, and tribal government plans, including
35 evacuation routes, are coordinated and integrated;

36 (3) identify primary and alternative evacuation routes and methods
37 to increase evacuation capabilities along the routes, such as conversion
38 of two-way traffic to one-way evacuation routes;

39 (4) identify evacuation transportation modes and capabilities, includ-
40 ing the use of mass and public transit capabilities, and coordinating
41 and integrating evacuation plans for all populations including for those

1 individuals located in hospitals, nursing homes, and other institutional
2 living facilities;

3 (5) develop procedures for informing the public of evacuation plans
4 before and during an evacuation, including individuals—

5 (A) with disabilities or other special needs, including the elderly;

6 (B) with limited English proficiency; or

7 (C) who might otherwise have difficulty in obtaining informa-
8 tion; and

9 (6) identify shelter locations and capabilities.

10 (c) ASSISTANCE.—

11 (1) IN GENERAL.—The Administrator may establish guidelines,
12 standards, or requirements determined appropriate to administer this
13 section and to ensure effective mass evacuation planning for State,
14 local, and tribal areas.

15 (2) REQUESTED ASSISTANCE.—The Administrator shall make assist-
16 ance available upon request of a State, local, or tribal government to
17 assist hospitals, nursing homes, and other institutions that house indi-
18 viduals with special needs to establish, maintain, and exercise mass
19 evacuation plans that are coordinated and integrated into the plans de-
20 veloped by that State, local, or tribal government under this section.

21 (d) MULTIPURPOSE FUNDS.—Nothing in this section may be construed
22 to preclude a State, local, or tribal government from using grant funds in
23 a manner that enhances preparedness for a natural or man-made disaster
24 unrelated to an act of terrorism, if the use assists the government in build-
25 ing capabilities for terrorism preparedness.

26 § 11313. Disability Coordinator

27 (a) IN GENERAL.—After consultation with organizations representing in-
28 dividuals with disabilities, the National Council on Disability, and the Inter-
29 agency Coordinating Council on Emergency Preparedness and Individuals
30 with Disabilities, established under Executive Order No. 13347 (July 22,
31 2004, 69 Fed. Reg. 44573), the Administrator shall appoint a Disability
32 Coordinator. The Disability Coordinator shall report directly to the Admin-
33 istrator, in order to ensure that the needs of individuals with disabilities are
34 being properly addressed in emergency preparedness and disaster relief.

35 (b) RESPONSIBILITIES.—The Disability Coordinator is responsible for—

36 (1) providing guidance and coordination on matters related to indi-
37 viduals with disabilities in emergency planning requirements and relief
38 efforts in the event of a natural disaster, act of terrorism, or other
39 man-made disaster;

40 (2) interacting with the staff of the Agency, the National Council on
41 Disability, the Interagency Coordinating Council on Emergency Pre-

1 paredness and Individuals with Disabilities established under Executive
2 Order No. 13347 (July 22, 2004, 69 Fed. Reg. 44573), other agencies
3 of the Federal Government, and State, local, and tribal government au-
4 thorities regarding the needs of individuals with disabilities in emer-
5 gency planning requirements and relief efforts in the event of a natural
6 disaster, act of terrorism, or other man-made disaster;

7 (3) consulting with organizations that represent the interests and
8 rights of individuals with disabilities about the needs of individuals with
9 disabilities in emergency planning requirements and relief efforts in the
10 event of a natural disaster, act of terrorism, or other man-made dis-
11 aster;

12 (4) ensuring the coordination and dissemination of best practices and
13 model evacuation plans for individuals with disabilities;

14 (5) ensuring the development of training materials and a curriculum
15 for training of emergency response providers, State, local, and tribal
16 government officials, and others on the needs of individuals with dis-
17 abilities;

18 (6) promoting the accessibility of telephone hotlines and websites re-
19 garding emergency preparedness, evacuations, and disaster relief;

20 (7) working to ensure that video programming distributors, including
21 broadcasters, cable operators, and satellite television services, make
22 emergency information accessible to individuals with hearing and vision
23 disabilities;

24 (8) ensuring the availability of accessible transportation options for
25 individuals with disabilities in the event of an evacuation;

26 (9) providing guidance and implementing policies to ensure that the
27 rights and wishes of individuals with disabilities regarding post-evacu-
28 ation residency and relocation are respected;

29 (10) ensuring that meeting the needs of individuals with disabilities
30 is included in the components of the national preparedness system es-
31 tablished under section 644 of the Post-Katrina Emergency Manage-
32 ment Reform Act of 2006 (Public Law 109–295, 120 Stat. 1425); and

33 (11) carrying out other duties assigned by the Administrator.

34 **§ 11314. National Operations Center**

35 (a) DEFINITION OF SITUATIONAL AWARENESS.—In this section, the term
36 “situational awareness” means information gathered from a variety of
37 sources that, when communicated to emergency managers, decision makers,
38 and other appropriate officials, can form the basis for incident management
39 decision-making and steady-state activity.

40 (b) ESTABLISHMENT.—The National Operations Center is the principal
41 operations center for the Department and shall—

1 (1) provide situational awareness and a common operating picture
2 for the entire Federal Government, and for State, local, tribal, and ter-
3 ritorial governments, the private sector, and international partners as
4 appropriate, for events, threats, and incidents involving a natural dis-
5 aster, act of terrorism, or other man-made disaster;

6 (2) ensure that critical terrorism and disaster-related information
7 reaches government decision-makers; and

8 (3) enter into agreements with other Federal operations centers and
9 other homeland security partners, as appropriate, to facilitate the shar-
10 ing of information.

11 (c) STATE AND LOCAL EMERGENCY RESPONDER REPRESENTATION.—

12 (1) ESTABLISHMENT OF EMERGENCY RESPONDER POSITION.—The
13 Secretary shall establish a position, on a rotating basis, for a represent-
14 ative of State and local emergency responders at the National Oper-
15 ations Center established under subsection (b) to ensure the effective
16 sharing of information between the Federal Government and State and
17 local emergency response services.

18 (2) MANAGEMENT.—The Secretary shall manage the position estab-
19 lished under paragraph (1) in accordance with the rules, regulations,
20 and practices that govern other similar rotating positions at the Na-
21 tional Operations Center.

22 **§ 11315. Nuclear incident response**

23 (a) IN GENERAL.—At the direction of the Secretary (in connection with
24 an actual or threatened terrorist attack, major disaster, or other emergency
25 in the United States), the Nuclear Incident Response Team shall operate
26 as an organizational unit of the Department. While so operating, the Nu-
27 clear Incident Response Team shall be subject to the direction, authority,
28 and control of the Secretary.

29 (b) RULE OF CONSTRUCTION.—Nothing in this subchapter shall be con-
30 strued to limit the ordinary responsibility of the Secretary of Energy and
31 the Administrator of the Environmental Protection Agency for organizing,
32 training, equipping, and utilizing their respective entities in the Nuclear In-
33 cident Response Team, or (subject to this subchapter) from exercising direc-
34 tion, authority, and control over them when they are not operating as a unit
35 of the Department.

36 **§ 11316. Conduct of certain public health-related activities**

37 (a) IN GENERAL.—With respect to all public health-related activities to
38 improve State, local, and hospital preparedness and response to chemical,
39 biological, radiological, and nuclear and other emerging terrorist threats car-
40 ried out by the Department of Health and Human Services (including the
41 Public Health Service), the Secretary of Health and Human Services shall

1 set priorities and preparedness goals and further develop a coordinated
2 strategy for these activities in collaboration with the Secretary.

3 (b) EVALUATION OF PROGRESS.—In carrying out subsection (a), the Sec-
4 retary of Health and Human Services shall collaborate with the Secretary
5 in developing specific benchmarks and outcome measurements for evaluating
6 progress toward achieving the priorities and goals described in subsection
7 (a).

8 **§ 11317. Use of national private-sector networks in emer-**
9 **gency response**

10 To the maximum extent practicable, the Secretary shall use national pri-
11 vate-sector networks and infrastructure for emergency response to chemical,
12 biological, radiological, nuclear, or explosive disasters, and other major dis-
13 asters.

14 **§ 11318. Model standards and guidelines for critical infra-**
15 **structure workers**

16 (a) IN GENERAL.—In coordination with appropriate national professional
17 organizations, Federal, State, local, and tribal government agencies, and pri-
18 vate-sector and nongovernmental entities, the Administrator shall establish
19 model standards and guidelines for credentialing critical infrastructure
20 workers that may be used by a State to credential critical infrastructure
21 workers that may respond to a natural disaster, act of terrorism, or other
22 man-made disaster.

23 (b) DISTRIBUTION AND ASSISTANCE.—The Administrator shall provide
24 the standards developed under subsection (a), including detailed written
25 guidance, to State, local, and tribal governments, and provide expertise and
26 technical assistance to aid the governments with credentialing critical infra-
27 structure workers that may respond to a natural disaster, act of terrorism,
28 or other man-made disaster.

29 **§ 11319. Guidance and recommendations**

30 (a) IN GENERAL.—Consistent with their responsibilities and authorities
31 under law, as of August 2, 2007, the Administrator and the Director of the
32 Cybersecurity and Infrastructure Security Agency, in consultation with the
33 private sector, may develop guidance or recommendations and identify best
34 practices to assist or foster action by the private sector in—

- 35 (1) identifying potential hazards and assessing risks and impacts;
36 (2) mitigating the impact of a wide variety of hazards, including
37 weapons of mass destruction;
38 (3) managing necessary emergency preparedness and response re-
39 sources;
40 (4) developing mutual aid agreements;

1 (5) developing and maintaining emergency preparedness and re-
2 sponse plans, and associated operational procedures;

3 (6) developing and conducting training and exercises to support and
4 evaluate emergency preparedness and response plans and operational
5 procedures;

6 (7) developing and conducting training programs for security guards
7 to implement emergency preparedness and response plans and oper-
8 ations procedures; and

9 (8) developing procedures to respond to requests for information
10 from the media or the public.

11 (b) ISSUANCE AND PROMOTION.—Any guidance or recommendations de-
12 veloped or best practices identified under subsection (a) shall be—

13 (1) issued through the Administrator; and

14 (2) promoted by the Secretary to the private sector.

15 (c) SMALL BUSINESS CONCERNS.—In developing guidance or rec-
16 ommendations or identifying best practices under subsection (a), the Admin-
17 istrator and the Director of the Cybersecurity and Infrastructure Security
18 Agency shall take into consideration small business concerns (under the
19 meaning given that term in section 3 of the Small Business Act (15 U.S.C.
20 632)), including a need for separate guidance or recommendations or best
21 practices, as necessary and appropriate.

22 (d) RULE OF CONSTRUCTION.—Nothing in this section may be construed
23 to supersede a requirement established under any other provision of law.

24 **§ 11320. Voluntary private-sector preparedness accredita-**
25 **tion and certification program**

26 (a) ESTABLISHMENT.—

27 (1) IN GENERAL.—The Secretary, acting through the officer des-
28 igned under paragraph (2), shall establish and implement the vol-
29 untary private-sector preparedness accreditation and certification pro-
30 gram under this section.

31 (2) DESIGNATION OF OFFICER.—The Secretary shall designate an
32 officer responsible for the accreditation and certification program under
33 this section. The officer (in this section referred to as the “designated
34 officer”) shall be one of the following:

35 (A) The Administrator, based on consideration of—

36 (i) the expertise of the Administrator in emergency man-
37 agement and preparedness in the United States; and

38 (ii) the responsibilities of the Administrator as the prin-
39 cipal advisor to the President for all matters relating to emer-
40 gency management in the United States.

1 (B) The Assistant Director for Infrastructure Security, based
2 on consideration of the expertise of the Assistant Director in, and
3 responsibilities for—

- 4 (i) protection of critical infrastructure;
- 5 (ii) risk assessment methodologies; and
- 6 (iii) interaction with the private sector on the issues de-
7 scribed in clauses (i) and (ii).

8 (C) The Under Secretary for Science and Technology, based on
9 consideration of the expertise of the Under Secretary in, and re-
10 sponsibilities associated with, standards.

11 (3) COORDINATION.—In carrying out the accreditation and certifi-
12 cation program under this section, the designated officer shall coordi-
13 nate with—

14 (A) the other officers of the Department referred to in para-
15 graph (2), using the expertise and responsibilities of the officers;
16 and

17 (B) the Special Assistant to the Secretary for the private sector,
18 based on consideration of the expertise of the Special Assistant in,
19 and responsibilities for, interacting with the private sector.

20 (b) VOLUNTARY PRIVATE-SECTOR PREPAREDNESS STANDARDS; VOL-
21 UNTARY ACCREDITATION AND CERTIFICATION PROGRAM FOR THE PRIVATE
22 SECTOR.—

23 (1) ACCREDITATION AND CERTIFICATION PROGRAM.—The designated
24 officer shall—

25 (A) begin supporting the development and updating, as nec-
26 essary, of voluntary preparedness standards through appropriate
27 organizations that coordinate or facilitate the development and use
28 of voluntary consensus standards and voluntary consensus stand-
29 ards development organizations; and

30 (B) in consultation with representatives of appropriate organiza-
31 tions that coordinate or facilitate the development and use of vol-
32 untary consensus standards, appropriate voluntary consensus
33 standards development organizations, each private-sector advisory
34 council created under section 10320(4) of this title, appropriate
35 representatives of State and local governments, including emer-
36 gency management officials, and appropriate private-sector advi-
37 sory groups, such as sector coordinating councils and information
38 sharing and analysis centers—

- 39 (i) develop and promote a program to certify the prepared-
40 ness of private-sector entities that voluntarily choose to seek
41 certification under the program; and

1 (ii) implement the program under this subsection through
2 an entity with which the designated officer enters into an
3 agreement under paragraph (3)(A), which shall accredit third
4 parties to carry out the certification process under this sec-
5 tion.

6 (2) PROGRAM ELEMENTS.—

7 (A) IN GENERAL.—

8 (i) The program developed and implemented under this
9 subsection shall assess whether a private-sector entity com-
10 plies with voluntary preparedness standards.

11 (ii) In developing the program under this subsection, the
12 designated officer shall develop guidelines for the accredita-
13 tion and certification processes established under this sub-
14 section.

15 (B) STANDARDS.—The designated officer, in consultation with
16 representatives of appropriate organizations that coordinate or fa-
17 cilitate the development and use of voluntary consensus standards,
18 representatives of appropriate voluntary consensus standards de-
19 velopment organizations, each private-sector advisory council cre-
20 ated under section 10320(4) of this title, appropriate representa-
21 tives of State and local governments, including emergency manage-
22 ment officials, and appropriate private-sector advisory groups such
23 as sector coordinating councils and information sharing and anal-
24 ysis centers—

25 (i) shall adopt one or more appropriate voluntary prepared-
26 ness standards that promote preparedness, which may be tai-
27 lored to address the unique nature of various sectors in the
28 private sector, as necessary and appropriate, that shall be
29 used in the accreditation and certification program under this
30 subsection; and

31 (ii) after the adoption of one or more standards under
32 clause (i), may adopt additional voluntary preparedness
33 standards or modify or discontinue the use of voluntary pre-
34 paredness standards for the accreditation and certification
35 program, as necessary and appropriate to promote prepared-
36 ness.

37 (C) SUBMISSION OF RECOMMENDATIONS.—In adopting one or
38 more standards under subparagraph (B), the designated officer
39 may receive recommendations from an entity described in that
40 subparagraph relating to appropriate voluntary preparedness

1 standards, including appropriate sector-specific standards, for
2 adoption in the program.

3 (D) SMALL BUSINESS CONCERNS.—The designated officer and
4 an entity with which the designated officer enters into an agree-
5 ment under paragraph (3)(A) shall establish separate classifica-
6 tions and methods of certification for small business concerns
7 (under the meaning given that term in section 3 of the Small
8 Business Act (15 U.S.C. 632)) for the program under this sub-
9 section.

10 (E) CONSIDERATIONS.—In developing and implementing the
11 program under this subsection, the designated officer shall—

12 (i) consider the unique nature of various sectors in the pri-
13 vate sector, including preparedness standards, business con-
14 tinuity standards, or best practices, established—

15 (I) under any other provision of Federal law; or

16 (II) by a Sector Risk Management Agency, as defined
17 under Homeland Security Presidential Directive–7; and

18 (ii) coordinate the program, as appropriate, with—

19 (I) other Department private-sector-related programs;
20 and

21 (II) preparedness and business continuity programs in
22 other Federal agencies.

23 (3) ACCREDITATION AND CERTIFICATION PROCESSES.—

24 (A) AGREEMENT.—

25 (i) The designated officer shall enter into one or more
26 agreements with a highly qualified nongovernmental entity
27 with experience or expertise in coordinating and facilitating
28 the development and use of voluntary consensus standards
29 and in managing or implementing accreditation and certifi-
30 cation programs for voluntary consensus standards, or a simi-
31 larly qualified private-sector entity, to carry out accreditations
32 and oversee the certification process under this subsection. An
33 entity entering into an agreement with the designated officer
34 under this clause (in this section referred to as a “selected
35 entity”) shall not perform certifications under this subsection.

36 (ii) A selected entity shall manage the accreditation process
37 and oversee the certification process in accordance with the
38 program established under this subsection and accredit quali-
39 fied third parties to carry out the certification program estab-
40 lished under this subsection.

1 (B) PROCEDURES AND REQUIREMENTS FOR ACCREDITATION
2 AND CERTIFICATION.—

3 (i) COLLABORATION.—A selected entity shall collaborate to
4 develop procedures and requirements for the accreditation
5 and certification processes under this subsection, in accord-
6 ance with the program established under this subsection and
7 guidelines developed under paragraph (2)(A)(ii).

8 (ii) REASONABLE UNIFORMITY; USE.—The procedures and
9 requirements developed under clause (i) shall—

10 (I) ensure reasonable uniformity in accreditation and
11 certification processes if there is more than one selected
12 entity; and

13 (II) be used by a selected entity in conducting accredi-
14 tations and overseeing the certification process under
15 this subsection.

16 (iii) RESOLUTION OF DISAGREEMENT.—A disagreement
17 among selected entities in developing procedures under clause
18 (i) shall be resolved by the designated officer.

19 (C) DESIGNATION.—A selected entity may accredit a qualified
20 third party to carry out the certification process under this sub-
21 section.

22 (D) DISADVANTAGED BUSINESS INVOLVEMENT.—In accrediting
23 qualified third parties to carry out the certification process under
24 this subsection, a selected entity shall ensure, to the extent prac-
25 ticable, that the third parties include qualified small, minority,
26 women-owned, or disadvantaged business concerns when appro-
27 priate. The term “disadvantaged business concern” means a small
28 business that is owned and controlled by socially and economically
29 disadvantaged individuals, as defined in part 124 of title 13, Code
30 of Federal Regulations.

31 (E) TREATMENT OF OTHER CERTIFICATIONS.—At the request
32 of an entity seeking certification, a selected entity may consider,
33 as appropriate, other relevant certifications acquired by the entity
34 seeking certification. If the selected entity determines that the
35 other certifications are sufficient to meet the certification require-
36 ment or aspects of the certification requirement under this section,
37 the selected entity may give credit to the entity seeking certifi-
38 cation, as appropriate, to avoid unnecessarily duplicative certifi-
39 cation requirements.

40 (F) THIRD PARTIES.—To be accredited under subparagraph
41 (C), a third party shall—

1 (i) demonstrate that the third party has the ability to cer-
2 tify private-sector entities in accordance with the procedures
3 and requirements developed under subparagraph (B);

4 (ii) agree to perform certifications in accordance with the
5 procedures and requirements;

6 (iii) agree not to have a beneficial interest in or direct or
7 indirect control over—

8 (I) a private-sector entity for which that third party
9 conducts a certification under this subsection; or

10 (II) an organization that provides preparedness con-
11 sulting services to private-sector entities;

12 (iv) agree not to have any other conflict of interest with re-
13 spect to a private-sector entity for which the third party con-
14 ducts a certification under this subsection;

15 (v) maintain liability insurance coverage at policy limits in
16 accordance with the requirements developed under subpara-
17 graph (B); and

18 (vi) enter into an agreement with the selected entity ac-
19 crediting that third party to protect proprietary information
20 of a private-sector entity obtained under this subsection.

21 (G) MONITORING.—

22 (i) ENSURE COMPLIANCE.—The designated officer and a
23 selected entity shall regularly monitor and inspect the oper-
24 ations of a third party conducting certifications under this
25 subsection to ensure that the third party is complying with
26 the procedures and requirements established under subpara-
27 graph (B) and all other applicable requirements.

28 (ii) PROCEDURES OR REQUIREMENTS NOT MET.—If the
29 designated officer or a selected entity determines that a third
30 party is not following the procedures or meeting the require-
31 ments established under subparagraph (B), the selected entity
32 shall—

33 (I) revoke the accreditation of that third party to con-
34 duct certifications under this subsection; and

35 (II) review the certifications conducted by that third
36 party, as necessary and appropriate.

37 (4) ANNUAL REVIEW.—

38 (A) IN GENERAL.—The designated officer, in consultation with
39 representatives of appropriate organizations that coordinate or fa-
40 cilitate the development and use of voluntary consensus standards,
41 appropriate voluntary consensus standards development organiza-

1 tions, appropriate representatives of State and local governments,
2 including emergency management officials, and each private-sector
3 advisory council created under section 10320(4) of this title, shall
4 annually review the voluntary accreditation and certification pro-
5 gram established under this subsection to ensure the effectiveness
6 of the program (including the operations and management of the
7 program by a selected entity and the selected entity's inclusion of
8 qualified disadvantaged business concerns under paragraph
9 (3)(D)) and make improvements and adjustments to the program
10 as necessary and appropriate.

11 (B) REVIEW OF STANDARDS.—Each review under subparagraph
12 (A) shall include an assessment of the voluntary preparedness
13 standard or standards used in the program under this subsection.

14 (5) VOLUNTARY PARTICIPATION.—Certification under this subsection
15 shall be voluntary for a private-sector entity.

16 (6) PUBLIC LISTING.—The designated officer shall maintain and
17 make public a listing of any private-sector entity certified as being in
18 compliance with the program established under this subsection, if that
19 private-sector entity consents to the listing.

20 (c) RULE OF CONSTRUCTION.—Nothing in this section may be construed
21 as—

22 (1) a requirement to replace preparedness, emergency response, or
23 business continuity standards, requirements, or best practices estab-
24 lished—

25 (A) under any other provision of federal law; or

26 (B) by a Sector Risk Management Agency, as defined under
27 Homeland Security Presidential Directive-7; or

28 (2) an exemption of a private-sector entity seeking certification or
29 meeting certification requirements under subsection (b) from compli-
30 ance with all applicable statutes, regulations, directives, policies, and
31 industry codes of practice.

32 **§ 11321. Acceptance of gifts**

33 (a) AUTHORITY.—The Secretary may accept and use gifts of property,
34 both real and personal, and may accept gifts of services, including from
35 guest lecturers, for otherwise authorized activities of the Center for Domes-
36 tic Preparedness that are related to efforts to prevent, prepare for, protect
37 against, or respond to a natural disaster, act of terrorism, or other man-
38 made disaster, including the use of a weapon of mass destruction.

39 (b) PROHIBITION.—The Secretary may not accept a gift under this sec-
40 tion if the Secretary determines that the use of the property or services
41 would compromise the integrity or appearance of integrity of—

- 1 (1) a program of the Department; or
2 (2) an individual involved in a program of the Department.

3 (c) REPORT.—

4 (1) IN GENERAL.—The Secretary shall submit to the Committee on
5 Homeland Security of the House of Representatives and the Committee
6 on Homeland Security and Governmental Affairs of the Senate an an-
7 nual report disclosing—

8 (A) gifts that were accepted under this section during the year
9 covered by the report;

10 (B) how the gifts contribute to the mission of the Center for
11 Domestic Preparedness; and

12 (C) the amount of Federal savings that were generated from the
13 acceptance of the gifts.

14 (2) PUBLICATION.—Each report required under paragraph (1) shall
15 be made publicly available.

16 **§ 11322. Integrated public alert and warning system mod-**
17 **ernization**

18 (a) IN GENERAL.—To provide timely and effective warnings regarding
19 natural disasters, acts of terrorism, and other man-made disasters or
20 threats to public safety, the Administrator shall—

21 (1) modernize the integrated public alert and warning system of the
22 United States (in this section referred to as the “public alert and warn-
23 ing system”) to help ensure that under all conditions the President
24 and, except to the extent the public alert and warning system is in use
25 by the President, Federal agencies and State, tribal, and local govern-
26 ments can alert and warn the civilian population in areas endangered
27 by natural disasters, acts of terrorism, and other man-made disasters
28 or threats to public safety; and

29 (2) implement the public alert and warning system to disseminate
30 timely and effective warnings regarding natural disasters, acts of ter-
31 rorism, and other man-made disasters or threats to public safety.

32 (b) IMPLEMENTATION REQUIREMENTS.—In carrying out subsection (a),
33 the Administrator shall—

34 (1) establish or adopt, as appropriate, common alerting and warning
35 protocols, standards, terminology, and operating procedures for the
36 public alert and warning system;

37 (2) include in the public alert and warning system the capability to
38 adapt the distribution and content of communications on the basis of
39 geographic location, risks, and multiple communication systems and
40 technologies, as appropriate and to the extent technically feasible;

1 (3) include in the public alert and warning system the capability to
2 alert, warn, and provide equivalent information to individuals with dis-
3 abilities, individuals with access and functional needs, and individuals
4 with limited-English proficiency, to the extent technically feasible;

5 (4) ensure that training, tests, and exercises are conducted for the
6 public alert and warning system, including by—

7 (A) incorporating the public alert and warning system into other
8 training and exercise programs of the Department, as appropriate;

9 (B) establishing and integrating into the National Incident
10 Management System a comprehensive and periodic training pro-
11 gram to instruct and educate Federal, State, tribal, and local gov-
12 ernment officials in the use of the Common Alerting Protocol en-
13 abled Emergency Alert System; and

14 (C) conducting, not less than once every 3 years, periodic na-
15 tionwide tests of the public alert and warning system;

16 (5) to the extent practicable, ensure that the public alert and warn-
17 ing system is resilient and secure and can withstand acts of terrorism
18 and other external attacks;

19 (6) conduct public education efforts so that State, tribal, and local
20 governments, private entities, and the people of the United States rea-
21 sonably understand the functions of the public alert and warning sys-
22 tem and how to access, use, and respond to information from the public
23 alert and warning system through a general market awareness cam-
24 paign;

25 (7) consult, coordinate, and cooperate with the appropriate private-
26 sector entities and Federal, State, tribal, and local governmental au-
27 thorities, including the Regional Administrators and emergency re-
28 sponse providers;

29 (8) consult and coordinate with the Federal Communications Com-
30 mission, taking into account rules and regulations promulgated by the
31 Federal Communications Commission; and

32 (9) coordinate with and consider the recommendations of the Inte-
33 grated Public Alert and Warning System Subcommittee established
34 under section 2(b) of the Integrated Public Alert and Warning System
35 Modernization Act of 2015 (Public Law 114–143, 130 Stat. 329).

36 (e) SYSTEM REQUIREMENTS.—The public alert and warning system
37 shall—

38 (1) to the extent determined appropriate by the Administrator, incor-
39 porate multiple communications technologies;

40 (2) be designed to adapt to, and incorporate, future technologies for
41 communicating directly with the public;

- 1 (3) to the extent technically feasible, be designed—
- 2 (A) to provide alerts to the largest portion of the affected popu-
- 3 lation feasible, including nonresident visitors and tourists, individ-
- 4 uals with disabilities, individuals with access and functional needs,
- 5 and individuals with limited-English proficiency; and
- 6 (B) to improve the ability of remote areas to receive alerts;
- 7 (4) promote local and regional public and private partnerships to en-
- 8 hance community preparedness and response;
- 9 (5) provide redundant alert mechanisms where practicable so as to
- 10 reach the greatest number of people; and
- 11 (6) to the extent feasible, include a mechanism to ensure the protec-
- 12 tion of individual privacy.
- 13 (d) USE OF SYSTEM.—Except to the extent necessary for testing the pub-
- 14 lic alert and warning system, the public alert and warning system shall not
- 15 be used to transmit a message that does not relate to a natural disaster,
- 16 act of terrorism, or other man-made disaster or threat to public safety.
- 17 (e) PERFORMANCE REPORTS.—
- 18 (1) IN GENERAL.—Not later than April 11, 2017, and 2018, the Ad-
- 19 ministrator shall make available on the public website of the Agency
- 20 a performance report, which shall—
- 21 (A) establish performance goals for the implementation of the
- 22 public alert and warning system by the Agency;
- 23 (B) describe the performance of the public alert and warning
- 24 system, including—
- 25 (i) the type of technology used for alerts and warnings
- 26 issued under the system;
- 27 (ii) the measures taken to alert, warn, and provide equiva-
- 28 lent information to individuals with disabilities, individuals
- 29 with access and functional needs, and individuals with lim-
- 30 ited-English proficiency; and
- 31 (iii) the training, tests, and exercises performed and the
- 32 outcomes obtained by the Agency;
- 33 (C) identify significant challenges to the effective operation of
- 34 the public alert and warning system and any plans to address the
- 35 challenges;
- 36 (D) identify other necessary improvements to the system; and
- 37 (E) provide an analysis comparing the performance of the public
- 38 alert and warning system with the performance goals established
- 39 under subparagraph (A).
- 40 (2) SUBMISSION TO CONGRESS.—The Administrator shall submit to
- 41 the Committee on Homeland Security and Governmental Affairs and

1 the Committee on Commerce, Science, and Transportation of the Sen-
2 ate and the Committee on Transportation and Infrastructure and the
3 Committee on Homeland Security of the House of Representatives each
4 report required under paragraph (1).

5 **§ 11323. Integrated public alert and warning system**

6 (a) DEFINITIONS.—In this section:

7 (1) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term “appro-
8 priate congressional committees” means—

9 (A) the Committee on Homeland Security and Governmental
10 Affairs of the Senate;

11 (B) the Committee on Transportation and Infrastructure of the
12 House of Representatives; and

13 (C) the Committee on Homeland Security of the House of Rep-
14 resentatives.

15 (2) PUBLIC ALERT AND WARNING SYSTEM.—The term “public alert
16 and warning system” means the integrated public alert and warning
17 system of the United States described in section 11322 of this title.

18 (3) STATE.—The term “State” means a State, the District of Co-
19 lumbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the
20 Northern Mariana Islands, and any possession of the United States.

21 (b) INTEGRATED PUBLIC ALERT AND WARNING SYSTEM.—

22 (1) MINIMUM REQUIREMENTS.—Not later than 1 year after Decem-
23 ber 20, 2019, the Administrator shall develop minimum requirements
24 for State, Tribal, and local governments to participate in the public
25 alert and warning system and that are necessary to maintain the integ-
26 rity of the public alert and warning system, including—

27 (A) guidance on the categories of public emergencies and appro-
28 priate circumstances that warrant an alert and warning from
29 State, Tribal, and local governments using the public alert and
30 warning system;

31 (B) the procedures for State, Tribal, and local government offi-
32 cials to authenticate civil emergencies and initiate, modify, and
33 cancel alerts transmitted through the public alert and warning sys-
34 tem, including protocols and technology capabilities for—

35 (i) the initiation, or prohibition on the initiation, of alerts
36 by a single authorized or unauthorized individual;

37 (ii) testing a State, Tribal, or local government incident
38 management and warning tool without accidentally initiating
39 an alert through the public alert and warning system; and

1 (iii) steps a State, Tribal, or local government official
2 should take to mitigate the possibility of the issuance of a
3 false alert through the public alert and warning system;

4 (C) the standardization, functionality, and interoperability of in-
5 cident management and warning tools used by State, Tribal, and
6 local governments to notify the public of an emergency through
7 the public alert and warning system;

8 (D) the annual training and recertification of emergency man-
9 agement personnel on requirements for originating and transmit-
10 ting an alert through the public alert and warning system;

11 (E) the procedures, protocols, and guidance concerning the pro-
12 tective action plans that State, Tribal, and local governments shall
13 issue to the public following an alert issued under the public alert
14 and warning system;

15 (F) the procedures, protocols, and guidance concerning the com-
16 munications that State, Tribal, and local governments shall issue
17 to the public following a false alert issued under the public alert
18 and warning system;

19 (G) a plan by which State, Tribal, and local government officials
20 may, during an emergency, contact each other as well as Federal
21 officials and participants in the Emergency Alert System and the
22 Wireless Emergency Alert System, when appropriate and nec-
23 essary, by telephone, text message, or other means of communica-
24 tion regarding an alert that has been distributed to the public; and

25 (H) any other procedure the Administrator considers appro-
26 priate for maintaining the integrity of and providing for public
27 confidence in the public alert and warning system.

28 (2) COORDINATION WITH NATIONAL ADVISORY COUNCIL REPORT.—
29 The Administrator shall ensure that the minimum requirements devel-
30 oped under paragraph (1) do not conflict with recommendations made
31 for improving the public alert and warning system provided in the re-
32 port submitted by the National Advisory Council under section
33 2(b)(7)(B) of the Integrated Public Alert and Warning System Mod-
34 ernization Act of 2015 (Public Law 114–143, 130 Stat. 332).

35 (3) PUBLIC CONSULTATION.—In developing the minimum require-
36 ments under paragraph (1), the Administrator shall ensure appropriate
37 public consultation and, to the extent practicable, coordinate the devel-
38 opment of the requirements with stakeholders of the public alert and
39 warning system, including—

1 (A) appropriate personnel from Federal agencies, including the
2 National Institute of Standards and Technology, the Agency, and
3 the Federal Communications Commission;

4 (B) representatives of State and local governments and emer-
5 gency services personnel, who shall be selected from among indi-
6 viduals nominated by national organizations representing those
7 governments and personnel;

8 (C) representatives of Federally recognized Indian tribes and
9 national Indian organizations;

10 (D) communications service providers;

11 (E) vendors, developers, and manufacturers of systems, facili-
12 ties, equipment, and capabilities for the provision of communica-
13 tions services;

14 (F) third-party service bureaus;

15 (G) the national organization representing the licensees and per-
16 mittees of noncommercial broadcast television stations;

17 (H) technical experts from the broadcasting industry;

18 (I) educators from the Emergency Management Institute; and

19 (J) other individuals with technical expertise as the Adminis-
20 trator determines appropriate.

21 (4) ADVICE TO THE ADMINISTRATOR.—In accordance with the chap-
22 ter 10 of title 5, the Administrator may obtain advice from an indi-
23 vidual or non-consensus advice from each of the several members of a
24 group without invoking that Act.

25 (e) INCIDENT MANAGEMENT AND WARNING TOOL VALIDATION.—

26 (1) ESTABLISHMENT.—The Administrator shall establish a process
27 to ensure that an incident management and warning tool used by a
28 State, Tribal, or local government to originate and transmit an alert
29 through the public alert and warning system meets the requirements
30 developed by the Administrator under subsection (b)(1).

31 (2) REQUIREMENTS.—The process required to be established under
32 paragraph (1) shall include—

33 (A) the ability to test an incident management and warning tool
34 in the public alert and warning system lab;

35 (B) the ability to certify that an incident management and
36 warning tool complies with the applicable cyber frameworks of the
37 Department and the National Institute of Standards and Tech-
38 nology;

39 (C) a process to certify developers of emergency management
40 software; and

1 (D) requiring developers to provide the Administrator with a
2 copy of, and rights of use for, ongoing testing of each version of
3 incident management and warning tool software before the soft-
4 ware is first used by a State, Tribal, or local government.

5 (d) REVIEW AND UPDATE OF MEMORANDA OF UNDERSTANDING.—The
6 Administrator shall review the memoranda of understanding between the
7 Agency and State, Tribal, and local governments with respect to the public
8 alert and warning system to ensure that all agreements ensure compliance
9 with the requirements developed by the Administrator under subsection
10 (b)(1).

11 (e) FUTURE MEMORANDA.—On and after the date that is 60 days after
12 the date on which the Administrator issues the requirements developed
13 under subsection (b)(1), any new memorandum of understanding entered
14 into between the Agency and a State, Tribal, or local government with re-
15 spect to the public alert and warning system shall comply with those re-
16 quirements.

17 (f) MISSILE ALERT AND WARNING AUTHORITIES.—

18 (1) IN GENERAL.—

19 (A) AUTHORITY.—The authority to originate an alert warning
20 the public of a missile launch directed against a State using the
21 public alert and warning system shall reside primarily with the
22 Federal Government.

23 (B) DELEGATION OF AUTHORITY.—The Secretary may delegate
24 the authority described in subparagraph (A) to a State, Tribal, or
25 local entity if, not later than 180 days after December 20, 2019,
26 the Secretary submitted a report to the appropriate congressional
27 committees that—

28 (i) it is not feasible for the Federal Government to alert
29 the public of a missile threat against a State; or

30 (ii) it is not in the national security interest of the United
31 States for the Federal Government to alert the public of a
32 missile threat against a State.

33 (C) ACTIVATION OF SYSTEM.—On verification of a missile
34 threat, the President, utilizing established authorities, protocols
35 and procedures, may activate the public alert and warning system.

36 (D) CONSTRUCTION.—Nothing in this paragraph shall be con-
37 strued to change the command and control relationship between
38 entities of the Federal Government with respect to the identifica-
39 tion, dissemination, notification, or alerting of information of mis-
40 sile threats against the United States that was in effect on the day
41 before December 20, 2019.

1 (2) NOTIFICATION PROCESS.—The Secretary, acting through the Ad-
2 ministrator, shall establish a process to promptly notify a State warn-
3 ing point, and any State entities that the Administrator determines ap-
4 propriate, following the issuance of an alert described in paragraph
5 (1)(A) so the State may take appropriate action to protect the health,
6 safety, and welfare of the residents of the State.

7 (3) WORK WITH GOVERNOR.—The Secretary, acting through the Ad-
8 ministrator, shall work with the Governor of a State warning point to
9 develop and implement appropriate protective action plans to respond
10 to an alert described in paragraph (1)(A) for that State.

11 (4) STUDY AND REPORT.—Not later than 1 year after December 20,
12 2019, the Secretary shall—

13 (A) examine the feasibility of establishing an alert designation
14 under the public alert and warning system that would be used to
15 alert and warn the public of a missile threat while concurrently
16 alerting a State warning point so that a State may activate related
17 protective action plans; and

18 (B) submit a report of the findings under subparagraph (A), in-
19 cluding of the costs and timeline for taking action to implement
20 an alert designation described in subparagraph (A), to—

21 (i) the Subcommittee on Homeland Security of the Com-
22 mittee on Appropriations of the Senate;

23 (ii) the Committee on Homeland Security and Govern-
24 mental Affairs of the Senate;

25 (iii) the Subcommittee on Homeland Security of the Com-
26 mittee on Appropriations of the House of Representatives;

27 (iv) the Committee on Transportation and Infrastructure of
28 the House of Representatives; and

29 (v) the Committee on Homeland Security of the House of
30 Representatives.

31 (g) USE OF INTEGRATED PUBLIC ALERT AND WARNING SYSTEM LAB.—
32 Not later than 1 year after December 20, 2019, the Administrator shall—

33 (1) develop a program to increase the utilization of the public alert
34 and warning system lab of the Agency by State, Tribal, and local gov-
35 ernments to test incident management and warning tools and train
36 emergency management professionals on alert origination protocols and
37 procedures; and

38 (2) submit to the appropriate congressional committees a report de-
39 scribing—

40 (A) the impact on utilization of the public alert and warning
41 system lab by State, Tribal, and local governments, with particular

1 attention given to the impact on utilization in rural areas, result-
2 ing from the program developed under paragraph (1); and

3 (B) any further recommendations that the Administrator would
4 make for additional statutory or appropriations authority nec-
5 essary to increase the utilization of the public alert and warning
6 system lab by State, Tribal, and local governments.

7 (h) REVIEW OF AWARENESS OF ALERTS AND WARNINGS.—Not later
8 than 1 year after December 20, 2019, the Administrator shall—

9 (1) conduct a review of the National Watch Center and each Re-
10 gional Watch Center of the Agency; and

11 (2) submit to the appropriate congressional committees a report on
12 the review conducted under paragraph (1), which shall include—

13 (A) an assessment of the technical capability of the National
14 and Regional Watch Centers described in paragraph (1) to be no-
15 tified of alerts and warnings issued by a State through the public
16 alert and warning system;

17 (B) a determination of which State alerts and warnings the Na-
18 tional and Regional Watch Centers described in paragraph (1)
19 should be aware of; and

20 (C) recommendations for improving the ability of the National
21 and Regional Watch Centers described in paragraph (1) to receive
22 State alerts and warnings that the Administrator determines are
23 appropriate.

24 (i) REPORTING FALSE ALERTS.—Not later than 15 days after the date
25 on which a State, Tribal, or local government official transmits a false alert
26 under the public alert and warning system, the Administrator shall report
27 to the appropriate congressional committees on—

28 (1) the circumstances surrounding the false alert;

29 (2) the content, cause, and population impacted by the false alert;
30 and

31 (3) any efforts to mitigate any negative impacts of the false alert.

32 (j) REPORTING PARTICIPATION RATES.—The Administrator shall, on an
33 annual basis, report to the appropriate congressional committees on—

34 (1) participation rates in the public alert and warning system; and

35 (2) efforts to expand alert, warning, and interoperable communica-
36 tions to rural and underserved areas.

37 (k) TIMELINE FOR COMPLIANCE.—Each State shall be given a reasonable
38 amount of time to comply with new rules, regulations, or requirements im-
39 posed under this section.

40 **§ 11324. National planning and education**

41 The Secretary shall, to the extent practicable—

1 (1) include in national planning frameworks the threat of an EMP
2 or GMD event; and

3 (2) conduct outreach to educate owners and operators of critical in-
4 frastructure, emergency planners, and emergency response providers at
5 all levels of government regarding threats of EMP and GMD.

6 **§ 11325. Coordination of Department efforts related to food,**
7 **agriculture, and veterinary defense against ter-**
8 **rorism**

9 (a) PROGRAM.—The Secretary, acting through the Assistant Secretary for
10 the Countering Weapons of Mass Destruction Office, shall carry out a pro-
11 gram to coordinate the Department’s efforts related to defending the food,
12 agriculture, and veterinary systems of the United States against terrorism
13 and other high-consequence events that pose a high risk to homeland secu-
14 rity.

15 (b) PROGRAM ELEMENTS.—The coordination program required by sub-
16 section (a) shall include, at a minimum, the following:

17 (1) Providing oversight and management of the Department’s re-
18 sponsibilities pursuant to Homeland Security Presidential Directive–
19 9—Defense of United States Agriculture and Food.

20 (2) Providing oversight and integration of the Department’s activi-
21 ties related to veterinary public health, food defense, and agricultural
22 security.

23 (3) Leading the Department’s policy initiatives relating to food, ani-
24 mal, and agricultural incidents, and the impact of the incidents on ani-
25 mal and public health.

26 (4) Leading the Department’s policy initiatives relating to overall do-
27 mestic preparedness for and collective response to agricultural ter-
28 rorism.

29 (5) Coordinating with other Department components, including U.S.
30 Customs and Border Protection, as appropriate, on activities related to
31 food and agriculture security and screening procedures for domestic
32 and imported products.

33 (6) Coordinating with appropriate Federal departments and agen-
34 cies.

35 (7) Engaging in other activities as determined necessary by the Sec-
36 retary.

37 (c) AUTHORITY NOT ALTERED OR SUPERSEDED.—Nothing in this sec-
38 tion may be construed as altering or superseding the authority of the Sec-
39 retary of Agriculture or the Secretary of Health and Human Services.

1 **§ 11326. Transfer of equipment during a public health emer-**
2 **gency**

3 (a) AUTHORIZATION OF TRANSFER OF EQUIPMENT.—During a public
4 health emergency declared by the Secretary of Health and Human Services
5 under section 319(a) of the Public Health Service Act (42 U.S.C. 247d(a)),
6 the Secretary, at the request of the Secretary of Health and Human Serv-
7 ices, may transfer to the Department of Health and Human Services, on
8 a reimbursable basis, excess personal protection equipment or medically nec-
9 essary equipment in the possession of the Department.

10 (b) DETERMINATION BY SECRETARIES.—

11 (1) IN GENERAL.—In carrying out this section—

12 (A) before requesting a transfer under subsection (a), the Sec-
13 retary of Health and Human Services shall determine whether the
14 personal protective equipment or medically necessary equipment is
15 otherwise available; and

16 (B) before initiating a transfer under subsection (a), the Sec-
17 retary, in consultation with the heads of each component in the
18 Department, shall—

19 (i) determine whether the personal protective equipment or
20 medically necessary equipment requested to be transferred
21 under subsection (a) is excess equipment; and

22 (ii) certify that the transfer of the personal protective
23 equipment or medically necessary equipment will not ad-
24 versely impact the health or safety of officers, employees, or
25 contractors of the Department.

26 (2) NOTIFICATION.—The Secretary of Health and Human Services
27 and the Secretary shall each submit to Congress a notification explain-
28 ing the determination made under subparagraphs (A) and (B), respec-
29 tively, of paragraph (1).

30 (3) REQUIRED INVENTORY.—

31 (A) IN GENERAL.—The Secretary shall—

32 (i) acting through the Chief Medical Officer, maintain an
33 inventory of all personal protective equipment and medically
34 necessary equipment in the possession of the Department;
35 and

36 (ii) make the inventory required under clause (i) available,
37 on a continual basis, to—

38 (I) the Secretary of Health and Human Services; and

39 (II) the Committee on Appropriations and the Com-
40 mittee on Homeland Security and Governmental Affairs
41 of the Senate and the Committee on Appropriations and

1 the Committee on Homeland Security of the House of
2 Representatives.

3 (B) FORM.—Each inventory required to be made available
4 under subparagraph (A) shall be submitted in unclassified form
5 but may include a classified annex.

6 **§ 11327. Continuity of the economy plan**

7 (a) DEFINITIONS.—In this section:

8 (1) AGENCY.—The term “agency” has the meaning given that term
9 in section 551 of title 5.

10 (2) ECONOMIC SECTOR.—The term “economic sector” means a sec-
11 tor of the economy of the United States.

12 (3) RELEVANT ACTOR.—The term “relevant actor” means—

13 (A) the Federal Government;

14 (B) a State, local, or Tribal government; or

15 (C) the private sector.

16 (4) SIGNIFICANT EVENT.—The term “significant event” means an
17 event that causes sever degradation to economic activity in the United
18 States due to—

19 (A) a cyber attack; or

20 (B) another significant event that is natural or human-caused.

21 (5) STATE.—The term “State” means a State, the District of Co-
22 lumbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, the
23 Northern Mariana Islands, and a possession of the United States.

24 (b) REQUIREMENT.—

25 (1) IN GENERAL.—The President shall develop and maintain a plan
26 to maintain and restore the economy of the United States in response
27 to a significant event.

28 (2) PRINCIPLES.—The plan under paragraph (1) shall—

29 (A) be consistent with—

30 (i) a free market economy; and

31 (ii) the rule of law; and

32 (B) respect private property rights.

33 (3) CONTENTS.—The plan required under paragraph (1) shall—

34 (A) examine the distribution of goods and services across the
35 United States necessary for the reliable functioning of the United
36 States during a significant event;

37 (B) identify the economic functions of relevant actors, the dis-
38 ruption, corruption, or dysfunction of which would have a debili-
39 tating effect in the United States on—

40 (i) security;

41 (ii) economic security;

- 1 (iii) defense readiness; or
- 2 (iv) public health or safety;
- 3 (C) identify the critical distribution mechanisms for each eco-
- 4 nomic sector that should be prioritized for operation during a sig-
- 5 nificant event, including—
- 6 (i) bulk power and electric transmission systems;
- 7 (ii) national and international financial systems, including
- 8 wholesale payments, stocks, and currency exchanges;
- 9 (iii) national and international communications networks,
- 10 data-hosting services, and cloud services;
- 11 (iv) interstate oil and natural gas pipelines; and
- 12 (v) mechanisms for the interstate and international trade
- 13 and distribution of materials, food, and medical supplies, in-
- 14 cluding road, rail, air, and maritime shipping;
- 15 (D) identify economic functions of relevant actors, the disrup-
- 16 tion, corruption, or dysfunction of which would cause—
- 17 (i) catastrophic economic loss;
- 18 (ii) the loss of public confidence; or
- 19 (iii) the widespread imperilment of human life;
- 20 (E) identify the economic functions of relevant actors that are
- 21 so vital to the economy of the United States that the disruption,
- 22 corruption, or dysfunction of those economic functions would un-
- 23 dermine response, recovery, or mobilization efforts during a sig-
- 24 nificant event;
- 25 (F) incorporate, to the greatest extent practicable, the principles
- 26 and practices contained in Federal plans for the continuity of Gov-
- 27 ernment and continuity of operations;
- 28 (G) identify—
- 29 (i) industrial control networks for which a loss of internet
- 30 connectivity, a loss of network integrity or availability, an ex-
- 31 ploitation of a system connected to the network, or another
- 32 failure, disruption, corruption, or dysfunction would have a
- 33 debilitating effect in the United States on—
- 34 (I) security;
- 35 (II) economic security;
- 36 (III) defense readiness; or
- 37 (IV) public health or safety; and
- 38 (ii) for each industrial control network identified under
- 39 clause (i), risk mitigation measures, including—
- 40 (I) the installation of parallel services;
- 41 (II) the use of stand-alone analog services; or

1 (III) the significant hardening of the industrial control
2 network against failure, disruption, corruption, or dys-
3 function;

4 (H) identify critical economic sectors for which the preservation
5 of data in a protected, verified, and uncorrupted status would be
6 required for the quick recovery of the economy of the United
7 States in the face of a significant disruption following a significant
8 event;

9 (I) include a list of raw materials, industrial goods, and other
10 items, the absence of which would significantly undermine the abil-
11 ity of the United States to sustain the functions described in sub-
12 paragraphs (B), (D), and (E);

13 (J) provide an analysis of supply chain diversification for the
14 items described in subparagraph (I) in the event of a disruption
15 caused by a significant event;

16 (K) include—

17 (i) a recommendation as to whether the United States
18 should maintain a strategic reserve of 1 or more of the items
19 described in subparagraph (I); and

20 (ii) for each item described in subparagraph (I) for which
21 the President recommends maintaining a strategic reserve
22 under clause (i), an identification of mechanisms for tracking
23 inventory and availability of the item in the strategic reserve;

24 (L) identify mechanisms in existence on January 1, 2021, and
25 mechanisms that can be developed to ensure that the swift trans-
26 port and delivery of the items described in subparagraph (I) are
27 feasible in the event of a distribution network disturbance or deg-
28 radation, including a distribution network disturbance or degrada-
29 tion caused by a significant event;

30 (M) include guidance for determining the prioritization for the
31 distribution of the items described in subparagraph (I), including
32 distribution to States and Indian Tribes;

33 (N) consider the advisability and feasibility of mechanisms for
34 extending the credit of the United States or providing other finan-
35 cial support authorized by law to key participants in the economy
36 of the United States if the extension or provision of other financial
37 support—

38 (i) is necessary to avoid severe economic degradation; or

39 (ii) allows for the recovery from a significant event;

40 (O) include guidance for determining categories of employees
41 that should be prioritized to continue to work to sustain the func-

1 tions described in subparagraphs (B), (D), and (E) in the event
2 that there are limitations on the ability of individuals to travel to
3 workplaces or to work remotely, including considerations for de-
4 fense readiness;

5 (P) identify critical economic sectors necessary to provide mate-
6 rial and operational support to the defense of the United States;

7 (Q) determine whether the Secretary, the National Guard, and
8 the Secretary of Defense have adequate authority to assist the
9 United States in a recovery from a severe economic degradation
10 caused by a significant event;

11 (R) review and assess the authority and capability of heads of
12 other agencies that the President determines necessary to assist
13 the United States in a recovery from a severe economic degrada-
14 tion caused by a significant event; and

15 (S) consider any other matter that would aid in protecting and
16 increasing the resilience of the economy of the United States from
17 a significant event.

18 (e) COORDINATION.—In developing the plan required under subsection
19 (b)(1), the President shall—

20 (1) receive advice from—

21 (A) the Secretary;

22 (B) the Secretary of Defense;

23 (C) the Secretary of the Treasury;

24 (D) the Secretary of Health and Human Services;

25 (E) the Secretary of Commerce;

26 (F) the Secretary of Transportation;

27 (G) the Secretary of Energy;

28 (H) the Administrator of the Small Business Administration;

29 and

30 (I) the head of any other agency that the President determines
31 necessary to complete the plan;

32 (2) consult with economic sectors relating to critical infrastructure
33 through sector-coordinated councils, as appropriate;

34 (3) consult with relevant State, Tribal, and local governments and
35 organizations that represent those governments; and

36 (4) consult with any other non-Federal entity that the President de-
37 termines necessary to complete the plan.

38 (d) SUBMISSION TO CONGRESS.—

39 (1) IN GENERAL.—Not later than 2 years after January 1, 2021,
40 and not less frequently than every 3 years thereafter, the President

1 shall submit the plan required under subsection (b)(1) and the informa-
2 tion described in paragraph (2) to—

3 (A) the majority and minority leaders of the Senate;

4 (B) the Speaker and the minority leader of the House of Rep-
5 resentatives;

6 (C) the Committee on Armed Services of the Senate;

7 (D) the Committee on Armed Services of the House of Rep-
8 resentatives;

9 (E) the Committee on Homeland Security and Governmental
10 Affairs of the Senate;

11 (F) the Committee on Homeland Security of the House of Rep-
12 resentatives;

13 (G) the Committee on Health, Education, Labor, and Pensions
14 of the Senate;

15 (H) the Committee on Commerce, Science, and Transportation
16 of the Senate;

17 (I) the Committee on Energy and Commerce of the House of
18 Representatives;

19 (J) the Committee on Banking, Housing, and Urban Affairs of
20 the Senate;

21 (K) the Committee on Finance of the Senate;

22 (L) the Committee on Financial Services of the House of Rep-
23 resentatives;

24 (M) the Committee on Small Business and Entrepreneurship of
25 the Senate;

26 (N) the Committee on Small Business of the House of Rep-
27 resentatives;

28 (O) the Committee on Energy and Natural Resources of the
29 Senate;

30 (P) the Committee on Environment and Public Works of the
31 Senate;

32 (Q) the Committee on Indian Affairs of the Senate;

33 (R) the Committee on Oversight and Reform of the House of
34 Representatives;

35 (S) the Committee on the Budget of the House of Representa-
36 tives; and

37 (T) any other committee of the Senate or the House of Rep-
38 resentatives that has jurisdiction over the subject of the plan.

39 (2) ADDITIONAL INFORMATION.—The information described in this
40 paragraph is—

1 (A) any change to Federal law that would be necessary to carry
2 out the plan required under subsection (b)(1); and

3 (B) any proposed change to the funding levels provided in ap-
4 propriation Acts for the most recent fiscal year that can be imple-
5 mented in future appropriation Acts or additional resources nec-
6 essary to—

7 (i) implement the plan required under subsection (b)(1); or

8 (ii) maintain any program offices and personnel necessary
9 to—

10 (I) maintain the plan required under subsection (b)(1)
11 and the plans described in subsection (b)(3)(F); and

12 (II) conduct exercises, assessments, and updates to the
13 plans described in subclause (I) over time.

14 (3) INCLUSION IN BUDGET OF THE PRESIDENT.—The President may
15 include the information described in paragraph (2)(B) in the budget
16 the President is required to submit under section 1105(a) of title 31.

17 **§ 11328. Guidance on how to prevent exposure to and re-**
18 **lease of PFAS**

19 (a) IN GENERAL.—Not later than December 20, 2023, the Secretary, in
20 consultation with the Administrator of the United States Fire Administra-
21 tion, the Administrator of the Environmental Protection Agency, the Direc-
22 tor of the National Institute for Occupational Safety and Health, and the
23 heads of any other relevant agencies, shall—

24 (1) develop and publish guidance for firefighters and other emer-
25 gency response personnel on training, education programs, and best
26 practices;

27 (2) make available a curriculum designed to—

28 (A) reduce and eliminate exposure to per- and polyfluoroalkyl
29 substances (in this section referred to as “PFAS”) from fire-
30 fighting foam and personal protective equipment;

31 (B) prevent the release of PFAS from firefighting foam into the
32 environment; and

33 (C) educate firefighters and other emergency response personnel
34 on foams and non-foam alternatives, personal protective equip-
35 ment, and other firefighting tools and equipment that do not con-
36 tain PFAS; and

37 (3) create an online public repository, which shall be updated on a
38 regular basis, on tools and best practices for firefighters and other
39 emergency response personnel to reduce, limit, and prevent the release
40 of and exposure to PFAS.

41 (b) CURRICULUM.—

1 (1) IN GENERAL.—For the purpose of developing the curriculum re-
2 quired under subsection (a)(2), the Administrator of the United States
3 Fire Administration shall make recommendations to the Secretary as
4 to the content of the curriculum.

5 (2) CONSULTATION.—For the purpose of making recommendations
6 under paragraph (1), the Administrator of the United States Fire Ad-
7 ministration shall consult with interested entities, as appropriate, in-
8 cluding—

9 (A) firefighters and other emergency response personnel, includ-
10 ing national fire service and emergency response organizations;

11 (B) impacted communities dealing with PFAS contamination;

12 (C) scientists, including public and occupational health and
13 safety experts, who are studying PFAS and PFAS alternatives in
14 firefighting foam;

15 (D) voluntary-standards organizations engaged in developing
16 standards for firefighter and firefighting equipment;

17 (E) State fire training academies;

18 (F) State fire marshals;

19 (G) manufacturers of firefighting tools and equipment; and

20 (H) any other relevant entities, as determined by the Secretary
21 and the Administrator of the United States Fire Administration.

22 (c) REVIEW.—Not later than 3 years after the date on which the guid-
23 ance and curriculum required under subsection (a) is issued, and not less
24 frequently than once every 3 years thereafter, the Secretary, in consultation
25 with the Administrator of the United States Fire Administration, the Ad-
26 ministrator of the Environmental Protection Agency, and the Director of
27 the National Institute for Occupational Safety and Health, shall review the
28 guidance and curriculum and, as appropriate, issue updates to the guidance
29 and curriculum.

30 (d) INAPPLICABILITY OF CHAPTER 5 OF TITLE 10.—Chapter 5 of title 10
31 shall not apply to this section.

32 (e) RULE OF CONSTRUCTION.—Nothing in this chapter shall be construed
33 to require the Secretary to promulgate or enforce regulations under sub-
34 chapter II of chapter 5 of title 5.

35 **Subchapter II—Fire Prevention and** 36 **Control**

37 **§ 11351. Declaration of purpose**

38 It is declared to be the purpose of Congress in this subchapter to—

39 (1) reduce the Nation's losses caused by fire through better fire pre-
40 vention and control;

1 (2) supplement existing programs of research, training, and edu-
2 cation, and to encourage new and improved programs and activities by
3 State and local governments;

4 (3) establish the United States Fire Administration and the Fire Re-
5 search Center in the Federal Emergency Management Agency; and

6 (4) establish an intensified program of research into the treatment
7 of burn and smoke injuries and the rehabilitation of victims of fires in
8 the National Institutes of Health.

9 **§ 11352. Definitions**

10 As used in this subchapter:

11 (1) ACADEMY.—The term “Academy” means the National Academy
12 for Fire Prevention and Control.

13 (2) ADMINISTRATION.—The term “Administration” means the
14 United States Fire Administration established pursuant to section
15 11353 of this title.

16 (3) ADMINISTRATOR.—The term “Administrator” means the Admin-
17 istrator of the Administration, in the Federal Emergency Management
18 Agency.

19 (4) ADMINISTRATOR OF FEMA.—The term “Administrator of
20 FEMA” means the Administrator of the Federal Emergency Manage-
21 ment Agency;

22 (5) FIRE SERVICE.—

23 (A) IN GENERAL.—The term “fire service” means any organiza-
24 tion in a State consisting of personnel, apparatus, and equipment
25 that has as its purpose protecting property and maintaining the
26 safety and welfare of the public from the dangers of fire, including
27 a private firefighting brigade.

28 (B) PERSONNEL, LOCATION, AND RESPONSIBILITY.—The per-
29 sonnel of the organization may be paid employees or unpaid volun-
30 teers or any combination. The location of the organization and its
31 responsibility for extinguishment and suppression of fires may in-
32 clude a Federal installation, State, city, town, borough, parish,
33 county, Indian tribe, fire district, fire protection district, rural fire
34 district, or other special district.

35 (C) FIRE PREVENTION, FIREFIGHTING, FIRE CONTROL.—The
36 terms “fire prevention”, “firefighting”, and “fire control” relate to
37 activities conducted by a fire service.

38 (6) INDIAN TRIBE.—

39 (A) IN GENERAL.—The term “Indian tribe” has the meaning
40 given the term in section 4 of the Indian Self-Determination and
41 Education Assistance Act (25 U.S.C. 5304).

1 (B) TRIBAL.—The term “tribal” means of or pertaining to an
2 Indian tribe.

3 (7) LOCAL.—The term “local” means of or pertaining to a city,
4 town, county, special purpose district, unincorporated territory, or
5 other political subdivision of a State.

6 (8) PLACE OF PUBLIC ACCOMMODATION AFFECTING COMMERCE.—
7 The term “place of public accommodation affecting commerce”—

8 (A) means an inn, hotel, or other establishment not owned by
9 the Federal Government that provides lodging to transient guests;
10 but

11 (B) does not include an establishment—

12 (i) treated as an apartment building for purposes of a
13 State or local law or regulation; or

14 (ii) located in a building that contains not more than 5
15 rooms for rent or hire and that is actually occupied as a resi-
16 dence by the proprietor of the establishment.

17 (9) WILDLIFE-URBAN INTERFACE.—The term “wildland-urban inter-
18 face” has the meaning given the term in section 101 of the Healthy
19 Forests Restoration Act of 2003 (16 U.S.C. 6511).

20 § 11353. United States Fire Administration

21 (a) ESTABLISHMENT.—There is in the Federal Emergency Management
22 Agency the United States Fire Administration.

23 (b) ADMINISTRATOR.—There shall be at the head of the Administration
24 the Administrator of the Administration. The Administrator shall be ap-
25 pointed by the President and shall be compensated at the rate provided for
26 level IV of the Executive Schedule pay rates (5 U.S.C. 5315). The Adminis-
27 trator shall report and be responsible to the Administrator of FEMA.

28 (c) DEPUTY ADMINISTRATOR.—The Administrator may appoint a Deputy
29 Administrator, who shall—

30 (1) perform such functions as the Administrator shall assign or dele-
31 gate; and

32 (2) act as Administrator during the absence or disability of the Ad-
33 ministrator or in the event of a vacancy in the office of Administrator.

34 § 11354. Public education

35 The Administrator may take such steps as the Administrator considers
36 appropriate to educate the public and overcome public indifference as to
37 fire, fire prevention, and individual preparedness. The steps may include
38 publications, audiovisual presentations, and demonstrations. The public edu-
39 cation efforts shall include programs to provide specialized information for
40 those groups of individuals who are particularly vulnerable to fire hazards,
41 such as the young and the elderly. The Administrator shall sponsor and en-

1 courage research, testing, and experimentation to determine the most effective means of the public education.

3 **§ 11355. National Academy for Fire Prevention and Control**

4 (a) ESTABLISHMENT AND PURPOSE.—The Administrator of FEMA shall establish a National Academy for Fire Prevention and Control. The purpose of the Academy shall be to advance the professional development of fire service personnel and of other individuals engaged in fire prevention and control activities.

9 (b) SUPERINTENDENT.—The Academy shall be headed by a Superintendent, who shall be appointed by the Administrator of FEMA. In exercising the powers and authority contained in this section the Superintendent shall be subject to the direction of the Administrator.

13 (c) POWERS OF SUPERINTENDENT.—The Superintendent may—

14 (1) develop and revise curricula, standards for admission and performance, and criteria for the awarding of degrees and certifications;

16 (2) consult with other Federal, State, and local agency officials in developing curricula for classes offered by the Academy;

18 (3) appoint such teaching staff and other personnel as the Superintendent determines to be necessary or appropriate;

20 (4) conduct courses and programs of training and education, as defined in subsection (d);

22 (5) appoint faculty members and consultants without regard to title 5, governing appointments in the competitive service, and, with respect to temporary and intermittent services, make appointments to the same extent as is authorized by section 3109 of title 5;

26 (6) establish, modify, or waive fees and other charges for attendance at, and subscription to, courses and programs offered by the Academy;

28 (7) conduct short courses, seminars, workshops, conferences, and similar education and training activities in all parts and localities of the United States, including on-site training;

31 (8) enter into such contracts and take such other actions as may be necessary in carrying out the purposes of the Academy; and

33 (9) consult with officials of the fire services and other interested persons in the exercise of the foregoing powers.

35 (d) PROGRAM OF THE ACADEMY.—The Superintendent may—

36 (1) train fire service personnel in such skills and knowledge as may be useful to advance their ability to prevent and control fires, including—

39 (A) techniques of fire prevention, fire inspection, firefighting, and fire and arson investigation;

- 1 (B) tactics and command of firefighting for present and future
- 2 fire chiefs and commanders;
- 3 (C) administration and management of fire services;
- 4 (D) tactical training in the specialized field of aircraft fire con-
- 5 trol and crash rescue;
- 6 (E) tactical training in the specialized field of fire control and
- 7 rescue aboard waterborne vessels;
- 8 (F) strategies for building collapse rescue;
- 9 (G) the use of technology in response to fires, including terrorist
- 10 incidents and other national emergencies;
- 11 (H) tactics and strategies for dealing with natural disasters,
- 12 acts of terrorism, and other man-made disasters;
- 13 (I) tactics and strategies for fighting large-scale fires or mul-
- 14 tiple fires in a general area that crosses jurisdictional boundaries;
- 15 (J) tactics and strategies for fighting fires occurring at the
- 16 wildland-urban interface;
- 17 (K) tactics and strategies for fighting fires involving hazardous
- 18 materials;
- 19 (L) advanced emergency medical services training;
- 20 (M) use of and familiarity with the Federal Response Plan;
- 21 (N) leadership and strategic skills, including integrated manage-
- 22 ment systems operations and integrated response;
- 23 (O) applying new technology and developing strategies and tac-
- 24 tics for fighting wildland fires;
- 25 (P) integrating the activities of terrorism response agencies into
- 26 national terrorism incident response systems;
- 27 (Q) tactics and strategies for fighting fires at United States
- 28 ports, including fires on the water and aboard vessels; and
- 29 (R) the training of present and future instructors in the afore-
- 30 mentioned subjects;
- 31 (2) develop model curricula, training programs and other educational
- 32 materials suitable for use at other educational institutions, and make
- 33 the materials available without charge;
- 34 (3) develop and administer a program of correspondence courses to
- 35 advance the knowledge and skills of fire service personnel;
- 36 (4) develop and distribute to appropriate officials model questions
- 37 suitable for use in conducting entrance and promotional examinations
- 38 for fire service personnel; and
- 39 (5) encourage the inclusion of fire prevention and detection tech-
- 40 nology and practices in the education and professional practice of ar-

1 architects, builders, city planners, and others engaged in design and plan-
2 ning affected by fire safety problems.

3 (e) COORDINATION OF TRAINING.—The Administrator shall coordinate
4 training provided under subsection (d)(1) with the Attorney General, the
5 Secretary of Health and Human Services, and the heads of other Federal
6 agencies—

7 (1) to ensure that the training does not duplicate existing courses
8 available to fire service personnel; and

9 (2) to establish a mechanism for eliminating duplicative training pro-
10 grams.

11 (f) TECHNICAL ASSISTANCE.—The Administrator may, to the extent that
12 the Administrator determines it necessary to meet the needs of the Nation,
13 encourage new programs and strengthen existing programs of education and
14 training by local fire services, units, and departments, State and local gov-
15 ernments, and private institutions, by providing technical assistance and ad-
16 vice to—

17 (1) vocational training programs in techniques of fire prevention, fire
18 inspection, firefighting, and fire and arson investigation;

19 (2) fire training courses and programs at junior colleges; and

20 (3) 4-year degree programs in fire engineering at colleges and uni-
21 versities.

22 (g) ASSISTANCE TO STATE AND LOCAL FIRE SERVICE TRAINING PRO-
23 GRAMS.—The Administrator may provide assistance to State and local fire
24 service training programs through grants, contracts, or otherwise. The as-
25 sistance shall not exceed 7.5 percent of the amount authorized to be appro-
26 priated in each fiscal year pursuant to section 11388 of this title.

27 (h) CONSTRUCTION COSTS.—Of the sums authorized to be appropriated
28 for the purpose of implementing the programs of the Administration, not
29 more than \$9,000,000 shall be available for the construction of facilities of
30 the Academy. Sums for the construction shall remain available until ex-
31 pended.

32 (i) EDUCATIONAL AND PROFESSIONAL ASSISTANCE.—

33 (1) IN GENERAL.—The Administrator may—

34 (A) provide stipends to students attending Academy courses and
35 programs, in amounts up to 75 percent of the expense of attend-
36 ance, as established by the Superintendent;

37 (B) provide stipends to students attending courses and non-
38 degree training programs approved by the Superintendent at uni-
39 versities, colleges, and junior colleges, in amounts up to 50 percent
40 of the cost of tuition;

1 (C) make or enter into contracts to make payments to institu-
2 tions of higher education for loans, not to exceed \$2,500 per aca-
3 demic year for an individual who is enrolled on a full-time basis
4 in an undergraduate or graduate program of fire research or engi-
5 neering that is certified by the Superintendent; and

6 (D) establish and maintain a placement and promotion opportu-
7 nities center in cooperation with the fire services, for firefighters
8 who wish to learn and take advantage of different or better career
9 opportunities.

10 (2) TERMS AND CONDITIONS OF LOANS.—Loans under paragraph
11 (1)(C) shall be made on such terms and subject to such conditions as
12 the Superintendent and each institution involved may jointly determine.

13 (3) CAREER ASSISTANCE NOT LIMITED TO ACADEMY STUDENTS AND
14 GRADUATES.—The placement and promotion opportunities center shall
15 not limit assistance under paragraph (1)(D) to students and graduates
16 of the Academy but shall undertake to assist all fire service personnel.

17 (j) BOARD OF VISITORS.—The Administrator of FEMA shall establish a
18 procedure for the selection of professionals in the field of fire safety, fire
19 prevention, fire control, research and development in fire protection, treat-
20 ment and rehabilitation of fire victims, or local government services manage-
21 ment to serve as members of a Board of Visitors for the Academy. Pursuant
22 to the procedure, the Administrator of FEMA shall select 8 individuals to
23 serve as members of the Board of Visitors to serve such terms as the Ad-
24 ministrator of FEMA may prescribe. The function of the Board of Visitors
25 shall be to review annually the program of the Academy and to make com-
26 ments and recommendations to the Administrator of FEMA regarding the
27 operation of the Academy and any improvements in the Academy that the
28 Board of Visitors considers appropriate. Each member of the Board of Visi-
29 tors shall be reimbursed for expenses actually incurred by the member in
30 the performance of the member's duties as a member of the Board of Visi-
31 tors.

32 (k) ADMISSION.—The Superintendent may admit to the courses and pro-
33 grams of the Academy individuals who are members of the firefighting, res-
34 cue, and civil defense forces of the Nation and such other individuals, in-
35 cluding candidates for membership in these forces, as the Superintendent
36 determines can benefit from attendance. Students shall be admitted from
37 any State, with due regard to adequate representation in the student body
38 of all geographic regions of the Nation. In selecting students, the Super-
39 intendent may seek nominations and advice from the fire services and other
40 organizations that wish to send students to the Academy. The Super-
41 intendent shall offer, at the Academy and at other sites, courses and train-

1 ing assistance as necessary to accommodate all geographic regions and
2 needs of career and volunteer firefighters.

3 (l) ON-SITE TRAINING.—

4 (1) IN GENERAL.—Except as provided in paragraph (2), the Admin-
5 istrator may enter into a contract with nationally recognized organiza-
6 tions that have established on-site training programs that comply with
7 national voluntary consensus standards for fire service personnel to fa-
8 cilitate the delivery of the education and training programs outlined in
9 subsection (d)(1) directly to fire service personnel.

10 (2) LIMITATION.—

11 (A) IN GENERAL.—The Administrator may not enter into a con-
12 tract with an organization described in paragraph (1) unless the
13 organization provides training that—

14 (i) leads to certification by a fire service training program
15 that is accredited by a nationally recognized accreditation or-
16 ganization; or

17 (ii) the Administrator determines is of equivalent quality to
18 a fire service training program described in clause (i).

19 (B) APPROVAL OF UNACCREDITED FIRE SERVICE TRAINING
20 PROGRAMS.—The Administrator may consider the fact that an or-
21 ganization has provided a satisfactory fire service training pro-
22 gram pursuant to a cooperative agreement with a Federal agency
23 as evidence that the program is of equivalent quality to a fire ser-
24 vice training program described in subparagraph (A)(i).

25 (3) RESTRICTION ON USE OF FUNDS.—The amounts expended by
26 the Administrator to carry out this subsection in a fiscal year shall not
27 exceed 7.5 percent of the amount authorized to be appropriated in that
28 fiscal year pursuant to section 11388 of this title.

29 (m) TRIENNIAL REPORT.—In the 1st annual report filed pursuant to sec-
30 tion 11387 of this title for which the deadline for filing is after the expira-
31 tion of the 18-month period that begins on October 8, 2008, and in every
32 3d annual report thereafter, the Administrator shall include information
33 about changes made to the National Fire Academy curriculum, including—

34 (1) the basis for the changes, including a review of the incorporation
35 of lessons learned by emergency response personnel after significant
36 emergency events and emergency preparedness exercises performed
37 under the National Exercise Program; and

38 (2) the desired training outcome of all the changes.

39 **§ 11356. Fire technology**

40 (a) DEVELOPMENT.—The Administrator shall conduct a continuing pro-
41 gram of development, testing, and evaluation of equipment for use by the

1 Nation's fire, rescue, and civil defense services, with the aim of making
2 available improved suppression, protective, auxiliary, and warning devices
3 incorporating the latest technology. Attention shall be given to the standard-
4 ization, compatibility, and interchangeability of the equipment. The develop-
5 ment, testing, and evaluation activities shall include—

6 (1) safer, less cumbersome articles of protective clothing, including
7 helmets, boots, and coats;

8 (2) breathing apparatus with the necessary duration of service, reli-
9 ability, low weight, and ease of operation for practical use;

10 (3) safe and reliable auxiliary equipment for use in fire prevention,
11 detection, and control, such as fire location detectors, visual and audio
12 communications equipment, and mobile equipment;

13 (4) special clothing and equipment needed for forest fires, brush
14 fires, oil and gasoline fires, aircraft fires and crash rescue, fires occur-
15 ring aboard waterborne vessels, and in other special firefighting situa-
16 tions;

17 (5) fire detectors and related equipment for residential use with high
18 sensitivity and reliability, and that are sufficiently inexpensive to pur-
19 chase, install, and maintain to ensure wide acceptance and use;

20 (6) in-place fire prevention systems of low cost and of increased reli-
21 ability and effectiveness;

22 (7) methods of testing fire alarms and fire protection devices and
23 systems on a non-interference basis;

24 (8) the development of purchase specifications, standards, and ac-
25 ceptance and validation test procedures for the equipment and devices;
26 and

27 (9) operation tests, demonstration projects, and fire investigations in
28 support of the activities set forth in this section.

29 (b) LIMITATION ON MANUFACTURE AND SALE OF EQUIPMENT.—The Ad-
30 ministration shall not engage in the manufacture or sale of any equipment
31 or device developed pursuant to this section, except to the extent that it con-
32 siders it necessary to adequately develop, test, or evaluate the equipment or
33 device.

34 (c) MANAGEMENT STUDIES.—

35 (1) IN GENERAL.—The Administrator may conduct, directly or
36 through contracts or grants, studies of the operations and management
37 aspects of fire services, utilizing quantitative techniques, such as oper-
38 ations research, management economics, cost effectiveness studies, and
39 such other techniques and methods as may be applicable and useful.
40 The studies shall include the allocation of resources, the optimum loca-
41 tion of fire stations, the optimum geographical area for an integrated

1 fire service, the manner of responding to alarms, the operation of city-
2 wide and regional fire dispatch centers, firefighting under conditions of
3 civil disturbance, and the effectiveness, frequency, and methods of
4 building inspections.

5 (2) EMERGENCY MEDICAL SERVICES.—The Administrator may con-
6 duct, directly or through contracts or grants, studies of the operations
7 and management aspects of fire service-based emergency medical serv-
8 ices and coordination between emergency medical services and fire serv-
9 ices. The studies may include the optimum protocols for on-scene care,
10 the allocation of resources, and the training requirements for fire serv-
11 ice-based emergency medical services.

12 (3) PRODUCTIVITY AND EFFICIENCY, JOB CATEGORIES AND SKILLS,
13 REDUCTION OF INJURIES, EFFECTIVE PROGRAMS AND ACTIVITIES, AND
14 TECHNIQUES.—The Administrator may conduct, directly or through
15 contracts or grants, research concerning the productivity and efficiency
16 of fire service personnel, the job categories and skills required by fire
17 services under varying conditions, the reduction of injuries to fire serv-
18 ice personnel, the most effective fire prevention programs and activities,
19 and techniques for accurately measuring and analyzing the foregoing.

20 (4) NEW TECHNOLOGY, STANDARDS, OPERATING METHODS, COM-
21 MAND TECHNIQUES, AND MANAGEMENT SYSTEMS.—The Administrator
22 may conduct, directly or through contracts, grants, or other forms of
23 assistance, development, testing and demonstration projects to the ex-
24 tent considered necessary to introduce and to encourage the acceptance
25 of new technology, standards, operating methods, command techniques,
26 and management systems for utilization by the fire services.

27 (5) ASSIST FIRE SERVICES.—The Administrator may assist the Na-
28 tion's fire services, directly or through contracts, grants, or other forms
29 of assistance, to measure and evaluate, on a cost-benefit basis, the ef-
30 fectiveness of the programs and activities of each fire service and the
31 predictable consequences on the applicable local fire services of coordi-
32 nation or combination, in whole or in part, in a regional, metropolitan,
33 or statewide fire service.

34 (d) RURAL AND REMOTE AREAS AND WILDLAND-URBAN INTERFACE AS-
35 SISTANCE.—The Administrator may, in coordination with the Secretary of
36 Agriculture, the Secretary of the Interior, and the Wildland Fire Leadership
37 Council, assist the fire services of the United States, directly or through
38 contracts, grants, or other forms of assistance, in sponsoring and encour-
39 aging research into approaches, techniques, systems, equipment, and land-
40 use policies to improve fire prevention and control in—

41 (1) the rural and remote areas of the United States; and

1 (2) the wildland-urban interface.

2 (e) ASSISTANCE TO OTHER FEDERAL AGENCIES.—At the request of
3 other Federal agencies, including the Department of Agriculture and the
4 Department of the Interior, the Administrator may provide assistance in fire
5 prevention and control technologies, including methods of containing insect-
6 infested forest fires and limiting dispersal of resultant fire particle smoke,
7 and methods of measuring and tracking the dispersal of fine-particle smoke
8 resulting from fires of insect-infested fuel.

9 (f) TECHNOLOGY EVALUATION AND STANDARDS DEVELOPMENT.—

10 (1) IN GENERAL.—In addition to, or as part of, the program con-
11 ducted under subsection (a), the Administrator, in consultation with
12 the National Institute of Standards and Technology, the Inter-Agency
13 Board for Equipment Standardization and Inter-Operability, the Na-
14 tional Institute for Occupational Safety and Health, the Science and
15 Technology Directorate of the Department, national voluntary con-
16 sensus standards development organizations, interested Federal, State,
17 and local agencies, and other interested parties, shall—

18 (A) develop new, and utilize existing, measurement techniques
19 and testing methodologies for evaluating new firefighting tech-
20 nologies, including—

- 21 (i) personal protection equipment;
22 (ii) devices for advance warning of extreme hazard;
23 (iii) equipment for enhanced vision;
24 (iv) devices to locate victims, firefighters, and other rescue
25 personnel in above-ground and below-ground structures;
26 (v) equipment and methods to provide information for inci-
27 dent command, including the monitoring and reporting of in-
28 dividual personnel welfare;
29 (vi) equipment and methods for training, especially for vir-
30 tual reality training; and
31 (vii) robotics and other remote-controlled devices;

32 (B) evaluate the compatibility of new equipment and technology
33 with existing firefighting technology; and

34 (C) support the development of new voluntary consensus stand-
35 ards through national voluntary consensus standards organizations
36 for new firefighting technologies based on techniques and meth-
37 odologies described in subparagraph (A).

38 (2) STANDARDS FOR NEW EQUIPMENT OR SYSTEMS.—

39 (A) REQUIREMENT THAT STANDARDS BE MET FOR NEW EQUIP-
40 MENT OR SYSTEMS PURCHASED THROUGH ASSISTANCE PRO-
41 GRAM.—The Administrator shall, by regulation, require that new

1 equipment or systems purchased through the assistance program
2 established by section 11377 of this title meet or exceed applicable
3 voluntary consensus standards for the equipment or systems for
4 which applicable voluntary consensus standards have been estab-
5 lished.

6 (B) EXPLANATION WHY NEW EQUIPMENT OR SYSTEMS THAT
7 DON'T MEET OR EXCEED STANDARDS WILL BETTER SERVE NEEDS
8 OF APPLICANT.—

9 (i) IN GENERAL.—If an applicant for a grant under section
10 11377 of this title proposes to purchase, with assistance pro-
11 vided under the grant, new equipment or systems that do not
12 meet or exceed applicable voluntary consensus standards, the
13 applicant shall include in the application an explanation of
14 why the equipment or systems will serve the needs of the ap-
15 plicant better than equipment or systems that do meet or ex-
16 ceed the standards.

17 (ii) SECOND GRANT REQUEST IN APPLICATION.—Applicants
18 that apply for a grant under the terms of clause (i) may in-
19 clude a 2d grant request in the application to be considered
20 by the Administrator in the event that the Administrator does
21 not approve the primary grant request on the grounds of the
22 equipment not meeting applicable voluntary consensus stand-
23 ards.

24 (C) WAIVER.—The Administrator may waive the requirement
25 under subparagraph (A) with respect to specific standards. In
26 making a determination whether or not to waive the requirement
27 with respect to a specific standard, the Administrator shall, to the
28 greatest extent practicable—

29 (i) consult with grant applicants and other members of the
30 fire services regarding the impact on fire departments of the
31 requirement to meet or exceed the specific standard;

32 (ii) take into consideration the explanation provided by the
33 applicant under subparagraph (B); and

34 (iii) seek to minimize the impact of the requirement to
35 meet or exceed the specific standard on the applicant, par-
36 ticularly if meeting the standard would impose additional
37 costs.

38 (g) COORDINATION.—In establishing and conducting programs under this
39 section, the Administrator shall take full advantage of applicable techno-
40 logical developments made by other departments and agencies of the Fed-

1 eral Government, by State and local governments, and by business, industry,
2 and nonprofit associations.

3 (h) PUBLICATION OF RESEARCH RESULTS.—

4 (1) IN GENERAL.—For each fire-related research program funded by
5 the Administration, the Administrator shall make available to the pub-
6 lic on the website of the Administration the following:

7 (A) A description of the research program, including the scope,
8 methodology, and goals of the research program.

9 (B) Information that identifies the individuals or institutions
10 conducting the research program.

11 (C) The amount of funding provided by the Administration for
12 the research program.

13 (D) The results or findings of the research program.

14 (2) DEADLINES.—The information required by paragraph (1) shall
15 be published with respect to a research program as follows:

16 (A) The information described in subparagraphs (A), (B), and
17 (C) of paragraph (1) with respect to the research program shall
18 be made available under paragraph (1) not later than 30 days
19 after the Administrator has awarded the funding for the research
20 program.

21 (B) The information described in subparagraph (D) of para-
22 graph (1) with respect to a research program shall be made avail-
23 able under paragraph (1) not later than 60 days after the date
24 the research program has been completed.

25 **§ 11357. National Fire Data Center**

26 (a) FUNCTIONS.—

27 (1) IN GENERAL.—The Administrator shall operate, directly or
28 through contracts or grants, an integrated, comprehensive National
29 Fire Data Center for the selection, analysis, publication, and dissemi-
30 nation of information related to the prevention, occurrence, control, and
31 results of fires of all types. The program of the National Fire Data
32 Center shall be designed to—

33 (A) provide an accurate nationwide analysis of the fire problem;

34 (B) identify major problem areas;

35 (C) assist in setting priorities;

36 (D) determine possible solutions to problems; and

37 (E) monitor the progress of programs to reduce fire losses.

38 (2) GATHERING AND ANALYZING INFORMATION.—To carry out the
39 functions described in paragraph (1), the National Fire Data Center
40 shall gather and analyze—

1 (A) information on the frequency, causes, spread, and extin-
2 guishment of fires;

3 (B) information on the number of injuries and deaths resulting
4 from fires, including the maximum available information on the
5 specific causes and nature of the injuries and deaths, categorized
6 by the type of fire, and information on property losses;

7 (C) information on the occupational hazards faced by fire-
8 fighters, including the causes of deaths and injuries arising, di-
9 rectly and indirectly, from firefighting activities, including—

10 (i) all injuries sustained by a firefighter and treated by a
11 doctor, categorized by the type of firefighter;

12 (ii) all deaths sustained while undergoing a pack test or
13 preparing for a work capacity;

14 (iii) all injuries or deaths resulting from vehicle accidents;
15 and

16 (iv) all injuries or deaths resulting from aircraft crashes;

17 (D) information on all types of firefighting activities, including
18 inspection practices;

19 (E) technical information related to building construction, fire
20 properties of materials, and similar information;

21 (F) information on fire prevention and control laws, systems,
22 methods, techniques, and administrative structures used in foreign
23 nations;

24 (G) information on the causes, behavior, and best method of
25 control of other types of fire, including forest fires, brush fires,
26 fire underground, oil blow-out fires, and water-borne fires; and

27 (H) such other information and data as is considered useful and
28 applicable.

29 (b) METHODS.—In carrying out the program of the National Fire Data
30 Center, the Administrator may—

31 (1) develop standardized data reporting methods;

32 (2) encourage and assist Federal, State, local, and other agencies,
33 public and private, in developing and reporting information; and

34 (3) make full use of existing data gathering and analysis organiza-
35 tions, both public and private, including the Center for Firefighter In-
36 jury Research and Safety Trends.

37 (c) DISSEMINATION OF FIRE DATA.—The Administrator shall ensure dis-
38 semination to the maximum extent possible of fire data collected and devel-
39 oped by the National Fire Data Center, and shall make the data, informa-
40 tion, and analysis available in appropriate form to Federal agencies, State

1 and local governments, private organizations, industry, business, and other
2 interested persons.

3 (d) NATIONAL FIRE INCIDENT REPORTING SYSTEM UPDATE.—The Ad-
4 ministrator shall update the National Fire Incident Reporting System to en-
5 sure that the information in the system is available, and can be updated,
6 through the Internet and in real time.

7 (e) MEDICAL PRIVACY OF FIREFIGHTERS.—The collection, storage, and
8 transfer of medical data collected under this section shall be conducted in
9 accordance with—

10 (1) the privacy regulations promulgated under section 264(e) of the
11 Health Insurance Portability and Accountability Act of 1996 (Public
12 Law 104–191, 42 U.S.C. 1320d–2 note); and

13 (2) other applicable regulations, including parts 160, 162, and 164
14 of title 45, Code of Federal Regulations (as in effect on March 12,
15 2019).

16 **§ 11358. Master plans**

17 (a) DEFINITION OF MASTER PLAN.—For the purposes of this section, the
18 term “master plan” means a plan that will result in the planning and imple-
19 mentation in the area involved of a general program of action for fire pre-
20 vention and control. The master plan is reasonably expected to include—

21 (1) a survey of the resources and personnel of existing fire services
22 and an analysis of the effectiveness of the fire and building codes in
23 the area;

24 (2) an analysis of short- and long-term fire prevention and control
25 needs in the area;

26 (3) a plan to meet the fire prevention and control needs in the area;
27 and

28 (4) an estimate of cost and realistic plans for financing the imple-
29 mentation of the plan and operation on a continuing basis and a sum-
30 mary of problems that are anticipated in implementing the master
31 plan.

32 (b) ENCOURAGEMENT BY ADMINISTRATOR.—The establishment of master
33 plans for fire prevention and control is the responsibility of the States and
34 the political subdivisions of the States. The Administrator may encourage
35 and assist the States and political subdivisions in the planning activities,
36 consistent with the Administrator’s powers and duties under this sub-
37 chapter.

38 (c) MUTUAL AID SYSTEMS.—

39 (1) IN GENERAL.—The Administrator shall provide technical assist-
40 ance and training to State and local fire service officials to establish

1 nationwide and State mutual aid systems for dealing with national
2 emergencies that—

3 (A) include threat assessment and equipment deployment strate-
4 gies;

5 (B) include means of collecting asset and resource information
6 to provide accurate and timely data for regional deployment; and

7 (C) are consistent with the Federal Response Plan.

8 (2) MODEL MUTUAL AID PLANS.—The Administrator shall develop
9 and make available to State and local fire service officials model mutual
10 aid plans for both intrastate and interstate assistance.

11 **§ 11359. Reimbursement for costs of firefighting on Federal**
12 **property**

13 (a) FILING OF CLAIMS.—Each fire service that engages in the fighting
14 of a fire on property that is under the jurisdiction of the United States may
15 file a claim with the Administrator for the amount of direct expenses and
16 direct losses incurred by the fire service as a result of fighting the fire. The
17 claim shall include such supporting information as the Administrator may
18 prescribe.

19 (b) DETERMINATION.—On receipt of a claim filed under subsection (a),
20 the Administrator shall determine—

21 (1) what payments, if any, to the fire service or its parent jurisdic-
22 tion, including taxes or payments in lieu of taxes, the United States
23 has made for the support of fire services on the property in question;

24 (2) the extent to which the fire service incurred additional fire-
25 fighting costs, over and above its normal operating costs, in connection
26 with the fire that is the subject of the claim; and

27 (3) the amount, if any, of the additional costs referred to in para-
28 graph (2) that were not adequately covered by the payments referred
29 to in paragraph (1).

30 (c) PAYMENT.—The Administrator of FEMA shall forward the claim and
31 a copy of the Administrator's determination under subsection (b)(3) to the
32 Secretary of the Treasury. The Secretary of the Treasury shall, on receipt
33 of the claim and determination, pay the fire service or its parent jurisdic-
34 tion, from any money in the Treasury not otherwise appropriated but sub-
35 ject to reimbursement (from any appropriations that may be available or
36 that may be made available for the purpose) by the Federal department or
37 agency under whose jurisdiction the fire occurred, an amount no greater
38 than the amount determined with respect to the claim under subsection
39 (b)(3).

1 (d) ADJUDICATION.—In the case of a dispute arising in connection with
2 a claim under this section, the United States Court of Federal Claims has
3 jurisdiction to adjudicate the claim and enter judgment accordingly.

4 **§ 11360. Review of fire prevention codes**

5 The Administrator may review, evaluate, and suggest improvements in
6 State and local fire prevention codes, building codes, and relevant Federal
7 or private codes and regulations. In evaluating a code, the Administrator
8 shall consider the human impact of all code requirements, standards, or pro-
9 visions in terms of comfort and habitability for residents or employees, as
10 well as the fire prevention and control value or potential of each require-
11 ment, standard, or provision.

12 **§ 11361. Fire safety effectiveness statements**

13 The Administrator may encourage owners and managers of residential
14 multiple-unit, commercial, industrial, and transportation structures to pre-
15 pare fire safety effectiveness statements, pursuant to standards, forms,
16 rules, and regulations to be developed and issued by the Administrator.

17 **§ 11362. Annual conference**

18 The Administrator may organize, or participate in organizing, an annual
19 conference on fire prevention and control. The Administrator may pay, in
20 whole or in part, the cost of the conference and the expenses of some or
21 all of the participants. All of the Nation's fire services are eligible to send
22 representatives to each conference to discuss, exchange ideas on, and par-
23 ticipate in educational programs on new techniques in fire prevention and
24 control. The conferences shall be open to the public.

25 **§ 11363. Public safety awards**

26 (a) DEFINITION OF PUBLIC SAFETY OFFICER.—As used in this section,
27 the term “public safety officer” means an individual serving a public agen-
28 cy, with or without compensation, as—

29 (1) a firefighter;

30 (2) a law enforcement officer, including a corrections or court officer;

31 or

32 (3) a civil defense officer.

33 (b) ESTABLISHMENT.—There is an honorary award for the recognition of
34 outstanding and distinguished service by public safety officers known as the
35 Administrator's Award For Distinguished Public Safety Service (in this sec-
36 tion referred to as the “Administrator's Award”).

37 (c) DESCRIPTION.—The Administrator's Award shall be presented by the
38 Administrator of FEMA or by the Attorney General to public safety officers
39 for distinguished service in the field of public safety.

40 (d) AWARD.—Each Administrator's Award shall consist of an appropriate
41 citation.

1 (e) REGULATIONS.—The Administrator of FEMA and the Attorney Gen-
2 eral shall issue jointly such regulations as may be necessary to carry out
3 this section.

4 **§ 11364. Public access to information**

5 (a) IN GENERAL.—Copies of any document, report, statement, or infor-
6 mation received or sent by the Administrator of FEMA or the Adminis-
7 trator shall be made available to the public pursuant to section 552 of title
8 5.

9 (b) TRADE SECRET.—Notwithstanding section 552(b) of title 5 and sec-
10 tion 1905 of title 18, the Administrator of FEMA may disclose information
11 that concerns or relates to a trade secret—

12 (1) on request, to other Federal Government departments and agen-
13 cies for official use;

14 (2) on request, to a committee of Congress having jurisdiction over
15 the subject matter to which the information relates;

16 (3) in a judicial proceeding under a court order formulated to pre-
17 serve the confidentiality of the information without impairing the pro-
18 ceedings; and

19 (4) to the public when the Administrator of FEMA determines the
20 disclosure to be necessary to protect health and safety after notice and
21 opportunity for comment in writing or for discussion in closed session
22 within 15 days by the party to which the information pertains (if the
23 delay resulting from the notice and opportunity for comment would not
24 be detrimental to health and safety).

25 **§ 11365. Assistance to Consumer Product Safety Commission**

26 On request, the Administrator shall assist the Consumer Product Safety
27 Commission in the development of fire safety standards or codes for con-
28 sumer products, as defined in the Consumer Product Safety Act (15 U.S.C.
29 2051 et seq.).

30 **§ 11366. Arson prevention, detection, and control**

31 The Administrator shall—

32 (1) develop arson detection techniques to assist Federal agencies and
33 States and local jurisdictions in improving arson prevention, detection,
34 and control;

35 (2) provide training and instructional materials in the skills and
36 knowledge necessary to assist Federal, State, and local fire service and
37 law enforcement personnel in arson prevention, detection, and control,
38 with particular emphasis on the needs of volunteer firefighters for im-
39 proved and more widely available arson training courses;

1 (3) formulate methods for collection of arson data that would be
2 compatible with methods of collection used for the uniform crime statis-
3 tics of the Federal Bureau of Investigation;

4 (4) develop and implement programs for improved collection of na-
5 tionwide arson statistics in the National Fire Incident Reporting Sys-
6 tem at the National Fire Data Center;

7 (5) develop programs for public education on the extent, causes, and
8 prevention of arson; and

9 (6) develop handbooks to assist Federal, State, and local fire service
10 and law enforcement personnel in arson prevention and detection.

11 **§ 11367. Arson prevention grants**

12 (a) DEFINITIONS.—As used in this section:

13 (1) ARSON.—The term “arson” includes all incendiary and sus-
14 picious fires.

15 (2) OFFICE.—The term “Office” means the Office of Fire Preven-
16 tion and Arson Control of the Administration.

17 (b) GRANTS.—The Administrator, acting through the Office, shall carry
18 out a demonstration program under which not more than 10 grant awards
19 shall be made to States, or consortia of States, for programs relating to
20 arson research, prevention, and control.

21 (c) GOALS.—In carrying out this section, the Administrator shall award
22 2-year grants on a competitive, merit basis to States, or consortia of States,
23 for projects that promote 1 or more of the following goals:

24 (1) To improve the training by States leading to professional certifi-
25 cation of arson investigators, in accordance with nationally recognized
26 certification standards.

27 (2) To provide resources for the formation of arson task forces or
28 interagency organizational arrangements involving police and fire de-
29 partments and other relevant local agencies, such as a State arson bu-
30 reau and the office of a fire marshal of a State.

31 (3) To combat fraud as a cause of arson and to advance research
32 at the State and local levels on the significance and prevention of fraud
33 as a motive for setting fires.

34 (4) To provide for the management of arson squads, including—

35 (A) training courses for fire departments in arson case manage-
36 ment, including standardization of investigative techniques and re-
37 porting methodology;

38 (B) the preparation of arson unit management guides; and

39 (C) the development and dissemination of new public education
40 materials relating to the arson problem.

1 (5) To combat civil unrest as a cause of arson and to advance re-
2 search at the State and local levels on the prevention and control of
3 arson linked to urban disorders.

4 (6) To combat juvenile arson, such as juvenile fire-setter counseling
5 programs and similar intervention programs, and to advance research
6 at the State and local levels on the prevention of juvenile arson.

7 (7) To combat drug-related arson and to advance research at the
8 State and local levels on the causes and prevention of drug-related
9 arson.

10 (8) To combat domestic violence as a cause of arson and to advance
11 research at the State and local levels on the prevention of arson arising
12 from domestic violence.

13 (9) To combat arson in rural areas and to improve the capability of
14 firefighters to identify and prevent arson-initiated fires in rural areas
15 and public forests.

16 (10) To improve the capability of firefighters to identify and combat
17 arson through expanded training programs, including—

18 (A) training courses at the State fire academies; and

19 (B) innovative courses developed with the Academy and made
20 available to volunteer firefighters through regional delivery meth-
21 ods, including teleconferencing and satellite delivered television
22 programs.

23 (d) ASSISTANCE IN STRUCTURING OF APPLICATIONS.—The Adminis-
24 trator shall assist grant applicants in structuring their applications so as
25 to ensure that at least 1 grant is awarded for each goal described in sub-
26 section (c).

27 (e) STATE QUALIFICATION CRITERIA.—To qualify for a grant under this
28 section, a State, or consortium of States, shall provide assurances adequate
29 to the Administrator that the State or consortium—

30 (1) will obtain at least 25 percent of the cost of programs funded
31 by the grant, in cash or in kind, from non-Federal sources;

32 (2) will not as a result of receiving the grant decrease the prior level
33 of spending of funds of the State or consortium from non-Federal
34 sources for arson research, prevention, and control programs;

35 (3) will use no more than 10 percent of funds provided under the
36 grant for administrative costs of the programs; and

37 (4) is making efforts to ensure that all local jurisdictions will provide
38 arson data to the National Fire Incident Reporting System or the Uni-
39 form Crime Reporting program.

1 (f) EXTENSION.—A grant awarded under this section may be extended
2 for 1 or more additional periods, at the discretion of the Administrator, sub-
3 ject to the availability of appropriations.

4 (g) TECHNICAL ASSISTANCE.—The Administrator shall provide technical
5 assistance to States in carrying out programs funded by grants under this
6 section.

7 (h) CONSULTATION AND COOPERATION.—In carrying out this section, the
8 Administrator shall consult and cooperate with other Federal agencies to en-
9 hance program effectiveness and avoid duplication of effort, including the
10 conduct of regular meetings initiated by the Administrator with representa-
11 tives of other Federal agencies concerned with arson and concerned with ef-
12 forts to develop a more comprehensive profile of the magnitude of the na-
13 tional arson problem.

14 (i) REGULATIONS.—The Administrator shall issue regulations to imple-
15 ment this section, including procedures for grant applications.

16 (j) ADMINISTRATION.—The Administrator shall directly administer the
17 grant program required by this section, and shall not enter into a contract
18 under which the grant program or a portion of the program will be adminis-
19 tered by another party.

20 (k) PURCHASE OF AMERICAN MADE EQUIPMENT AND PRODUCTS.—

21 (1) SENSE OF CONGRESS.—It is the sense of Congress that a recipi-
22 ent of a grant under this section should purchase, when available and
23 cost-effective, American made equipment and products when expending
24 grant monies.

25 (2) NOTICE TO RECIPIENTS OF ASSISTANCE.—In allocating grants
26 under this section, the Administrator shall provide to each recipient a
27 notice describing the statement made in paragraph (1) by Congress.

28 **§ 11368. Review of existing response information**

29 (a) DEFINITION OF EMERGENCY RESPONSE PERSONNEL.—As used in
30 this section, the term “emergency response personnel” means personnel re-
31 sponsible for mitigation activities in a medical emergency, fire emergency,
32 hazardous material emergency, or natural disaster.

33 (b) IN GENERAL.—The Administrator shall conduct a review of existing
34 response information used by emergency response personnel at the State
35 and local levels to evaluate its accuracy and consistency, and to determine
36 whether it is properly expressed. The information should clearly commu-
37 nicate to emergency response personnel the probable hazards that they must
38 contend with in an emergency situation involving hazardous materials, and
39 the appropriate response to those hazards.

1 **§ 11369. Working group**

2 (a) ESTABLISHMENT.—For the purpose of carrying out section 11368 of
3 this title, there is a working group established by the Administrator that,
4 at a minimum, consists of—

5 (1) program officials from each of—

6 (A) the Environmental Protection Agency;

7 (B) the National Oceanic and Atmospheric Administration;

8 (C) the Department of Transportation;

9 (D) the Occupational Safety and Health Administration; and

10 (E) the Bureau of Alcohol, Tobacco, Firearms, and Explosives,
11 Department of Justice;

12 (2) State and local operational officials with emergency response or
13 relevant regulatory responsibilities; and

14 (3) representatives of companies engaged in the manufacture and
15 processing of chemicals.

16 (b) DUTIES.—The working group shall develop and disseminate haz-
17 ardous materials identification and response data and collect, collate, ana-
18 lyze, and disseminate hazardous materials incident data.

19 **§ 11370. Annual revision of recommendations**

20 The working group established under section 11369 of this title shall
21 meet as needed, but at least once every 12 months, to review and recom-
22 mend changes and additions to the report cited in section 4 of the Fire-
23 fighters' Safety Study Act (Public Law 101-446, 104 Stat. 1045) that are
24 necessary and appropriate for operational personnel at the local level.

25 **§ 11371. Listings of places of public accommodation that**
26 **meet guidelines**

27 (a) PERIODIC UPDATE OF LIST BY STATES.—The Administrator of
28 FEMA shall formulate procedures under which each State (acting through
29 its Governor (or if none exists, chief executive officer) or the Governor's or
30 chief executive officer's designee) shall periodically update the list of those
31 places of public accommodation affecting commerce located in each State
32 that meet the requirements of the guidelines described in section 11372 of
33 this title that the State submitted pursuant to section 28(a)(1) of the Fed-
34 eral Fire Prevention and Control Act of 1974 (Public Law 93-498, as
35 added by section 3(a) of the Hotel and Motel Fire Safety Act of 1990 (Pub-
36 lic Law 101-391, 104 Stat. 747)).

37 (b) COMPILATION AND DISTRIBUTION OF MASTER LIST BY ADMINIS-
38 TRATOR OF FEMA.—

39 (1) DEFINITION OF AGENCY.—For purposes of this subsection, the
40 term “agency” has the same meaning given the term in section 5701
41 of title 5.

1 (2) IN GENERAL.—The Administrator of FEMA shall periodically
2 update the national master list of all of the places of public accommo-
3 dation affecting commerce located in each State that meet the require-
4 ments of the guidelines described in section 11372 of this title compiled
5 and published in the Federal Register pursuant to section 28(b)(1) of
6 the Federal Fire Prevention and Control Act of 1974 (Public Law 93–
7 498, as added by section 3(a) of the Hotel and Motel Fire Safety Act
8 of 1990 (Public Law 101–391, 104 Stat. 748)) to reflect changes in
9 the State lists submitted to the Administrator of FEMA pursuant to
10 subsection (a), and shall periodically redistribute the updated master
11 list to each agency of the Federal Government.

12 **§ 11372. Dissemination of fire prevention and control infor-**
13 **mation**

14 The Administrator of FEMA, acting through the Administrator, may take
15 steps to encourage the States to promote the use of automatic sprinkler sys-
16 tems and automatic smoke detection systems and disseminate to the max-
17 imum extent possible information on the life safety value and use of those
18 systems. The steps may include providing copies of the guidelines described
19 in section 11373 of this title and of the master list compiled under section
20 28(b)(1) of the Federal Fire Prevention and Control Act of 1974 (Public
21 Law 93–498, as added by section 3(a) of the Hotel and Motel Fire Safety
22 Act of 1990 (Public Law 101–391, 104 Stat. 748)) to Federal agencies,
23 State and local governments, and fire services throughout the United States,
24 and making copies of the master list available on request to interested pri-
25 vate organizations and individuals.

26 **§ 11373. Fire prevention and control guidelines for places of**
27 **public accommodation**

28 (a) DEFINITIONS.—For purposes of this section, the following definitions
29 apply:

30 (1) AUTOMATIC SPRINKLER SYSTEM.—The term “automatic sprin-
31 kler system” means an electronically supervised, integrated system of
32 piping to which sprinklers are attached in a systematic pattern, and
33 that, when activated by heat from a fire, will protect human lives by
34 discharging water over the fire area, and by providing appropriate
35 warning signals (to the extent the signals are required by Federal,
36 State, or local laws or regulations) through the building’s fire alarm
37 system.

38 (2) GOVERNMENTAL AUTHORITY HAVING JURISDICTION.—The term
39 “governmental authority having jurisdiction” means the Federal, State,
40 local, or other governmental entity with statutory or regulatory author-

1 ity for the approval of fire safety systems, equipment, installations, or
2 procedures in a specified locality.

3 (3) SMOKE DETECTOR.—The term “smoke detector” means an
4 alarm that is designed to respond to the presence of visible or invisible
5 particles of combustion.

6 (b) CONTENTS.—The guidelines referred to in sections 11371 and 11372
7 of this title consist of—

8 (1) a requirement that hard-wired, single-station smoke detectors be
9 installed in accordance with National Fire Protection Association
10 Standard 74 or any successor standard to that standard in each guest
11 room in each place of public accommodation affecting commerce; and

12 (2) a requirement that an automatic sprinkler system be installed in
13 accordance with National Fire Protection Association Standard 13 or
14 13–R, or any successor standard to that standard, whichever is appro-
15 priate, in each place of public accommodation affecting commerce ex-
16 cept those places that are 3 stories or lower.

17 (c) EXCEPTIONS.—

18 (1) AUTOMATIC SPRINKLER SYSTEM ALREADY INSTALLED.—The re-
19 quirement described in subsection (b)(2) shall not apply to a place of
20 public accommodation affecting commerce with an automatic sprinkler
21 system installed before October 25, 1992, if the automatic sprinkler
22 system is installed in compliance with an applicable standard (adopted
23 by the governmental authority having jurisdiction, and in effect, at the
24 time of installation) that required the placement of a sprinkler head in
25 the sleeping area of each guest room.

26 (2) STANDARD PREVENTS COMPLIANCE WITH AUTOMATIC SPRIN-
27 KLER SYSTEM STANDARD.—The requirement described in subsection
28 (a)(2) shall not apply to a place of public accommodation affecting
29 commerce to the extent that the place of public accommodation affect-
30 ing commerce is subject to a standard that includes a requirement or
31 prohibition that prevents compliance with a provision of National Fire
32 Protection Association Standard 13 or 13–R, or any successor standard
33 to that standard. In that, the place of public accommodation affecting
34 commerce is exempt only from that specific provision.

35 (d) EFFECT ON STATE AND LOCAL LAW.—This section shall not be con-
36 strued to limit the power of a State or political subdivision of a State to
37 implement or enforce any law, rule, regulation, or standard concerning fire
38 prevention and control.

1 **§ 11374. Prohibiting Federal funding of conferences held at**
2 **non-certified places of public accommodation**

3 (a) IN GENERAL.—No Federal funds may be used to sponsor or fund in
4 whole or in part a meeting, convention, conference, or training seminar that
5 is conducted in, or that otherwise uses the rooms, facilities, or services of,
6 a place of public accommodation that does not meet the requirements of the
7 fire prevention and control guidelines described in section 11373 of this
8 title.

9 (b) WAIVER.—

10 (1) IN GENERAL.—The head of an agency of the Federal Govern-
11 ment sponsoring or funding a particular meeting, convention, con-
12 ference, or training seminar may waive the prohibition described in
13 subsection (a) if the head of the agency determines that a waiver of
14 the prohibition is necessary in the public interest in the case of the par-
15 ticular event.

16 (2) DELEGATION OF AUTHORITY.—The head of an agency of the
17 Federal Government may delegate the authority provided under para-
18 graph (1) to waive the prohibition described in subsection (a) and to
19 determine whether the waiver is necessary in the public interest to an
20 officer or employee of the agency if the officer or employee is given the
21 authority with respect to all meetings, conventions, conferences, and
22 training seminars sponsored or funded by the agency.

23 (c) NOTICE REQUIREMENTS.—

24 (1) ADVERTISEMENTS AND APPLICATIONS.—

25 (A) IN GENERAL.—An advertisement for, or application for at-
26 tendance at, a meeting, convention, conference, or training sem-
27 inar sponsored or funded in whole or in part by the Federal Gov-
28 ernment shall include a notice regarding the prohibition described
29 in subsection (a).

30 (B) NONAPPLICATION.—The requirement described in subpara-
31 graph (A) shall not apply in the case of an event for which a head
32 of an agency of the Federal Government, pursuant to subsection
33 (b), waives the prohibition described in subsection (a).

34 (2) PROVIDING NOTICE TO RECIPIENTS OF FUNDS.—

35 (A) DEFINITIONS.—In subparagraph (B), the terms “Executive
36 department”, “Government corporation”, and “independent estab-
37 lishment” have the meanings given those terms in chapter 1 of
38 title 5.

39 (B) IN GENERAL.—Each Executive department, Government
40 corporation, and independent establishment providing Federal

1 funds to non-Federal entities shall notify recipients of the funds
2 of the prohibition described in subsection (a).

3 **§ 11375. Fire safety systems in federally assisted buildings**

4 (a) DEFINITIONS.—For purposes of this section, the following definitions
5 apply:

6 (1) AFFORDABLE COST.—The term “affordable cost” means the cost
7 to a Federal agency of leasing office space in a building that is pro-
8 tected by an automatic sprinkler system or equivalent level of safety,
9 which cost is no more than 10 percent greater than the cost of leasing
10 available comparable office space in a building that is not so protected.

11 (2) AUTOMATIC SPRINKLER SYSTEM.—The term “automatic sprin-
12 kler system” means an electronically supervised, integrated system of
13 piping to which sprinklers are attached in a systematic pattern, and
14 that, when activated by heat from a fire—

15 (A) will protect human lives by discharging water over the fire
16 area, in accordance with the National Fire Protection Association
17 Standard 13, 13D, or 13R, whichever is appropriate for the type
18 of building and occupancy being protected, or any successor stand-
19 ard to that standard; and

20 (B) includes an alarm signaling system with appropriate warn-
21 ing signals (to the extent the alarm systems and warning signals
22 are required by Federal, State, or local laws or regulations) in-
23 stalled in accordance with the National Fire Protection Associa-
24 tion Standard 72, or any successor standard to that standard.

25 (3) EQUIVALENT LEVEL OF SAFETY.—The term “equivalent level of
26 safety” means an alternative design or system (that may include auto-
27 matic sprinkler systems), based on fire protection engineering analysis,
28 that achieves a level of safety equal to or greater than that provided
29 by automatic sprinkler systems.

30 (4) FEDERAL EMPLOYEE OFFICE BUILDING.—The term “Federal
31 employee office building” means an office building in the United
32 States, whether owned or leased by the Federal Government, that is
33 regularly occupied by more than 25 full-time Federal employees in the
34 course of their employment.

35 (5) HOUSING ASSISTANCE.—The term “housing assistance”—

36 (A) means assistance provided by the Federal Government to be
37 used in connection with the provision of housing that is provided
38 in the form of a grant, contract, loan, loan guarantee, cooperative
39 agreement, interest subsidy, insurance, or direct appropriation; but

40 (B) does not include assistance provided by—

41 (i) the Secretary of Veterans Affairs;

- 1 (ii) the Federal Emergency Management Agency;
2 (iii) the Secretary of Housing and Urban Development
3 under the single family mortgage insurance programs under
4 the National Housing Act (12 U.S.C. 1701 et seq.) or the
5 homeownership assistance program under section 235 of the
6 National Housing Act (12 U.S.C. 1715z);
7 (iv) the National Homeownership Trust; or
8 (v) the Federal Deposit Insurance Corporation under the
9 affordable housing program under section 40 of the Federal
10 Deposit Insurance Act (12 U.S.C. 1831q).

11 (6) HAZARDOUS AREAS.—The term “hazardous areas” means those
12 areas in a building referred to as hazardous areas in National Fire
13 Protection Association Standard 101, known as the Life Safety Code,
14 or any successor standard to that standard.

15 (7) MULTIFAMILY PROPERTY.—The term “multifamily property”
16 means—

17 (A) in the case of housing for Federal employees or their de-
18 pendents, a residential building consisting of more than 2 residen-
19 tial units that are under 1 roof; and

20 (B) in any other case, a residential building consisting of more
21 than 4 residential units that are under 1 roof.

22 (8) PREFIRE PLAN.—The term “prefire plan” means specific plans
23 for firefighting activities at a property or location.

24 (9) REBUILDING.—The term “rebuilding” means the repairing or re-
25 constructing of portions of a multifamily property where the cost of the
26 alterations is 70 percent or more of the replacement cost of the com-
27 pleted multifamily property, not including the value of the land on
28 which the multifamily property is located.

29 (10) RENOVATED.—The term “renovated” means the repairing or
30 reconstructing of 50 percent or more of the current value of a Federal
31 employee office building, not including the value of the land on which
32 the Federal employee office building is located.

33 (11) SMOKE DETECTORS.—The term “smoke detectors” means sin-
34 gle or multiple station, self-contained alarm devices designed to respond
35 to the presence of visible or invisible particles of combustion, installed
36 in accordance with the National Fire Protection Association Standard
37 74 or any successor standard to that standard.

38 (b) FEDERAL EMPLOYEE OFFICE BUILDINGS.—

39 (1) RESTRICTION ON USE OF FEDERAL FUNDS.—

40 (A) CONSTRUCTION OR PURCHASE.—No Federal funds may be
41 used for the construction or purchase of—

1 (i) a Federal employee office building of 6 or more stories
2 unless during the period of occupancy by Federal employees
3 the building is protected by an automatic sprinkler system or
4 equivalent level of safety; or

5 (ii) any other Federal employee office building unless dur-
6 ing the period of occupancy by Federal employees the haz-
7 ardous areas of the building are protected by automatic sprin-
8 kler systems or an equivalent level of safety.

9 (B) LEASE.—

10 (i) IN GENERAL.—No Federal funds may be used for the
11 lease of—

12 (I) a Federal employee office building of 6 or more
13 stories, where at least some portion of the federally
14 leased space is on the 6th floor or above and at least
15 35,000 square feet of space is federally occupied, unless
16 during the period of occupancy by Federal employees the
17 entire Federal employee office building is protected by an
18 automatic sprinkler system or equivalent level of safety;
19 or

20 (II) any other Federal employee office building unless
21 during the period of occupancy by Federal employees the
22 hazardous areas of the entire Federal employee office
23 building are protected by automatic sprinkler systems or
24 an equivalent level of safety.

25 (ii) EXCEPTION.—Clause (i)(I) shall not apply to the lease
26 of a building the construction of which is completed before
27 October 26, 1992, if the leasing agency certifies that no suit-
28 able building with automatic sprinkler systems or an equiva-
29 lent level of safety is available at an affordable cost.

30 (C) RENOVATION.—No Federal funds may be used for the ren-
31 ovation of—

32 (i) a Federal employee office building of 6 or more stories
33 that is owned by the Federal Government unless after that
34 renovation the Federal employee office building is protected
35 by an automatic sprinkler system or equivalent level of safety;
36 or

37 (ii) any other Federal employee office building that is
38 owned by the Federal Government unless after that renova-
39 tion the hazardous areas of the Federal employee office build-
40 ing are protected by automatic sprinkler systems or an equiv-
41 alent level of safety.

1 (D) ENTERING INTO OR RENEWING A LEASE OF A FEDERAL
2 EMPLOYEE OFFICE BUILDING RENOVATED AFTER OCTOBER 26,
3 1992.—No Federal funds may be used for entering into or renew-
4 ing a lease of—

5 (i) a Federal employee office building of 6 or more stories
6 that is renovated after October 26, 1992, where at least some
7 portion of the federally leased space is on the 6th floor or
8 above and at least 35,000 square feet of space is federally oc-
9 cupied, unless after that renovation the Federal employee of-
10 fice building is protected by an automatic sprinkler system or
11 equivalent level of safety; or

12 (ii) any other Federal employee office building that is ren-
13 ovated after October 26, 1992, unless after that renovation
14 the hazardous areas of the Federal employee office building
15 are protected by automatic sprinkler systems or an equivalent
16 level of safety.

17 (2) EXCEPTIONS.—

18 (A) ACTIONS BEFORE OCTOBER 26, 1992, OR TEMPORARY
19 LEASE.—Subparagraphs (A) and (B) of paragraph (1) shall not
20 apply to—

21 (i) a Federal employee office building that was owned by
22 the Federal Government before October 26, 1992;

23 (ii) space leased in a Federal employee office building if the
24 space was leased by the Federal Government before October
25 26, 1992;

26 (iii) space leased on a temporary basis for not longer than
27 6 months; or

28 (iv) a Federal employee office building that becomes a Fed-
29 eral employee office building pursuant to a commitment to
30 move Federal employees into the building that is made prior
31 to October 26, 1992.

32 (B) INSTALLATION OF AUTOMATIC SPRINKLER SYSTEM OR
33 EQUIVALENT LEVEL OF SAFETY NOT REQUIRED.—Nothing in this
34 subsection shall require the installation of an automatic sprinkler
35 system or equivalent level of safety by reason of the leasing, after
36 October 26, 1992, of space below the 6th floor in a Federal em-
37 ployee office building.

38 (c) HOUSING.—

39 (1) FOR FEDERAL EMPLOYEES AND THEIR DEPENDENTS.—

40 (A) IN GENERAL.—No Federal funds may be used for the con-
41 struction, purchase, lease, or operation by the Federal Government

1 of housing in the United States for Federal employees or their de-
2 pendents unless—

3 (i) in the case of a multifamily property acquired or rebuilt
4 by the Federal Government after October 26, 1992, the hous-
5 ing is protected, before occupancy by Federal employees or
6 their dependents, by an automatic sprinkler system (or equiv-
7 alent level of safety) and hard-wired smoke detectors; and

8 (ii) in the case of any other housing, the housing is pro-
9 tected by hard-wired smoke detectors.

10 (B) HIGHER LEVEL OF FIRE SAFETY PROTECTION NOT SUPER-
11 SEDED.—Nothing in this paragraph shall be construed to super-
12 sede any guidelines or requirements applicable to housing for Fed-
13 eral employees that call for a higher level of fire safety protection
14 than is required under this paragraph.

15 (C) ADEQUATE AND RELIABLE ELECTRICAL SYSTEM NOT AVAIL-
16 ABLE.—Housing covered by this paragraph that does not have an
17 adequate and reliable electrical system shall not be subject to the
18 requirement under subparagraph (A) for protection by hard-wired
19 smoke detectors but shall be protected by battery operated smoke
20 detectors.

21 (D) HOUSING SCHEDULED FOR DEMOLITION.—If funding has
22 been programmed or designated for the demolition of housing cov-
23 ered by this paragraph, the housing shall not be subject to the fire
24 protection requirements of subparagraph (A) but shall be pro-
25 tected by battery operated smoke detectors.

26 (2) HOUSING ASSISTANCE.—

27 (A) NEWLY CONSTRUCTED MULTIFAMILY PROPERTY.—

28 (i) DEFINITION OF NEWLY CONSTRUCTED MULTIFAMILY
29 PROPERTY.—For purposes of clause (ii), the term “newly
30 constructed multifamily property” means a multifamily prop-
31 erty of 4 or more stories above ground level—

32 (I) that is newly constructed after October 26, 1992;
33 and

34 (II) for which—

35 (aa) housing assistance is used for the new con-
36 struction; or

37 (bb) a binding commitment is made, before com-
38 mencement of the construction, to provide housing
39 assistance for the newly constructed property.

40 (ii) RESTRICTION ON USE OF HOUSING ASSISTANCE.—
41 Housing assistance may not be used in connection with newly

1 constructed multifamily property, unless after the new con-
2 struction the multifamily property is protected by an auto-
3 matic sprinkler system and hard-wired smoke detectors.

4 (iii) EXCEPTION.—Clause (ii) shall not apply to multifamily
5 property for which, before October 26, 1992, a binding com-
6 mitment was made to provide housing assistance for the new
7 construction of the property or for the newly constructed
8 property.

9 (B) REBUILT MULTIFAMILY PROPERTY.—

10 (i) DEFINITION OF REBUILT MULTIFAMILY PROPERTY.—
11 For purposes of this subparagraph, the term “rebuilt multi-
12 family property” means a multifamily property of 4 or more
13 stories above ground level—

14 (I) that is rebuilt after the last day of the second fis-
15 cal year that ends after October 26, 1992; and

16 (II) for which—

17 (aa) housing assistance is used for the rebuilding;

18 or

19 (bb) a binding commitment is made, before com-
20 mencement of the rebuilding, to provide housing as-
21 sistance for the rebuilt property.

22 (ii) RESTRICTION ON USE OF HOUSING ASSISTANCE.—Ex-
23 cept as provided in clause (iii), housing assistance may not
24 be used in connection with rebuilt multifamily property, un-
25 less after the rebuilding the multifamily property complies
26 with the chapter on existing apartment buildings of National
27 Fire Protection Association Standard 101 (known as the Life
28 Safety Code) or any successor standard to that standard, as
29 in effect at the earlier of—

30 (I) the time of any approval by the Department of
31 Housing and Urban Development of the specific plan or
32 budget for rebuilding; or

33 (II) the time that a binding commitment is made to
34 provide housing assistance for the rebuilt property.

35 (iii) EXCEPTION.—If a rebuilt multifamily property is sub-
36 ject to, and in compliance with, a provision of a State or local
37 fire safety standard or code that prevents compliance with a
38 specific provision of National Fire Protection Association
39 Standard 101 or any successor standard to that standard, the
40 requirement under clause (ii) shall not apply with respect to
41 the specific provision.

1 (C) OTHER DWELLING UNIT.—Housing assistance may not be
2 used in connection with any other dwelling unit, unless the unit
3 is protected by a hard-wired or battery-operated smoke detector.
4 For purposes of this subparagraph, housing assistance shall be
5 considered to be used in connection with a particular dwelling unit
6 only if the assistance is provided—

7 (i) for the particular unit, in the case of assistance pro-
8 vided on a unit-by-unit basis; or

9 (ii) for the multifamily property in which the unit is lo-
10 cated, in the case of assistance provided on a structure-by-
11 structure basis.

12 (d) REGULATIONS.—The Administrator of General Services, in coopera-
13 tion with the Administration, the National Institute of Standards and Tech-
14 nology, and the Department of Defense shall promulgate regulations to fur-
15 ther define the term “equivalent level of safety”, and shall, to the extent
16 practicable, base those regulations on nationally recognized codes.

17 (e) STATE AND LOCAL AUTHORITY NOT LIMITED.—Nothing in this sec-
18 tion shall be construed—

19 (1) to limit the power of a State or political subdivision of a State
20 to implement or enforce a law, rule, regulation, or standard that estab-
21 lishes requirements concerning fire prevention and control; or

22 (2) to reduce fire resistance requirements that otherwise would have
23 been required.

24 (f) PREFIRE PLAN.—The head of a Federal agency that owns, leases, or
25 operates a building or housing unit with Federal funds shall invite the local
26 agency or voluntary organization having responsibility for fire protection in
27 the jurisdiction where the building or housing unit is located to prepare, and
28 biennially review, a prefire plan for the building or housing unit.

29 (g) REPORTS TO CONGRESS.—Within 3 years after October 26, 1992,
30 and every 3 years thereafter, the Administrator of General Services shall
31 transmit to Congress a report on the level of fire safety in Federal employee
32 office buildings subject to fire safety requirements under this section. The
33 report shall contain a description of the buildings for each Federal agency.

34 (h) RELATION TO OTHER REQUIREMENTS.—In the implementation of
35 this section, the process for meeting space needs in urban areas shall con-
36 tinue to give first consideration to a centralized community business area
37 and adjacent areas of similar character to the extent of any Federal require-
38 ment for meeting those needs.

1 **§ 11376. CPR training**

2 No funds shall be made available to a State or local government under
3 section 11367 of this title unless the government has a policy to actively
4 promote the training of its firefighters in cardiopulmonary resuscitation.

5 **§ 11377. Firefighter assistance**

6 (a) DEFINITIONS.—In this section:

7 (1) ADMINISTRATOR OF FEMA.—The term “Administrator of
8 FEMA” means the Administrator of FEMA, acting through the Ad-
9 ministrator.

10 (2) AVAILABLE GRANT FUNDS.—The term “available grant funds”,
11 with respect to a fiscal year, means those funds appropriated pursuant
12 to the authorization of appropriations in subsection (q)(1) for the fiscal
13 year less funds used for administrative costs pursuant to subsection
14 (q)(2) in that fiscal year.

15 (3) CAREER FIRE DEPARTMENT.—The term “career fire depart-
16 ment” means a fire department that has an all-paid force of fire-
17 fighting personnel other than paid-on-call firefighters.

18 (4) COMBINATION FIRE DEPARTMENT.—The term “combination fire
19 department” means a fire department that has—

20 (A) paid firefighting personnel; and

21 (B) volunteer firefighting personnel.

22 (5) FIREFIGHTING PERSONNEL.—The term “firefighting personnel”
23 means individuals, including volunteers, who are firefighters, officers of
24 fire departments, or emergency medical service personnel of fire depart-
25 ments.

26 (6) INSTITUTION OF HIGHER EDUCATION.—The term “institution of
27 higher education” has the meaning given the term in section 101 of
28 the Higher Education Act of 1965 (20 U.S.C. 1001).

29 (7) NONAFFILIATED EMS ORGANIZATION.—The term “nonaffiliated
30 EMS organization” means a public or private nonprofit emergency
31 medical services organization that is not affiliated with a hospital and
32 does not serve a geographic area in which the Administrator of FEMA
33 finds that emergency medical services are adequately provided by a fire
34 department.

35 (8) PAID-ON-CALL.—The term “paid-on-call” with respect to fire-
36 fighting personnel means firefighting personnel who are paid a stipend
37 for each event to which they respond.

38 (9) VOLUNTEER FIRE DEPARTMENT.—The term “volunteer fire de-
39 partment” means a fire department that has an all-volunteer force of
40 firefighting personnel.

41 (b) ASSISTANCE PROGRAM.—

1 (1) AUTHORITY TO AWARD ASSISTANCE.—In accordance with this
2 section, the Administrator of FEMA may award—

- 3 (A) assistance to firefighters grants under subsection (c); and
4 (B) fire prevention and safety grants and other assistance under
5 subsection (d).

6 (2) DUTIES OF ADMINISTRATOR OF FEMA.—The Administrator of
7 FEMA shall—

- 8 (A) establish specific criteria for the selection of grant recipients
9 under this section; and
10 (B) provide assistance with application preparation to applicants
11 for the grants.

12 (c) ASSISTANCE TO FIREFIGHTERS GRANTS.—

13 (1) IN GENERAL.—The Administrator of FEMA may, in consultation
14 with the chief executives of the States in which the recipients are lo-
15 cated, award grants on a competitive basis directly to—

- 16 (A) fire departments for the purpose of protecting the health
17 and safety of the public and firefighting personnel throughout the
18 United States against fire, fire-related, and other hazards;
19 (B) nonaffiliated EMS organizations to support the provision of
20 emergency medical services; and
21 (C) State fire training academies for the purposes described in
22 subparagraphs (G), (H), and (I) of paragraph (3).

23 (2) MAXIMUM GRANT AMOUNTS.—

24 (A) POPULATION.—The Administrator of FEMA may not
25 award a grant under this subsection in excess of amounts as fol-
26 lows:

27 (i) In the case of a recipient that serves a jurisdiction with
28 100,000 people or fewer, the amount of the grant awarded to
29 the recipient shall not exceed \$1,000,000 in a fiscal year.

30 (ii) In the case of a recipient that serves a jurisdiction with
31 more than 100,000 people but not more than 500,000 people,
32 the amount of the grant awarded to the recipient shall not
33 exceed \$2,000,000 in a fiscal year.

34 (iii) In the case of a recipient that serves a jurisdiction
35 with more than 500,000 but not more than 1,000,000 people,
36 the amount of the grant awarded to the recipient shall not
37 exceed \$3,000,000 in a fiscal year.

38 (iv) In the case of a recipient that serves a jurisdiction with
39 more than 1,000,000 people but not more than 2,500,000
40 people, the amount of the grant awarded to the recipient shall
41 not exceed \$6,000,000 for a fiscal year.

1 (v) In the case of a recipient that serves a jurisdiction with
2 more than 2,500,000 people, the amount of the grant award-
3 ed to the recipient shall not exceed \$9,000,000 in a fiscal
4 year.

5 (B) AGGREGATE.—

6 (i) IN GENERAL.—Notwithstanding subparagraph (A) and
7 except as provided under clause (ii), the Administrator of
8 FEMA may not award a grant under this subsection in a fis-
9 cal year that exceeds 1 percent of the available grant funds
10 in that fiscal year.

11 (ii) EXCEPTION.—The Administrator of FEMA may waive
12 the limitation in clause (i) with respect to a grant recipient
13 if the Administrator of FEMA determines that the recipient
14 has an extraordinary need for a grant in an amount that ex-
15 ceeds the limit under clause (i).

16 (3) USE OF GRANT FUNDS.—Each entity receiving a grant under
17 this subsection shall use the grant for 1 or more of the following pur-
18 poses:

19 (A) To train firefighting personnel in—

20 (i) firefighting;

21 (ii) emergency medical services and other emergency re-
22 sponse (including response to natural disasters, acts of ter-
23 rorism, and other man-made disasters);

24 (iii) arson prevention and detection;

25 (iv) maritime firefighting; or

26 (v) the handling of hazardous materials.

27 (B) To train firefighting personnel to provide any of the train-
28 ing described under subparagraph (A).

29 (C) To fund the creation of rapid intervention teams to protect
30 firefighting personnel at the scenes of fires and other emergencies.

31 (D) To certify—

32 (i) fire inspectors; and

33 (ii) building inspectors—

34 (I) whose responsibilities include fire safety inspec-
35 tions; and

36 (II) who are employed by or serving as volunteers with
37 a fire department.

38 (E) To establish wellness and fitness programs for firefighting
39 personnel to ensure that the firefighting personnel are able to
40 carry out their duties as firefighters, including programs dedicated

1 to raising awareness of, and preventing, job-related mental health
2 issues.

3 (F) To fund emergency medical services provided by fire depart-
4 ments and nonaffiliated EMS organizations.

5 (G) To acquire additional firefighting vehicles, including fire
6 trucks and other apparatus.

7 (H) To acquire additional firefighting equipment, including
8 equipment for—

9 (i) fighting fires with foam in remote areas without access
10 to water; and

11 (ii) communications, monitoring, and responding to a nat-
12 ural disaster or act of terrorism or other man-made disaster,
13 including the use of a weapon of mass destruction.

14 (I) To acquire personal protective equipment, including personal
15 protective equipment—

16 (i) prescribed for firefighting personnel by the Occupational
17 Safety and Health Administration of the Department of
18 Labor; or

19 (ii) for responding to a natural disaster or act of terrorism
20 or other man-made disaster, including the use of a weapon
21 of mass destruction.

22 (J) To modify fire stations, fire training facilities, and other fa-
23 cilities to protect the health and safety of firefighting personnel.

24 (K) To educate the public about arson prevention and detection.

25 (L) To provide incentives for the recruitment and retention of
26 volunteer firefighting personnel for volunteer firefighting depart-
27 ments and other firefighting departments that utilize volunteers.

28 (M) To provide specialized training to firefighters, paramedics,
29 emergency medical service workers, and other first responders to
30 recognize individuals who have mental illness and how to properly
31 intervene with individuals with mental illness, including strategies
32 for verbal de-escalation of crisis.

33 (N) To support such other activities, consistent with the pur-
34 poses of this subsection, as the Administrator of FEMA deter-
35 mines appropriate.

36 (d) FIRE PREVENTION AND SAFETY GRANTS

37 (1) IN GENERAL.—For the purpose of assisting fire prevention pro-
38 grams and supporting firefighter health and safety research and devel-
39 opment, the Administrator of FEMA may, on a competitive basis—

40 (A) award grants to fire departments;

1 (B) award grants to, or enter into contracts or cooperative
2 agreements with, national, State, local, tribal, or nonprofit organi-
3 zations that are not fire departments and that are recognized for
4 their experience and expertise with respect to fire prevention or
5 fire safety programs and activities and firefighter research and de-
6 velopment programs, for the purpose of carrying out—

- 7 (i) fire prevention programs; and
8 (ii) research to improve firefighter health and life safety;
9 and

10 (C) award grants to institutions of higher education, national
11 fire service organizations, or national fire safety organizations to
12 establish and operate fire safety research centers.

13 (2) MAXIMUM GRANT AMOUNT.—A grant awarded under this sub-
14 section may not exceed \$1,500,000 for a fiscal year.

15 (3) USE OF GRANT FUNDS.—Each entity receiving a grant under
16 this subsection shall use the grant for 1 or more of the following pur-
17 poses:

18 (A) To enforce fire codes and promote compliance with fire safe-
19 ty standards.

20 (B) To fund fire prevention programs, including programs that
21 educate the public about arson prevention and detection.

22 (C) To fund wildland fire prevention programs, including edu-
23 cation, awareness, and mitigation programs that protect lives,
24 property, and natural resources from fire in the wildland-urban
25 interface.

26 (D) In the case of a grant awarded under paragraph (1)(C), to
27 fund the establishment or operation of a fire safety research center
28 for the purpose of significantly reducing the number of fire-related
29 deaths and injuries among firefighters and the general public
30 through research, development, and technology transfer activities.

31 (E) To support such other activities, consistent with the pur-
32 poses of this subsection, as the Administrator of FEMA deter-
33 mines appropriate.

34 (4) LIMITATION.—None of the funds made available under this sub-
35 section may be provided to the Association of Community Organiza-
36 tions for Reform Now (ACORN) or any of its affiliates, subsidiaries,
37 or allied organizations.

38 (e) APPLICATIONS FOR GRANTS.—

39 (1) IN GENERAL.—An entity seeking a grant under this section shall
40 submit to the Administrator of FEMA an application in such form and
41 in such manner as the Administrator of FEMA determines appropriate.

1 (2) ELEMENTS.—Each application submitted under paragraph (1)
2 shall include the following:

3 (A) A description of the financial need of the applicant for the
4 grant.

5 (B) An analysis of the costs and benefits, with respect to public
6 safety, of the use for which a grant is requested.

7 (C) An agreement to provide information to the national fire in-
8 cident reporting system for the period covered by the grant.

9 (D) A list of other sources of funding received by the appli-
10 cant—

11 (i) for the same purpose for which the application for a
12 grant under this section was submitted; or

13 (ii) from the Federal Government for other fire-related pur-
14 poses.

15 (E) Such other information as the Administrator of FEMA de-
16 termines appropriate.

17 (3) JOINT OR REGIONAL APPLICATIONS.—

18 (A) IN GENERAL.—Two or more entities may submit an applica-
19 tion under paragraph (1) for a grant under this section to fund
20 a joint program or initiative, including acquisition of shared equip-
21 ment or vehicles.

22 (B) NONEXCLUSIVITY.—Applications under this paragraph may
23 be submitted instead of or in addition to any other application
24 submitted under paragraph (1).

25 (C) GUIDANCE.—The Administrator of FEMA shall—

26 (i) publish guidance on applying for and administering
27 grants awarded for joint programs and initiatives described in
28 subparagraph (A); and

29 (ii) encourage applicants to apply for grants for joint pro-
30 grams and initiatives described in subparagraph (A) as the
31 Administrator of FEMA determines appropriate to achieve
32 greater cost effectiveness and regional efficiency.

33 (f) PEER REVIEW OF GRANT APPLICATIONS.—

34 (1) IN GENERAL.—The Administrator of FEMA shall, after con-
35 sultation with national fire service and emergency medical services or-
36 ganizations, appoint fire service personnel to conduct peer reviews of
37 applications received under subsection (e)(1).

38 (2) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of
39 title 5 shall not apply to activities carried out pursuant to this sub-
40 section.

1 (g) CONSIDERATIONS FOR GRANT AWARDS.—In awarding grants under
2 this section, the Administrator of FEMA shall consider the following:

3 (1) The findings and recommendations of the peer reviews carried
4 out under subsection (f).

5 (2) The degree to which an award will reduce deaths, injuries, and
6 property damage by reducing the risks associated with fire-related and
7 other hazards.

8 (3) The extent of the need of an applicant for a grant under this
9 section and the need to protect the United States as a whole.

10 (4) The number of calls requesting or requiring a firefighting or
11 emergency medical response received by an applicant.

12 (h) ALLOCATION OF GRANT AWARDS.—In awarding grants under this
13 section, the Administrator of FEMA shall ensure that of the available grant
14 funds in each fiscal year—

15 (1) not less than 25 percent is awarded under subsection (c) to ca-
16 reer fire departments;

17 (2) not less than 25 percent is awarded under subsection (c) to vol-
18 unteer fire departments;

19 (3) not less than 25 percent is awarded under subsection (c) to com-
20 bination fire departments and fire departments using paid-on-call fire-
21 fighting personnel;

22 (4) not less than 10 percent is available for open competition among
23 career fire departments, volunteer fire departments, combination fire
24 departments, and fire departments using paid-on-call firefighting per-
25 sonnel for grants awarded under subsection (c);

26 (5) not less than 10 percent is awarded under subsection (d); and

27 (6) not more than 2 percent is awarded under this section to non-
28 affiliated EMS organizations described in subsection (c)(1)(B).

29 (i) ADDITIONAL REQUIREMENTS AND LIMITATIONS.—

30 (1) FUNDING FOR EMERGENCY MEDICAL SERVICES.—Not less than
31 3.5 percent of the available grant funds for a fiscal year shall be
32 awarded under this section for purposes described in subsection
33 (c)(3)(F).

34 (2) STATE FIRE TRAINING ACADEMIES.—

35 (A) MAXIMUM SHARE.—Not more than 3 percent of the avail-
36 able grant funds for a fiscal year may be awarded under sub-
37 section (c)(1)(C).

38 (B) MAXIMUM GRANT AMOUNT.—The Administrator of FEMA
39 may not award a grant under subsection (c)(1)(C) to a State fire
40 training academy in an amount that exceeds \$1,000,000 in a fiscal
41 year.

1 (3) AMOUNTS FOR PURCHASING FIREFIGHTING VEHICLES.—Not
2 more than 25 percent of the available grant funds for a fiscal year may
3 be used to assist grant recipients to purchase vehicles pursuant to sub-
4 section (e)(3)(G).

5 (j) FURTHER CONSIDERATIONS.—

6 (1) ASSISTANCE TO FIREFIGHTERS GRANTS TO FIRE DEPART-
7 MENTS.—In considering applications for grants under subsection
8 (e)(1)(A), the Administrator of FEMA shall consider—

9 (A) the extent to which the grant would enhance the daily oper-
10 ations of the applicant and the impact of the grant on the protec-
11 tion of lives and property; and

12 (B) a broad range of factors important to the applicant's ability
13 to respond to fires and related hazards, such as the following:

14 (i) Population served.

15 (ii) Geographic response area.

16 (iii) Hazards vulnerability.

17 (iv) Call volume.

18 (v) Financial situation, including unemployment rate of the
19 area being served.

20 (vi) Need for training or equipment.

21 (2) APPLICATIONS FROM NONAFFILIATED EMS ORGANIZATIONS.—In
22 the case of an application submitted under subsection (e)(1) by a non-
23 affiliated EMS organization, the Administrator of FEMA shall consider
24 the extent to which other sources of Federal funding are available to
25 the applicant to provide the assistance requested in the application.

26 (3) FIRE PREVENTION AND SAFETY GRANTS TO CERTAIN ORGANIZA-
27 TIONS THAT ARE NOT FIRE DEPARTMENTS.—In the case of applicants
28 for grants under this section that are described in subsection (d)(1)(B),
29 the Administrator of FEMA shall give priority to applicants that focus
30 on

31 (A) prevention of injuries to high risk groups from fire; and

32 (B) research programs that demonstrate a potential to improve
33 firefighter safety.

34 (4) GRANTS FOR FIRE SAFETY RESEARCH CENTERS.—

35 (A) CONSIDERATIONS.—In awarding grants under subsection
36 (d)(1)(C), the Administrator of FEMA shall—

37 (i) select each grant recipient on—

38 (I) the demonstrated research and extension resources
39 available to the recipient to carry out the research, devel-
40 opment, and technology transfer activities;

- 1 (II) the capability of the recipient to provide leader-
- 2 ship in making national contributions to fire safety;
- 3 (III) the recipient’s ability to disseminate the results
- 4 of fire safety research; and
- 5 (IV) the strategic plan the recipient proposes to carry
- 6 out under the grant;

7 (ii) give special consideration in selecting recipients under
 8 clause (i) to an applicant for a grant that consists of a part-
 9 nership between—

10 (I) a national fire service organization or a national
 11 fire safety organization; and

12 (II) an institution of higher education, including a mi-
 13 nority-serving institution (as described in section 371(a)
 14 of the Higher Education Act of 1965 (20 U.S.C.
 15 1067q(a)); and

16 (iii) consider the research needs identified and prioritized
 17 through the workshop required by subparagraph (B)(i).

18 (B) RESEARCH NEEDS.—

19 (i) WORKSHOP TO IDENTIFY NEEDS.—The Administrator
 20 of FEMA shall convene a workshop of the fire safety research
 21 community, fire service organizations, and other appropriate
 22 stakeholders to identify and prioritize fire safety research
 23 needs.

24 (ii) PUBLICATION OF RESULTS.—The Administrator of
 25 FEMA shall ensure that the results of the workshop are
 26 made available to the public.

27 (C) LIMITATIONS ON GRANTS FOR FIRE SAFETY RESEARCH
 28 CENTERS.—

29 (i) IN GENERAL.—The Administrator of FEMA may award
 30 grants under subsection (d) to establish not more than 3 fire
 31 safety research centers.

32 (ii) RECIPIENTS.—An institution of higher education, a na-
 33 tional fire service organization, and a national fire safety or-
 34 ganization may not directly receive a grant under subsection
 35 (d) for a fiscal year for more than 1 fire safety research cen-
 36 ter.

37 (5) AVOIDING DUPLICATION.—The Administrator of FEMA shall re-
 38 view lists submitted by applicants pursuant to subsection (e)(2)(D) and
 39 take such actions as the Administrator of FEMA considers necessary
 40 to prevent unnecessary duplication of grant awards.

41 (k) MATCHING AND MAINTENANCE OF EXPENDITURE REQUIREMENTS.—

1 (1) MATCHING REQUIREMENT FOR ASSISTANCE TO FIREFIGHTERS
2 GRANTS.—

3 (A) IN GENERAL.—Except as provided in subparagraph (B), an
4 applicant seeking a grant to carry out an activity under subsection
5 (c) shall agree to make available non-Federal funds to carry out
6 the activity in an amount equal to not less than 15 percent of the
7 grant awarded to the applicant under subsection (c).

8 (B) EXCEPTION FOR ENTITIES SERVING SMALL COMMU-
9 NITIES.—In the case that an applicant seeking a grant to carry
10 out an activity under subsection (c) serves a jurisdiction of—

11 (i) more than 20,000 residents but not more than
12 1,000,000 residents, the applicant shall agree to make avail-
13 able non-Federal funds in an amount equal to not less than
14 10 percent of the grant awarded to the applicant under sub-
15 section (c); and

16 (ii) 20,000 residents or fewer, the applicant shall agree to
17 make available non-Federal funds in an amount equal to not
18 less than 5 percent of the grant awarded to the applicant
19 under subsection (c).

20 (2) MATCHING REQUIREMENT FOR FIRE PREVENTION AND SAFETY
21 GRANTS.—

22 (A) IN GENERAL.—An applicant seeking a grant to carry out
23 an activity under subsection (d) shall agree to make available non-
24 Federal funds to carry out the activity in an amount equal to not
25 less than 5 percent of the grant awarded to the applicant under
26 subsection (d).

27 (B) MEANS OF MATCHING.—An applicant for a grant under
28 subsection (d) may meet the matching requirement under subpara-
29 graph (A) through direct funding, funding of complementary ac-
30 tivities, or the provision of staff, facilities, services, material, or
31 equipment.

32 (3) MAINTENANCE OF EXPENDITURES.—An applicant seeking a
33 grant under subsection (c) or (d) shall agree to maintain during the
34 term of the grant the applicant's aggregate expenditures relating to the
35 uses described in subsections (c)(3) and (d)(3) at not less than 80 per-
36 cent of the average amount of the expenditures in the 2 fiscal years
37 preceding the fiscal year in which the grant amounts are received.

38 (4) WAIVER OR REDUCTION OF REQUIREMENTS.—

39 (A) IN GENERAL.—Except as provided in subparagraph (C)(ii),
40 the Administrator of FEMA may waive or reduce the requirements

1 of paragraphs (1), (2), and (3) in cases of demonstrated economic
2 hardship.

3 (B) GUIDELINES.—

4 (i) IN GENERAL.—The Administrator of FEMA shall estab-
5 lish and publish guidelines for determining what constitutes
6 economic hardship for purposes of this paragraph.

7 (ii) CONSULTATION.—In developing guidelines under clause
8 (i), the Administrator of FEMA shall consult with individuals
9 who are—

10 (I) recognized for expertise in firefighting, emergency
11 medical services provided by fire services, or the eco-
12 nomic affairs of State and local governments; and

13 (II) members of national fire service organizations or
14 national organizations representing the interests of State
15 and local governments.

16 (iii) CONSIDERATIONS.—In developing guidelines under
17 clause (i), the Administrator of FEMA shall consider, with
18 respect to relevant communities, the following:

19 (I) Changes in rates of unemployment from previous
20 years.

21 (II) Whether the rates of unemployment of the rel-
22 evant communities are currently exceeding and have con-
23 sistently exceeded the annual national average rates of
24 unemployment.

25 (III) Changes in percentages of individuals eligible to
26 receive food stamps from previous years.

27 (IV) Such other factors as the Administrator of
28 FEMA considers appropriate.

29 (C) CERTAIN APPLICANTS FOR FIRE PREVENTION AND SAFETY
30 GRANTS NOT ELIGIBLE FOR WAIVER OR REDUCTION.—The author-
31 ity under subparagraph (A) shall not apply with respect to a non-
32 profit organization that—

33 (i) is described in subsection (d)(1)(B); and

34 (ii) is not a fire department or emergency medical services
35 organization.

36 (I) GRANT GUIDELINES.—

37 (1) ANNUAL PUBLICATION IN FEDERAL REGISTER.—For each fiscal
38 year, prior to awarding grants under this section, the Administrator of
39 FEMA shall publish in the Federal Register—

40 (A) guidelines that describe—

1 (i) the process for applying for grants under this section;
2 and

3 (ii) the criteria that will be used for selecting grant recipi-
4 ents; and

5 (B) an explanation of any differences between the guidelines
6 and the recommendations obtained under paragraph (2).

7 (2) ANNUAL MEETING TO OBTAIN RECOMMENDATIONS.—

8 (A) QUALIFIED MEMBERS.—For purposes of this paragraph, a
9 qualified member of an organization is a member who—

10 (i) is recognized for expertise in firefighting or emergency
11 medical services;

12 (ii) is not an employee of the Federal Government; and

13 (iii) in the case of a member of an emergency medical serv-
14 ice organization, is a member of an organization that rep-
15 resents—

16 (I) providers of emergency medical services that are
17 affiliated with fire departments; or

18 (II) nonaffiliated EMS providers.

19 (B) IN GENERAL.—For each fiscal year, the Administrator of
20 FEMA shall convene a meeting of qualified members of national
21 fire service organizations and, at the discretion of the Adminis-
22 trator of FEMA, qualified members of emergency medical service
23 organizations to obtain recommendations regarding the following:

24 (i) Criteria for the awarding of grants under this section.

25 (ii) Administrative changes to the assistance program es-
26 tablished under subsection (b).

27 (3) INAPPLICABILITY OF CHAPTER 5 OF TITLE 10.—Chapter 5 of
28 title 10 shall not apply to activities carried out under this subsection.

29 (m) ACCOUNTING DETERMINATION.—Notwithstanding another law, for
30 purposes of this section, equipment costs shall include all costs attributable
31 to any design, purchase of components, assembly, manufacture, and trans-
32 portation of equipment not otherwise commercially available.

33 (n) ELIGIBLE GRANTEE ON BEHALF OF ALASKA NATIVE VILLAGES.—
34 The Alaska Village Initiatives, a non-profit organization incorporated in
35 Alaska, shall be eligible to apply for and receive a grant or other assistance
36 under this section on behalf of Alaska Native villages.

37 (o) TRAINING STANDARDS.—If an applicant for a grant under this sec-
38 tion is applying for the grant to purchase training that does not meet or
39 exceed any applicable national voluntary consensus standards, including
40 those developed under section 20507 of this title, the applicant shall submit
41 to the Administrator of FEMA an explanation of the reasons that the train-

1 ing proposed to be purchased will serve the needs of the applicant better
2 than training that meets or exceeds the standards.

3 (p) ENSURING EFFECTIVE USE OF GRANTS.—

4 (1) AUDITS.—The Administrator of FEMA may audit a recipient of
5 a grant awarded under this section to ensure that—

6 (A) the grant amounts are expended for the intended purposes;

7 and

8 (B) the grant recipient complies with the requirements of sub-
9 section (k).

10 (2) PERFORMANCE ASSESSMENT.—

11 (A) IN GENERAL.—The Administrator of FEMA shall develop
12 and implement a performance assessment system, including quan-
13 tifiable performance metrics, to evaluate the extent to which
14 grants awarded under this section are furthering the purposes of
15 this section, including protecting the health and safety of the pub-
16 lic and firefighting personnel against fire and fire-related hazards.

17 (B) CONSULTATION.—The Administrator of FEMA shall con-
18 sult with fire service representatives and with the Comptroller
19 General in developing the assessment system required by subpara-
20 graph (A).

21 (3) ANNUAL REPORTS TO ADMINISTRATOR OF FEMA.—Not less fre-
22 quently than once each year during the term of a grant awarded under
23 this section, the recipient of the grant shall submit to the Adminis-
24 trator of FEMA an annual report describing how the recipient used the
25 grant amounts.

26 (q) AUTHORIZATION OF APPROPRIATIONS.—

27 (1) IN GENERAL.—There is authorized to be appropriated to carry
28 out this section for fiscal year 2023 an amount equal to the amount
29 authorized for the previous fiscal year increased by the percentage by
30 which—

31 (A) the Consumer Price Index (all items, United States city av-
32 erage) for the previous fiscal year; exceeds

33 (B) the Consumer Price Index for the fiscal year preceding the
34 fiscal year described in subparagraph (A).

35 (2) ADMINISTRATIVE EXPENSES.—Of the amounts appropriated pur-
36 suant to paragraph (1) for a fiscal year, the Administrator of FEMA
37 may use not more than 5 percent of the amounts for salaries and ex-
38 penses and other administrative costs incurred by the Administrator of
39 FEMA in the course of awarding grants and providing assistance
40 under this section.

1 (3) CONGRESSIONALLY DIRECTED SPENDING NOT ALLOWED.—Con-
2 sistent with the requirements in subsections (c)(1) and (d)(1) that
3 grants under those subsections be awarded on a competitive basis, none
4 of the funds appropriated pursuant to this subsection may be used for
5 a congressionally directed spending item (as defined under the rules of
6 the Senate and the House of Representatives).

7 (r) SUNSET OF AUTHORITIES.—The authority to award assistance and
8 grants under this section shall expire on September 30, 2024.

9 **§ 11378. Staffing for adequate fire and emergency response**

10 (a) DEFINITION OF FIREFIGHTER.—In this section, the term “fire-
11 fighter” has the meaning given the term “employee in fire protection activi-
12 ties” under section 3 of the Fair Labor Standards Act of 1938 (29 U.S.C.
13 203).

14 (b) EXPANDED AUTHORITY TO MAKE GRANTS.—

15 (1) HIRING GRANTS.—

16 (A) PURPOSE.—The Administrator of FEMA shall make grants
17 directly to career fire departments, combination fire departments,
18 and volunteer fire departments, in consultation with the chief execu-
19 tive of the State in which the applicant is located, for the purpose
20 of increasing the number of firefighters to help communities meet
21 industry minimum standards and attain 24-hour staffing to pro-
22 vide adequate protection from fire and fire-related hazards, and to
23 fulfill traditional missions of fire departments that antedate the
24 creation of the Department.

25 (B) TERM AND USE.—Grants made under this paragraph shall
26 be for 3 years and be used for programs to hire new, additional
27 firefighters or to change the status of part-time or paid-on-call (as
28 defined in section 11377 of this title) firefighters to full-time fire-
29 fighters.

30 (C) PREFERENTIAL CONSIDERATION.—In awarding grants
31 under this subsection, the Administrator of FEMA may give pref-
32 erential consideration to applications that involve a non-Federal
33 contribution exceeding the minimums under subparagraph (E).

34 (D) TECHNICAL ASSISTANCE.—The Administrator of FEMA
35 may provide technical assistance to States, units of local govern-
36 ment, Indian tribal governments, and other public entities in fur-
37 therance of the purposes of this section.

38 (E) MAXIMUM GRANT AMOUNT.—The portion of the costs of
39 hiring firefighters provided by a grant under this paragraph may
40 not exceed—

41 (i) 75 percent in the 1st year of the grant;

1 (ii) 75 percent in the 2d year of the grant; and

2 (iii) 35 percent in the 3d year of the grant.

3 (F) VOLUNTEER ACTIVITIES ALLOWED.—Notwithstanding an-
4 other law, a firefighter hired with funds provided under this sub-
5 section shall not be discriminated against for, or be prohibited
6 from, engaging in volunteer activities in another jurisdiction dur-
7 ing off-duty hours.

8 (G) AWARD ON COMPETITIVE BASIS.—All grants made pursuant
9 to this subsection shall be awarded on a competitive basis through
10 a neutral peer review process.

11 (H) SET ASIDE FOR DEPARTMENT WITH A MAJORITY OF VOL-
12 UNTEER OR ALL-VOLUNTEER PERSONNEL.—At the beginning of
13 the fiscal year, the Administrator of FEMA shall set aside 10 per-
14 cent of the funds appropriated for carrying out this paragraph for
15 departments with majority volunteer or all-volunteer personnel.
16 After awards have been made, if less than 10 percent of the funds
17 appropriated for carrying out this paragraph are not awarded to
18 departments with a majority of volunteer or all-volunteer per-
19 sonnel, the Administrator of FEMA shall transfer from funds ap-
20 propriated for carrying out this paragraph to funds available for
21 carrying out paragraph (2) an amount equal to the difference be-
22 tween the amount that is provided to the fire departments and 10
23 percent.

24 (2) RECRUITMENT AND RETENTION GRANTS.—In addition to
25 amounts transferred under paragraph (1)(H), the Administrator of
26 FEMA shall direct at least 10 percent of the total amount of funds
27 appropriated pursuant to this section annually to a competitive grant
28 program for the recruitment and retention of volunteer firefighters who
29 are involved with or trained in the operations of firefighting and emer-
30 gency response. Eligible entities shall include volunteer or combination
31 fire departments, and national, State, local, or tribal organizations that
32 represent the interests of volunteer firefighters.

33 (c) APPLICATIONS.—

34 (1) APPROVED APPLICATION REQUIRED.—No grant may be made
35 under this section unless an application has been submitted to, and ap-
36 proved by, the Administrator of FEMA.

37 (2) REQUIRED FORM AND INFORMATION.—An application for a
38 grant under this section shall be submitted in such form, and contain
39 such information, as the Administrator of FEMA may prescribe.

40 (3) CONTENTS.—At a minimum, each application for a grant under
41 this section shall—

1 (A) explain the applicant's inability to address the need without
2 Federal assistance;

3 (B) in the case of a grant under subsection (b)(1), explain how
4 the applicant plans to meet the requirements of subsection
5 (b)(1)(F);

6 (C) specify long-term plans for retaining firefighters following
7 the conclusion of Federal support provided under this section; and

8 (D) provide assurances that the applicant will, to the extent
9 practicable, seek, recruit, and hire members of racial and ethnic
10 minority groups and women in order to increase their ranks within
11 firefighting.

12 (d) REQUIREMENTS AND ALLOWANCES FOR USE OF FUNDS.—

13 (1) FUNDS DO NOT SUPPLANT OTHER FUNDS.—Funds made avail-
14 able under this section to fire departments for salaries and benefits to
15 hire new, additional firefighters shall not be used to supplant State or
16 local funds, or, in the case of Indian tribal governments, funds supplied
17 by the Bureau of Indian Affairs, but shall be used to increase the
18 amount of funds that would, in the absence of Federal funds received
19 under this section, be made available from State or local sources, or
20 in the case of Indian tribal governments, from funds supplied by the
21 Bureau of Indian Affairs.

22 (2) MINIMUM REQUIRED BUDGET OF RECIPIENT FOR FIRE-RELATED
23 PROGRAMS AND EMERGENCY RESPONSE.—No grant shall be awarded
24 pursuant to this section to a municipality or other recipient whose an-
25 nual budget at the time of the application for fire-related programs and
26 emergency response has been reduced below 80 percent of the average
27 funding level in the 3 years prior to the date of the application for the
28 grant.

29 (3) USE FOR NON-FEDERAL SHARE OF COST OF PROGRAMS OR
30 PROJECTS.—Funds appropriated by Congress for the activities of an
31 agency of an Indian tribal government or the Bureau of Indian Affairs
32 performing firefighting functions on Indian lands may be used to pro-
33 vide the non-Federal share of the cost of programs or projects funded
34 under this section.

35 (4) MAXIMUM PROVIDED FOR HIRING FIREFIGHTERS.—The amount
36 of funding provided under this section to a recipient fire department
37 for hiring a firefighter in a fiscal year may not exceed—

38 (A) in the 1st year of the grant, 75 percent of the usual annual
39 cost of a 1st-year firefighter in that department at the time the
40 grant application was submitted;

1 (B) in the 2d year of the grant, 75 percent of the usual annual
2 cost of a 1st-year firefighter in that department at the time the
3 grant application was submitted; and

4 (C) in the 3d year of the grant, 35 percent of the usual annual
5 cost of a 1st-year firefighter in that department at the time the
6 grant application was submitted.

7 (e) WAIVERS.—

8 (1) IN GENERAL.—In a case of demonstrated economic hardship, the
9 Administrator of FEMA may—

10 (A) waive the requirements of subsection (d)(1); or

11 (B) waive or reduce the requirements in subsection (b)(1)(E) or
12 paragraph (2) or (4) of subsection (d).

13 (2) GUIDELINES.—

14 (A) DEVELOPMENT AND PUBLICATION.—The Administrator of
15 FEMA shall develop and publish guidelines for determining what
16 constitutes economic hardship for purposes of paragraph (1).

17 (B) CONSULTATION.—In developing guidelines under subpara-
18 graph (A), the Administrator of FEMA shall consult with individ-
19 uals who are—

20 (i) recognized for expertise in firefighting, emergency med-
21 ical services provided by fire services, or the economic affairs
22 of State and local governments; and

23 (ii) members of national fire service organizations or na-
24 tional organizations representing the interests of State and
25 local governments.

26 (C) CONSIDERATIONS.—In developing guidelines under subpara-
27 graph (A), the Administrator of FEMA shall consider, with re-
28 spect to relevant communities, the following:

29 (i) Changes in rates of unemployment from previous years.

30 (ii) Whether the rates of unemployment of the relevant
31 communities are currently exceeding, and have consistently
32 exceeded, the annual national average rates of unemployment.

33 (iii) Changes in percentages of individuals eligible to receive
34 food stamps from previous years.

35 (iv) Such other factors as the Administrator of FEMA con-
36 siders appropriate.

37 (f) PERFORMANCE EVALUATION.—

38 (1) ESTABLISHMENT.—The Administrator of FEMA shall establish
39 a performance assessment system, including quantifiable performance
40 metrics, to evaluate the extent to which grants awarded under this sec-
41 tion are furthering the purposes of this section.

1 (2) SUBMITTAL OF INFORMATION.—The Administrator of FEMA
2 may require a grant recipient to submit any information the Adminis-
3 trator of FEMA considers reasonably necessary to evaluate the pro-
4 gram.

5 (g) REVOCATION OR SUSPENSION OF FUNDING.—If the Administrator of
6 FEMA determines that a grant recipient under this section is not in sub-
7 stantial compliance with the terms and requirements of an approved grant
8 application submitted under this section, the Administrator of FEMA may
9 revoke or suspend funding of that grant, in whole or in part.

10 (h) ACCESS TO DOCUMENTS.—

11 (1) ADMINISTRATOR OF FEMA.—The Administrator of FEMA shall
12 have access for the purpose of audit and examination to any pertinent
13 books, documents, papers, or records of a grant recipient under this
14 section and to the pertinent books, documents, papers, or records of
15 State and local governments, persons, businesses, and other entities
16 that are involved in programs, projects, or activities for which assist-
17 ance is provided under this section.

18 (2) COMPTROLLER GENERAL.—Paragraph (1) shall apply with re-
19 spect to audits and examinations conducted by the Comptroller General
20 or by an authorized representative of the Comptroller General.

21 (i) AUTHORIZATION OF APPROPRIATIONS.—

22 (1) IN GENERAL.—There is authorized to be appropriated for the
23 purposes of carrying out this section for fiscal year 2023 an amount
24 equal to the amount authorized for the previous fiscal year increased
25 by the percentage by which—

26 (A) the Consumer Price Index (all items, United States city av-
27 erage) for the previous fiscal year, exceeds

28 (B) the Consumer Price Index for the fiscal year preceding the
29 fiscal year described in subparagraph (A).

30 (2) ADMINISTRATIVE EXPENSES.—Of the amounts appropriated pur-
31 suant to paragraph (1) for a fiscal year, the Administrator of FEMA
32 may use not more than 5 percent of the amounts for salaries and ex-
33 penses and other administrative costs incurred by the Administrator of
34 FEMA to make grants and provide assistance under this section.

35 (3) CONGRESSIONALLY DIRECTED SPENDING NOT ALLOWED.—Con-
36 sistent with the requirement in subsection (a) that grants under this
37 section be awarded on a competitive basis, none of the funds appro-
38 priated pursuant to this subsection may be used for a congressionally
39 direct spending item (as defined under the rules of the Senate and the
40 House of Representatives).

1 (j) SUNSET OF AUTHORITIES.—The authority to award assistance and
2 grants under this section shall expire on September 30, 2024.

3 **§ 11379. Training for administration, and oversight and**
4 **monitoring, of grants programs**

5 (a) TRAINING ON ADMINISTRATION OF FIRE GRANT PROGRAMS.—

6 (1) DEVELOPMENT OF TRAINING COURSE.—The Administrator of
7 FEMA, acting through the Administrator, may develop and make wide-
8 ly available an electronic, online training course for members of the fire
9 and emergency response community on matters relating to the adminis-
10 tration of grants under sections 11377 and 11378 of this title.

11 (2) REQUIREMENTS.—The Administrator of FEMA shall ensure that
12 training developed and made available under paragraph (1) is—

13 (A) tailored to the financial and time constraints of members
14 of the fire and emergency response community; and

15 (B) accessible to all individuals in the career, combination, paid-
16 on-call, and volunteer fire and emergency response community.

17 (b) GRANT MONITORING AND OVERSIGHT FRAMEWORK.—

18 (1) FRAMEWORK.—The Administrator of FEMA shall develop and
19 implement a grant monitoring and oversight framework to mitigate and
20 minimize risks of fraud, waste, abuse, and mismanagement relating to
21 the grants programs under sections 11377 and 11378 of this title.

22 (2) ELEMENTS.—The framework required under paragraph (1) shall
23 include the following:

24 (A) Developing standardized guidance and training for all par-
25 ticipants in the grant programs described in paragraph (1).

26 (B) Conducting regular risk assessments.

27 (C) Conducting desk reviews and site visits.

28 (D) Enforcement actions to recoup potential questionable costs
29 of grant recipients.

30 (E) Such other oversight and monitoring tools as the Adminis-
31 trator of FEMA considers necessary to mitigate and minimize
32 fraud, waste, abuse, and mismanagement relating to the grant
33 programs described in paragraph (1).

34 **§ 11380. Surplus and excess Federal equipment**

35 The Administrator shall make publicly available, including through the
36 Internet, information on procedures for acquiring surplus and excess equip-
37 ment or property that may be useful to State and local fire, emergency, and
38 hazardous material handling service providers.

39 **§ 11381. Cooperative agreements with Federal facilities**

40 The Administrator shall make publicly available, including through the
41 Internet, information on procedures for establishing cooperative agreements

1 between State and local fire and emergency services and Federal facilities
2 in their region relating to the provision of fire and emergency services.

3 **§ 11382. Burn research**

4 (a) OFFICE.—The Administrator of FEMA shall establish an office in the
5 Federal Emergency Management Agency to establish specific criteria of
6 grant recipients and to administer grants under this section.

7 (b) SAFETY ORGANIZATION GRANTS.—The Administrator of FEMA may
8 make grants, on a competitive basis, to safety organizations that have expe-
9 rience in conducting burn safety programs for the purpose of assisting those
10 organizations in conducting burn prevention programs or augmenting exist-
11 ing burn prevention programs.

12 (c) HOSPITAL GRANTS.—The Administrator of FEMA may make grants,
13 on a competitive basis, to hospitals that serve as regional burn centers to
14 conduct acute burn care research.

15 (d) OTHER GRANTS.—The Administrator of FEMA may make grants, on
16 a competitive basis, to governmental and nongovernmental entities to pro-
17 vide after-burn treatment and counseling to individuals that are burn vic-
18 tims.

19 **§ 11383. Removal of civil liability barriers that discourage**
20 **the donation of fire equipment to volunteer fire**
21 **companies**

22 (a) DEFINITIONS.—In this section:

23 (1) AUTHORIZED TECHNICIAN.—The term “authorized technician”
24 means a technician who has been certified by the manufacturer of fire
25 control or fire rescue equipment to inspect the equipment. The author-
26 ized technician need not be employed by the State or local agency ad-
27 ministering the distribution of the fire control or fire rescue equipment.

28 (2) FIRE CONTROL OR RESCUE EQUIPMENT.—The term “fire control
29 or fire rescue equipment” includes any fire vehicle, firefighting tool,
30 communications equipment, protective gear, fire hose, or breathing ap-
31 paratus.

32 (3) PERSON.—The term “person” includes a governmental or other
33 entity.

34 (4) QUALIFIED FIRE CONTROL OR RESCUE EQUIPMENT.—The term
35 “qualified fire control or rescue equipment” means fire control or fire
36 rescue equipment that has been recertified by an authorized technician
37 as meeting the manufacturer’s specifications.

38 (5) STATE.—The term “State” includes the States, the District of
39 Columbia, Puerto Rico, the Northern Mariana Islands, American
40 Samoa, Guam, the Virgin Islands, any other territory (including a pos-

1 session) of the United States, and a political subdivision of a State or
2 territory.

3 (6) VOLUNTEER FIRE COMPANY.—The term “volunteer fire com-
4 pany” means an association of individuals who provide fire protection
5 and other emergency services, where at least 30 percent of the individ-
6 uals receive little or no compensation compared with an entry level full-
7 time paid individual in that association or in the nearest association
8 with an entry level full-time paid individual.

9 (b) LIABILITY PROTECTION.—A person that donates qualified fire control
10 or rescue equipment to a volunteer fire company shall not be liable for civil
11 damages under any State or Federal law for personal injuries, property
12 damage or loss, or death caused by the equipment after the donation.

13 (c) EXCEPTIONS.—Subsection (b) does not apply to a person if—

14 (1) the person’s act or omission causing the injury, damage, loss, or
15 death constitutes gross negligence or intentional misconduct;

16 (2) the person is the manufacturer of the qualified fire control or
17 rescue equipment; or

18 (3) the person or agency modified or altered the equipment after it
19 had been recertified by an authorized technician as meeting the manu-
20 facturer’s specifications.

21 (d) PREEMPTION.—This section—

22 (1) preempts the laws of a State to the extent that the laws are in-
23 consistent with this section; except that

24 (2) notwithstanding subsection (c) shall not preempt a State law that
25 provides additional protection from liability for a person that donates
26 fire control or fire rescue equipment to a volunteer fire company.

27 **§ 11384. Encouraging adoption of standards for firefighter**
28 **health and safety**

29 The Administrator shall promote adoption by fire services of national vol-
30 untary consensus standards for firefighter health and safety, including
31 standards for firefighter operations, training, staffing, and fitness, by—

32 (1) educating fire services about the standards;

33 (2) encouraging the adoption of the standards at all levels of govern-
34 ment; and

35 (3) making recommendations on other ways in which the Federal
36 Government can promote the adoption of the standards by fire services.

37 **§ 11385. Investigation authorities**

38 (a) DEFINITION OF MAJOR FIRE.—For purposes of this section, the term
39 “major fire” has the meaning given the term under regulations to be issued
40 by the Administrator.

1 (b) FIRE SAFETY INVESTIGATION OF MAJOR FIRE.—In the case of a
2 major fire, the Administrator may send incident investigators, which may
3 include safety specialists, fire protection engineers, codes and standards ex-
4 perts, researchers, and fire training specialists, to the site of the fire to con-
5 duct a fire safety investigation as described in subsection (c).

6 (c) REQUIREMENTS OF INVESTIGATION.—A fire safety investigation con-
7 ducted under this section—

8 (1) shall be conducted in coordination and cooperation with appro-
9 priate Federal, State, local, Tribal, and territorial authorities, including
10 Federal agencies that are authorized to investigate any fire; and

11 (2) shall examine the previously determined cause and origin of the
12 fire and assess broader systematic matters to include use of codes and
13 standards, demographics, structural characteristics, smoke and fire dy-
14 namics (movement) during the event, and costs of associated injuries
15 and deaths.

16 (d) REPORT.—

17 (1) IN GENERAL.—Subject to paragraph (2), on concluding a fire
18 safety investigation under this section, the Administrator shall—

19 (A) issue a public report to the appropriate Federal, State,
20 local, Tribal, and territorial authorities on the findings of the in-
21 vestigation; or

22 (B) collaborate with another investigating Federal, State, local,
23 Tribal, or territorial agency on the report of that agency.

24 (2) CONTENTS.—Each public report issued under paragraph (1)
25 shall include recommendations on—

26 (A) any other buildings with similar characteristics that may
27 bear similar fire risks;

28 (B) improving tactical response to similar fires;

29 (C) improving civilian safety practices;

30 (D) assessing the costs and benefits to the community of adding
31 fire safety features; and

32 (E) how to mitigate the causes of the fire.

33 (3) EXCEPTION.—If the Administrator, in consultation with appro-
34 priate Federal, State, local, Tribal, and territorial authorities, deter-
35 mines that issuing a report under paragraph (1) would have a negative
36 impact on a potential or ongoing criminal investigation, the Adminis-
37 trator is not required to issue the report.

38 (e) ADDITIONAL FIRE SAFETY INVESTIGATION.—In addition to a fire
39 safety investigation conducted pursuant to subsection (b), provided doing so
40 would not have a negative impact on a potential or ongoing criminal inves-
41 tigation, the Administrator may send fire investigators to conduct a fire

1 safety investigation at the site of any fire with unusual or remarkable con-
2 text that results in losses less severe than those occurring as a result of a
3 major fire, in coordination and cooperation with the appropriate Federal,
4 State, local, Tribal, and territorial authorities, including Federal agencies
5 that are authorized to investigate the fire.

6 (f) CONSTRUCTION.—Nothing in this section shall be construed to—

7 (1) affect or otherwise diminish the authorities or the mandates vest-
8 ed in other Federal agencies;

9 (2) grant the Administrator authority to investigate a major fire for
10 the purpose of an enforcement action or criminal prosecution; or

11 (3) require the Administrator to send investigators or issue a report
12 for a major fire when the Administrator, in coordination and coopera-
13 tion with the appropriate Federal, State, local, Tribal, and territorial
14 authorities, determines that it may compromise a potential or ongoing
15 criminal investigation.

16 § 11386. Administrative provisions

17 (a) ASSISTANCE TO ADMINISTRATOR.—Each department, agency, and in-
18 strumentality of the executive branch of the Federal Government and each
19 independent regulatory agency of the United States shall furnish to the Ad-
20 ministrator, on request, on a reimbursable basis or otherwise, such assist-
21 ance as the Administrator considers necessary to carry out the Administra-
22 tor's functions and duties pursuant to this subchapter, including transfer
23 of personnel with their consent and without prejudice to their position and
24 ratings.

25 (b) POWERS OF ADMINISTRATOR.—With respect to this subchapter, the
26 Administrator may—

27 (1) enter into, without regard to section 6101 of title 41, such con-
28 tracts, grants, leases, cooperative agreements, or other transactions as
29 may be necessary to carry out this subchapter;

30 (2) accept gifts and voluntary and uncompensated services, notwith-
31 standing section 1342 of title 31;

32 (3) purchase, lease, or otherwise acquire, own, hold, improve, use, or
33 deal in and with any property (real, personal, or mixed, tangible or in-
34 tangible), or interest in property, wherever situated, and sell, convey,
35 mortgage, pledge, lease, exchange, or otherwise dispose of property and
36 assets;

37 (4) procure temporary and intermittent services to the same extent
38 as is authorized under section 3109 of title 5, but at rates not to ex-
39 ceed the daily equivalent of the maximum annual rate of basic pay then
40 in effect for grade GS-15 of the General Schedule (5 U.S.C. 5332(a))
41 for qualified experts; and

1 (5) establish such rules, regulations, and procedures as are necessary
2 to carry out this subchapter.

3 (c) AUDIT.—The Administrator of FEMA and the Comptroller Genera,
4 or any of their duly authorized representatives, shall have access to any
5 books, documents, papers, and records of the recipients of contracts, grants,
6 or other forms of assistance that are pertinent to its activities under this
7 subchapter for the purpose of audit or to determine if a proposed activity
8 is in the public interest.

9 (d) INVENTIONS AND DISCOVERIES.—All property rights with respect to
10 inventions and discoveries, which are made in the course of or under con-
11 tract with a government agency pursuant to this subchapter, shall be sub-
12 ject to the basic policies set forth in the President’s Statement of Govern-
13 ment Patent Policy issued August 23, 1971, or such revisions of that state-
14 ment of the policy as may subsequently be promulgated and published in
15 the Federal Register.

16 (e) COORDINATION.—

17 (1) USE OF EXISTING RESOURCES.—To the extent practicable, the
18 Administrator shall use existing programs, data, information, and fa-
19 cilities already available in other Federal Government departments and
20 agencies and, where appropriate, existing research organizations, cen-
21 ters, and universities.

22 (2) COORDINATION OF FIRE PREVENTION AND CONTROL PRO-
23 GRAMS.—The Administrator shall provide liaison at an appropriate or-
24 ganizational level to ensure coordination of the activities of the Admin-
25 istrator with Federal, State, and local government agencies and depart-
26 ments and nongovernmental organizations concerned with any matter
27 relating to programs of fire prevention and control.

28 (3) COORDINATION OF EMERGENCY MEDICAL SERVICES PRO-
29 GRAMS.—The Administrator shall provide liaison at an appropriate or-
30 ganizational level to ensure coordination of the activities of the Admin-
31 istrator relating to emergency medical services provided by fire service-
32 based systems with Federal, State, and local government agencies and
33 departments and nongovernmental organizations so concerned, as well
34 as those entities concerned with emergency medical services generally.

35 (f) ENHANCEMENT OF SCIENCE AND MATHEMATICS PROGRAMS.—

36 (1) DEFINITIONS.—In this section:

37 (A) EDUCATIONALLY USEFUL FEDERAL EQUIPMENT.—The
38 term “educationally useful Federal equipment” means computers
39 and related peripheral tools and research equipment that is appro-
40 priate for use in schools.

1 (B) SCHOOL.—The term “school” means a public or private
2 educational institution that serves any of the grades of kinder-
3 garten through grade 12.

4 (2) REPORTS.—Not later than 1 year after November 20, 1997, and
5 annually thereafter, the Administrator shall prepare and submit to the
6 President a report that describes donations of educationally useful Fed-
7 eral equipment to schools to enhance the science and mathematics pro-
8 grams of those schools made during the period covered by the report.
9 The President shall submit the report to Congress at the same time
10 as the President submits a budget request to Congress under section
11 1105(a) of title 31.

12 **§ 11387. Reports to Congress and the President**

13 The Administrator of FEMA shall report to Congress and the President
14 not later than 90 calendar days following the year ending September 30,
15 1980, and similarly each year thereafter on all activities relating to fire pre-
16 vention and control, and all measures taken to implement and carry out this
17 subchapter during the preceding calendar year. The report shall include—

18 (1) a thorough appraisal, including statistical analysis, estimates,
19 and long-term projections of the human and economic losses due to
20 fire;

21 (2) a survey and summary, in such detail as is considered advisable,
22 of the research and technology program undertaken or sponsored pur-
23 suant to this subchapter;

24 (3) a summary of the activities of the Academy for the preceding 12
25 months, including—

26 (A) an explanation of the curriculum of study;

27 (B) a description of the standards of admission and perform-
28 ance;

29 (C) the criteria for the awarding of degrees and certificates; and

30 (D) a statistical compilation of the number of students attend-
31 ing the Academy and receiving degrees or certificates;

32 (4) a summary of the activities undertaken to assist the Nation’s fire
33 services;

34 (5) a summary of the public education programs undertaken;

35 (6) an analysis of the extent of participation in preparing and sub-
36 mitting Fire Safety Effectiveness Statements;

37 (7) a summary of outstanding problems confronting the administra-
38 tion of this subchapter, in order of priority;

39 (8) such recommendations for additional legislation as are considered
40 necessary or appropriate; and

1 (9) a summary of reviews, evaluations, and suggested improvements
2 in State and local fire prevention and building codes, fire services, and
3 relevant Federal or private codes, regulations, and fire services.

4 **§ 11388. Authorization of appropriations**

5 (a) IN GENERAL.—Except as otherwise specifically provided with respect
6 to the payment of claims under section 11360 of this title, there is author-
7 ized to be appropriated to carry out the purposes of this subchapter
8 \$76,490,890 for fiscal year 2023, of which \$2,753,672 shall be used to
9 carry out section 11357(f) of this title.

10 (b) NATIONAL EMERGENCY TRAINING CENTER SITE ADMINISTRATION.—
11 Of the amounts referred to in subsection (a), not more than \$4,150,000 is
12 authorized to be appropriated for each fiscal year for National Emergency
13 Training Center site administration.

14 **Subchapter III—Global catastrophic risk**
15 **management**

16 **§ 11401. Definitions.—**

17 In this subchapter:

18 (1) ADMINISTRATOR.—The term “Administrator” means the Admin-
19 istrator of the Federal Emergency Management Agency.

20 (2) BASIC NEED.—The term “basic need”—

21 (A) means any good, service, or activity necessary to protect the
22 health, safety, and general welfare of the civilian population of the
23 United States; and

24 (B) includes—

25 (i) food;

26 (ii) water;

27 (iii) shelter;

28 (iv) basic communication services;

29 (v) basic sanitation and health services; and

30 (vi) public safety.

31 (3) CATASTROPHIC INCIDENT.—The term “catastrophic incident”—

32 (A) means any natural or man-made disaster that results in ex-
33 traordinary levels of casualties or damage, mass evacuations, or
34 disruption severely affecting the population, infrastructure, envi-
35 ronment, economy, national morale, or government functions in an
36 area; and

37 (B) may include an incident—

38 (i) with a sustained national impact over a prolonged pe-
39 riod of time;

1 (ii) that may rapidly exceed resources available to State
2 and local government and private sector authorities in the im-
3 pacted area; or

4 (iii) that may significantly interrupt governmental oper-
5 ations and emergency services to such an extent that national
6 security could be threatened.

7 (4) CRITICAL INFRASTRUCTURE.—The term “critical infrastructure”
8 has the meaning given such term in section 1016(e) of the Critical In-
9 frastructures Protection Act of 2001 (42 U.S.C. 5195c(e)).

10 (5) EXISTENTIAL RISK.—The term “existential risk” means the po-
11 tential for an outcome that would result in human extinction.

12 (6) GLOBAL CATASTROPHIC RISK.—The term “global catastrophic
13 risk” means the risk of events or incidents consequential enough to sig-
14 nificantly harm or set back human civilization at the global scale.

15 (7) GLOBAL CATASTROPHIC AND EXISTENTIAL THREATS.—The term
16 “global catastrophic and existential threats” means threats that with
17 varying likelihood may produce consequences severe enough to result in
18 systemic failure or destruction of critical infrastructure or significant
19 harm to human civilization. Examples of global catastrophic and exist-
20 tential threats include severe global pandemics, nuclear war, asteroid
21 and comet impacts, supervolcanoes, sudden and severe changes to the
22 climate, and intentional or accidental threats arising from the use and
23 development of emerging technologies.

24 (8) INDIAN TRIBAL GOVERNMENT.—The term “Indian Tribal govern-
25 ment” has the meaning given the term “Indian tribal government”
26 in section 102 of the Robert T. Stafford Disaster Relief and Emergency
27 Assistance Act (42 U.S.C. 5122).

28 (9) LOCAL GOVERNMENT.—The term “local government” has the
29 meaning given the term in section 102 of the Robert T. Stafford Dis-
30 aster Relief and Emergency Assistance Act (42 U.S.C. 5122).

31 (10) NATIONAL EXERCISE PROGRAM.—The term “national exercise
32 program” means activities carried out to test and evaluate the national
33 preparedness goal and related plans and strategies as described
34 in section 20508(b) of this title.

35 (11) STATE.—The term “State” has the meaning given the term in
36 section 102 of the Robert T. Stafford Disaster Relief and Emergency
37 Assistance Act (42 U.S.C. 5122)

38 **§ 11402. Assessment of global catastrophic risk**

39 (a) IN GENERAL.—The Secretary and the Administrator shall coordinate
40 an assessment of global catastrophic risk.

1 (b) COORDINATION.—When coordinating the assessment under subsection
2 (a), the Secretary and the Administrator shall coordinate with senior des-
3 ignees of—

4 (1) the Assistant to the President for National Security Affairs;

5 (2) the Director of the Office of Science and Technology Policy;

6 (3) the Secretary of State and the Under Secretary of State for
7 Arms Control and International Security;

8 (4) the Attorney General and the Director of the Federal Bureau of
9 Investigation;

10 (5) the Secretary of Energy, the Under Secretary of Energy for Nu-
11 clear Security, and the Director of Science;

12 (6) the Secretary of Health and Human Services, the Assistant Sec-
13 retary for Preparedness and Response, and the Assistant Secretary of
14 Global Affairs;

15 (7) the Secretary of Commerce, the Under Secretary of Commerce
16 for Oceans and Atmosphere, and the Under Secretary of Commerce for
17 Standards and Technology;

18 (8) the Secretary of the Interior and the Director of the United
19 States Geological Survey;

20 (9) the Administrator of the Environmental Protection Agency and
21 the Assistant Administrator for Water;

22 (10) the Administrator of the National Aeronautics and Space Ad-
23 ministration;

24 (11) the Director of the National Science Foundation;

25 (12) the Secretary of the Treasury;

26 (13) the Secretary of Defense, the Assistant Secretary of the Army
27 for Civil Works, and the Chief of Engineers and Commanding General
28 of the Army Corps of Engineers;

29 (14) the Chairman of the Joint Chiefs of Staff;

30 (15) the Administrator of the United States Agency for International
31 Development;

32 (16) the Secretary of Transportation; and

33 (17) other stakeholders the Secretary and the Administrator deter-
34 mine appropriate.

35 **§ 11403. Report**

36 (a) IN GENERAL.—Not later than December 23, 2023, and every 10
37 years thereafter, the Secretary, in coordination with the Administrator, shall
38 submit to the Committee on Homeland Security and Governmental Affairs
39 and the Committee on Armed Services of the Senate and the Committee on
40 Transportation and Infrastructure and the Committee on Armed Services
41 of the House of Representatives a report containing a detailed assessment,

1 based on the input and coordination required undersection 10742 of this
2 title, of global catastrophic and existential risk.

3 (b) MATTERS COVERED.—Each report required under subsection (a) shall
4 include—

5 (1) expert estimates of cumulative global catastrophic and existential
6 risk in the next 30 years, including separate estimates for the likeli-
7 hood of occurrence and potential consequences;

8 (2) expert-informed analyses of the risk of the most concerning spe-
9 cific global catastrophic and existential threats, including separate esti-
10 mates, where reasonably feasible and credible, of each threat for its
11 likelihood of occurrence and its potential consequences, as well as asso-
12 ciated uncertainties;

13 (3) a comprehensive list of potential catastrophic or existential
14 threats, including even those that may have very low likelihood;

15 (4) technical assessments and lay explanations of the analyzed global
16 catastrophic and existential risks, including their qualitative character
17 and key factors affecting their likelihood of occurrence and potential
18 consequences;

19 (5) an explanation of any factors that limit the ability of the Sec-
20 retary to assess the risk both cumulatively and for particular threats,
21 and how those limitations may be overcome through future research or
22 with additional resources, programs, or authorities;

23 (6) a forecast of if and why global catastrophic and existential risk
24 is likely to increase or decrease significantly in the next 10 years, both
25 qualitatively and quantitatively, as well as a description of associated
26 uncertainties;

27 (7) proposals for how the Federal Government may more adequately
28 assess global catastrophic and existential risk on an ongoing basis in
29 future years;

30 (8) recommendations for legislative actions, as appropriate, to sup-
31 port the evaluation and assessment of global catastrophic and existen-
32 tial risk; and

33 (9) other matters considered appropriate by the Secretary, in coordi-
34 nation with the Administrator, and based on the input and coordination
35 required undersection 11402 of this title.

36 (c) CONSULTATION REQUIREMENT.—In producing the report required
37 under subsection (a), the Secretary shall—

38 (1) regularly consult with experts on severe global pandemics, nu-
39 clear war, asteroid and comet impacts, supervolcanoes, sudden and se-
40 vere changes to the climate, and intentional or accidental threats aris-
41 ing from the use and development of emerging technologies; and

1 (2) share information gained through the consultation required
2 under paragraph (1) with relevant Federal partners listed in section
3 11402(b) of this title.

4 11404. Enhanced catastrophic incident annex

5 (a) IN GENERAL.—The Secretary, in coordination with the Administrator
6 and the Federal partners listed in section 11402(b) of this title, shall supple-
7 ment each Federal Interagency Operational Plan to include an annex con-
8 taining a strategy to ensure the health, safety, and general welfare of the
9 civilian population affected by catastrophic incidents by—

10 (1) providing for the basic needs of the civilian population of the
11 United States that is impacted by catastrophic incidents in the United
12 States;

13 (2) coordinating response efforts with State, local, and Indian Tribal
14 governments, the private sector, and nonprofit relief organizations;

15 (3) promoting personal and local readiness and non-reliance on gov-
16 ernment relief during periods of heightened tension or after cata-
17 strophic incidents; and

18 (4) developing international partnerships with allied nations for the
19 provision of relief services and goods.

20 (b) ELEMENTS OF STRATEGY.—The strategy required under subsection
21 (a) shall include a description of—

22 (1) actions the Federal Government should take to ensure the basic
23 needs of the civilian population of the United States in a catastrophic
24 incident are met;

25 (2) how the Federal Government should coordinate with non-Federal
26 entities to multiply resources and enhance relief capabilities, includ-
27 ing—

28 (A) State and local governments;

29 (B) Indian Tribal governments;

30 (C) State disaster relief agencies;

31 (D) State and local disaster relief managers;

32 (E) State National Guards;

33 (F) law enforcement and first response entities; and

34 (G) nonprofit relief services;

35 (3) actions the Federal Government should take to enhance indi-
36 vidual resiliency to the effects of a catastrophic incident, which actions
37 shall include—

38 (A) readiness alerts to the public during periods of elevated
39 threat;

40 (B) efforts to enhance domestic supply and availability of crit-
41 ical goods and basic necessities; and

1 (C) information campaigns to ensure the public is aware of re-
2 sponse plans and services that will be activated when necessary;

3 (4) efforts the Federal Government should undertake and agree-
4 ments the Federal Government should seek with international allies to
5 enhance the readiness of the United States to provide for the general
6 welfare;

7 (5) how the strategy will be implemented should multiple levels of
8 critical infrastructure be destroyed or taken offline entirely for an ex-
9 tended period of time; and

10 (6) the authorities the Federal Government should implicate in re-
11 sponding to a catastrophic incident.

12 (e) ASSUMPTIONS.—In designing the strategy under subsection (a), the
13 Secretary, in coordination with the Administrator and the Federal partners
14 listed in section 11402(b) of this title, shall account for certain factors to
15 make the strategy operationally viable, including the assumption that—

16 (1) multiple levels of critical infrastructure have been taken offline
17 or destroyed by catastrophic incidents or the effects of catastrophic in-
18 cidents;

19 (2) impacted sectors may include—

20 (A) the transportation sector;

21 (B) the communication sector;

22 (C) the energy sector;

23 (D) the healthcare and public health sector; and

24 (E) the water and wastewater sector;

25 (3) State, local, Indian Tribal, and territorial governments have been
26 equally affected or made largely inoperable by catastrophic incidents or
27 the effects of catastrophic incidents;

28 (4) the emergency has exceeded the response capabilities of State,
29 local, and Indian Tribal governments under the Robert T. Stafford Dis-
30 aster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.)
31 and other relevant disaster response laws; and

32 (5) the United States military is sufficiently engaged in armed or
33 cyber conflict with State or non-State adversaries, or is otherwise un-
34 able to augment domestic response capabilities in a significant manner
35 due to a catastrophic incident.(.)

36 **§ 11405. Rules of construction**

37 (a) ADMINISTRATOR.—Nothing in this subchapter shall be construed to
38 supersede the civilian emergency management authority of the Adminis-
39 trator under the Robert T. Stafford Disaster Relief and Emergency Assist-
40 ance Act (42 U.S.C. 5121 et seq.) or subtitle II (except section 20525) of
41 this title.

1 (b) SECRETARY.—Nothing in this subchapter shall be construed as pro-
 2 viding new authority to the Secretary, except to coordinate and facilitate the
 3 development of the assessments and reports required pursuant to this sub-
 4 chapter.

5 **Chapter 115—Transportation Security** 6 **Administration**

Subchapter I—General

Sec.

- 11501. Functions.
- 11502. National emergency responsibilities.
- 11503. Management of security information.
- 11504. View of National Transportation Safety Board.
- 11505. Acquisitions.
- 11506. Transfers of funds.
- 11507. Regulations.
- 11508. Personnel and services.
- 11509. Personnel management system.
- 11510. Authority of Inspector General.
- 11511. Law enforcement powers.
- 11512. Authority to exempt.
- 11513. Nondisclosure of security activities.
- 11514. Transportation security strategic planning.
- 11515. Risk scenarios.
- 11516. Transportation Security Information Sharing Plan.
- 11517. Public area security.
- 11518. Best practices to secure against vehicle-based attacks.
- 11519. Enforcement of certain regulations and orders of the Secretary.
- 11520. Registered traveler fee.
- 11521. Enhanced security measures.
- 11522. Performance management system.
- 11523. Voluntary provision of emergency services.
- 11524. Disposition of unclaimed money and clothing.
- 11525. Transmittals to Congress.
- 11526. Transportation security preparedness plan for communicable disease outbreak.
- 11527. Airport security directives and emergency amendments.

Subchapter II—Acquisition Improvements

- 11541. Definitions.
- 11542. Technology investment plan.
- 11543. Acquisition justification and reports and certification.
- 11544. Baseline establishment and reports.
- 11545. Inventory utilization.
- 11546. Small business contracting goals.
- 11547. Consistency with Federal Acquisition Regulation and Department policies and direc-
 tives.
- 11548. Diversified security technology industry marketplace.
- 11549. Third party testing and verification of screening technology.
- 11550. Transportation Security Administration Systems Integration Facility.

Subchapter III—Maintenance of Security-Related Technology

- 11561. Preventive maintenance validation process for security-related technology deployed to
 airports.

7 **Subchapter I—General**

8 **§ 11501. Functions**

9 (a) FUNCTIONS.—The Administrator of the Transportation Security Ad-
 10 ministration (in this chapter referred to as the “Administrator”), is respon-
 11 sible for security in all modes of transportation, including—

- 12 (1) carrying out chapter 409 of this title and related research and
 13 development activities; and

1 (2) assuming security responsibilities over other modes of transpor-
2 tation that are exercised by the Department.

3 (b) SCREENING OPERATIONS.—The Administrator shall—

4 (1) be responsible for day-to-day Federal security screening oper-
5 ations for passenger air transportation and intrastate air transpor-
6 tation under sections 40911 and 40955 of this title;

7 (2) develop standards for the hiring and retention of security screen-
8 ing personnel;

9 (3) train and test security screening personnel; and

10 (4) be responsible for hiring and training personnel to provide secu-
11 rity screening at all airports in the United States where screening is
12 required under section 40911 of this title, in consultation with the Sec-
13 retary of Transportation and the heads of other appropriate Federal
14 agencies and departments.

15 (c) ADDITIONAL DUTIES AND POWERS.—In addition to carrying out the
16 functions specified in subsections (a) and (b), the Administrator shall—

17 (1) receive, assess, and distribute intelligence information related to
18 transportation security;

19 (2) assess threats to transportation;

20 (3) develop policies, strategies, and plans for dealing with threats to
21 transportation security;

22 (4) make other plans related to transportation security, including co-
23 ordinating countermeasures with appropriate departments, agencies,
24 and instrumentalities of the United States Government;

25 (5) serve as the primary liaison for transportation security to the in-
26 telligence and law enforcement communities;

27 (6) on a day-to-day basis, manage and provide operational guidance
28 to the field security resources of the Administration, including Federal
29 Security Directors as provided by section 40953 of this title;

30 (7) enforce security-related regulations and requirements;

31 (8) identify and undertake research and development activities nec-
32 essary to enhance transportation security;

33 (9) inspect, maintain, and test security facilities, equipment, and sys-
34 tems;

35 (10) ensure the adequacy of security measures for the transportation
36 of cargo;

37 (11) oversee the implementation, and ensure the adequacy, of secu-
38 rity measures at airports and other transportation facilities;

39 (12) require background checks for airport security screening per-
40 sonnel, individuals with access to secure areas of airports, and other
41 transportation security personnel;

1 (13) work in conjunction with the Administrator of the Federal Avia-
2 tion Administration with respect to actions or activities that may affect
3 aviation safety or air carrier operations;

4 (14) maintain a National Deployment Office as required under sec-
5 tion 10310(f) of this title;

6 (15) work with the International Civil Aviation Organization and ap-
7 propriate aeronautic authorities of foreign governments under section
8 40917 of this title, to address security concerns on passenger flights
9 by foreign air carriers in foreign air transportation; and

10 (16) carry out other duties, and exercise other powers, relating to
11 transportation security the Administrator considers appropriate, to the
12 extent authorized by law.

13 **§ 11502. National emergency responsibilities**

14 (a) IN GENERAL.—Subject to the direction and control of the Secretary,
15 the Administrator, during a national emergency, has the following respon-
16 sibilities:

17 (1) To coordinate domestic transportation, including aviation, rail,
18 and other surface transportation, and maritime transportation (includ-
19 ing port security).

20 (2) To coordinate and oversee the transportation-related responsibil-
21 ities of other departments and agencies of the Federal Government
22 other than the Department of Defense and the military departments.

23 (3) To coordinate and provide notice to other departments and agen-
24 cies of the Federal Government, and appropriate agencies of State and
25 local governments, including departments and agencies for transpor-
26 tation, law enforcement, and border control, about threats to transpor-
27 tation.

28 (4) To carry out other duties, and exercise other powers, relating to
29 transportation during a national emergency, that the Secretary shall
30 prescribe.

31 (b) AUTHORITY OF OTHER DEPARTMENTS AND AGENCIES.—The author-
32 ity of the Administrator under this section shall not supersede the authority
33 of another department or agency of the Federal Government under law with
34 respect to transportation or transportation-related matters, whether or not
35 during a national emergency.

36 (c) CIRCUMSTANCES.—The Secretary shall prescribe the circumstances
37 constituting a national emergency for purposes of this section.

38 **§ 11503. Management of security information**

39 In consultation with the Transportation Security Oversight Board, the
40 Administrator shall—

1 (1) enter into memoranda of understanding with Federal agencies or
2 other entities to share or otherwise cross-check, as necessary, data on
3 individuals identified on Federal agency databases who may pose a risk
4 to transportation or national security;

5 (2) establish procedures for notifying the Administrator of the Fed-
6 eral Aviation Administration, appropriate State and local law enforce-
7 ment officials, and airport or airline security officers of the identity of
8 individuals known to pose, or suspected of posing, a risk of air piracy
9 or terrorism or a threat to airline or passenger safety;

10 (3) in consultation with other appropriate Federal agencies and air
11 carriers, establish policies and procedures requiring air carriers—

12 (A) to use information from government agencies to identify in-
13 dividuals on passenger lists who may be a threat to civil aviation
14 or national security; and

15 (B) if such an individual is identified, to notify appropriate law
16 enforcement agencies, prevent the individual from boarding an air-
17 craft, or take other appropriate action with respect to that indi-
18 vidual; and

19 (4) consider requiring passenger air carriers to share passenger lists
20 with appropriate Federal agencies for the purpose of identifying indi-
21 viduals who may pose a threat to aviation safety or national security.

22 **§ 11504. View of National Transportation Safety Board**

23 In taking an action under this section that could affect safety, the Admin-
24 istrator shall give great weight to the timely views of the National Transpor-
25 tation Safety Board.

26 **§ 11505. Acquisitions**

27 (a) IN GENERAL.—The Administrator may—

28 (1) acquire (by purchase, lease, condemnation, or otherwise) real
29 property, or an interest in the property, in and outside the continental
30 United States, that the Administrator considers necessary;

31 (2) acquire (by purchase, lease, condemnation, or otherwise) and to
32 construct, repair, operate, and maintain personal property (including
33 office space and patents), or an interest in the property, in and outside
34 the continental United States, that the Administrator considers nec-
35 essary;

36 (3) lease to others the real and personal property and to provide by
37 contract or otherwise for necessary facilities for the welfare of Trans-
38 portation Security Administration employees and to acquire, maintain,
39 and operate equipment for these facilities;

40 (4) acquire services, including personal services the Secretary deter-
41 mines necessary, and acquire (by purchase, lease, condemnation, or

1 otherwise) and construct, repair, operate, and maintain research and
2 testing sites and facilities; and

3 (5) in cooperation with the Administrator of the Federal Aviation
4 Administration, utilize the research and development facilities of the
5 Federal Aviation Administration.

6 (b) TITLE.—Title to property or an interest in property acquired under
7 this section shall be held by the Government of the United States.

8 (c) CHARGE FOR LEASE OF REAL AND PERSONAL PROPERTY.—Notwith-
9 standing section 3302 of title 31, the Administrator may impose a reason-
10 able charge for the lease of real and personal property to Transportation
11 Security Administration employees and for use by Transportation Security
12 Administration employees and may credit amounts received to the appro-
13 priation or fund initially charged for operating and maintaining the prop-
14 erty. The amounts are available, without fiscal year limitation, for expendi-
15 ture for property management, operation, protection, construction, repair,
16 alteration, and related activities.

17 **§ 11506. Transfers of funds**

18 The Administrator may accept transfers of unobligated balances and un-
19 expended balances of funds appropriated to other Federal agencies (as the
20 term “agency” is defined in section 551 of title 5) to carry out functions
21 assigned by law to the Administrator.

22 **§ 11507. Regulations**

23 (a) IN GENERAL.—The Administrator may issue, rescind, and revise reg-
24 ulations as necessary to carry out the functions of the Transportation Secu-
25 rity Administration.

26 (b) EMERGENCY PROCEDURES.—

27 (1) IN GENERAL.—Notwithstanding another law or Executive order
28 (including an Executive order requiring a cost-benefit analysis), if the
29 Administrator determines that a regulation or security directive must
30 be issued immediately in order to protect transportation security, the
31 Administrator shall issue the regulation or security directive without
32 providing notice or an opportunity for comment and without prior ap-
33 proval of the Secretary.

34 (2) REVIEW BY TRANSPORTATION SECURITY OVERSIGHT BOARD.—A
35 regulation or security directive issued under this subsection shall be
36 subject to review by the Transportation Security Oversight Board es-
37 tablished under section 10319 of this title. A regulation or security di-
38 rective issued under this subsection shall remain effective for a period
39 not to exceed 90 days unless ratified or disapproved by the Board or
40 rescinded by the Secretary.

1 (c) FACTORS TO CONSIDER.—In determining whether to issue, rescind,
2 or revise a regulation under this chapter, the Administrator shall consider,
3 as a factor in the final determination, whether the costs of the regulation
4 are excessive in relation to the enhancement of security the regulation will
5 provide. The Administrator may waive requirements for an analysis that es-
6 timates the number of lives that will be saved by the regulation and the
7 monetary value of lives if the Administrator determines that it is not fea-
8 sible to make an estimate.

9 (d) AIRWORTHINESS OBJECTIONS BY FEDERAL AVIATION ADMINISTRA-
10 TION.—

11 (1) IN GENERAL.—The Administrator shall not take an aviation se-
12 curity action under this title if the Administrator of the Federal Avia-
13 tion Administration notifies the Administrator that the action could ad-
14 versely affect the airworthiness of an aircraft.

15 (2) REVIEW BY ADMINISTRATOR.—Notwithstanding paragraph (1),
16 the Administrator may take an aviation security action, after receiving
17 a notification concerning the action from the Administrator of the Fed-
18 eral Aviation Administration under paragraph (1), if the Secretary of
19 Transportation subsequently approves the action.

20 § 11508. Personnel and services

21 (a) AUTHORITY OF ADMINISTRATOR.—In carrying out the functions of
22 the Transportation Security Administration, the Administrator has the same
23 authority as is provided to the Administrator of the Federal Aviation Ad-
24 ministration under subsections (l) and (m) of section 106 of title 49.

25 (b) AUTHORITY OF AGENCY HEADS.—The head of a Federal agency shall
26 have the same authority to provide services, supplies, equipment, personnel,
27 and facilities to the Secretary as the head has to provide services, supplies,
28 equipment, personnel, and facilities to the Administrator of the Federal
29 Aviation Administration under section 106(m) of title 49.

30 (c) COORDINATION TO PREPARE FOR, PROTECT AGAINST, AND RESPOND
31 TO PUBLIC HEALTH THREATS TO THE TRANSPORTATION SECURITY SYS-
32 TEM.—

33 (1) IN GENERAL.—Pursuant to section 106(m) of title 49, the Ad-
34 ministrator may provide Transportation Security Administration per-
35 sonnel, who are not engaged in front line transportation security ef-
36 forts, to other components of the Department and other Federal agen-
37 cies to improve coordination with the components and agencies to pre-
38 pare for, protect against, and respond to public health threats to the
39 transportation security system of the United States.

40 (2) BRIEFING.—Not later than 180 days after December 27, 2021,
41 the Administrator shall brief the appropriate congressional committees

1 regarding efforts to improve coordination with other components of the
2 Department and other Federal agencies to prepare for, protect against,
3 and respond to public health threats to the transportation security sys-
4 tem of the United States

5 **§ 11509. Personnel management system**

6 (a) IN GENERAL.—The personnel management system established by the
7 Administrator of the Federal Aviation Administration under section 40122
8 of title 49 applies to employees of the Transportation Security Administra-
9 tion.

10 (b) MODIFICATIONS.—Subject to the requirements of section 40122 of
11 title 49, the Administrator may make modifications to the personnel man-
12 agement system with respect to those employees as the Administrator con-
13 siders appropriate, such as adopting aspects of other personnel systems of
14 the Department.

15 (c) MERITORIOUS EXECUTIVE OR DISTINGUISHED EXECUTIVE RANK
16 AWARDS.—

17 (1) DEFINITION OF APPLICABLE SECTIONS OF TITLE 5.—In this sub-
18 section, the term “applicable sections of title 5” means—

19 (A) section 4507(b) through (d) of title 5; and

20 (B) section 4507a(b) and (c) of title 5.

21 (2) IN GENERAL.—Notwithstanding section 40122(g)(2) of title 49,
22 the applicable sections of title 5 shall apply to the Transportation Secu-
23 rity Administration personnel management system, except that—

24 (A) for purposes of applying the applicable sections of title 5
25 to the personnel management system—

26 (i) the term “agency” means the Department;

27 (ii) the term “career appointee” means a Transportation
28 Security Administration employee serving on a career Trans-
29 portation Security Administration Executive appointment;

30 (iii) the term “senior career employee” means a Transpor-
31 tation Security Administration employee covered by the
32 Transportation Security Administration Core Compensation
33 System at the L or M pay band; and

34 (iv) the term “senior executive” means a Transportation
35 Security Administration executive serving on a Transpor-
36 tation Security Administration Executive appointment;

37 (B) receipt by a career appointee or a senior career employee
38 of the rank of Meritorious Executive or Meritorious Senior Profes-
39 sional entitles the individual to a lump-sum payment of an amount
40 equal to 20 percent of annual basic pay, which shall be in addition

1 to the basic pay paid under the applicable Transportation Security
2 Administration pay system; and

3 (C) receipt by a career appointee or a senior career employee
4 of the rank of Distinguished Executive or Distinguished Senior
5 Professional entitles the individual to a lump-sum payment of an
6 amount equal to 35 percent of annual basic pay, which shall be
7 in addition to the basic pay paid under the applicable Transpor-
8 tation Security Administration pay system.

9 **§ 11510. Authority of Inspector General**

10 The Transportation Security Administration is subject to chapter 4 of
11 title 5 and other laws relating to the authority of the Inspector General of
12 the Department.

13 **§ 11511. Law enforcement powers**

14 (a) IN GENERAL.—The Administrator may designate an employee of the
15 Transportation Security Administration or other Federal agency to serve as
16 a law enforcement officer.

17 (b) POWERS.—While engaged in official duties of the Transportation Se-
18 curity Administration as required to fulfill the responsibilities under this
19 section, a law enforcement officer designated under paragraph (1) may—

20 (1) carry a firearm;

21 (2) make an arrest without a warrant for any offense against the
22 United States committed in the presence of the officer, or for any fel-
23 ony cognizable under the laws of the United States if the officer has
24 probable cause to believe that the person to be arrested has committed
25 or is committing the felony; and

26 (3) seek and execute warrants for arrest or seizure of evidence issued
27 under the authority of the United States upon probable cause that a
28 violation has been committed.

29 (c) GUIDELINES ON EXERCISE OF AUTHORITY.—The authority provided
30 by this section shall be exercised in accordance with guidelines prescribed
31 by the Administrator, in consultation with the Attorney General, and shall
32 include adherence to the Attorney General's policy on use of deadly force.

33 (d) REVOCATION OR SUSPENSION OF AUTHORITY.—The powers author-
34 ized by this section may be rescinded or suspended should the Attorney
35 General determine that the Administrator has not complied with the guide-
36 lines prescribed in subsection (c) and convey the determination in writing
37 to the Secretary and the Administrator.

38 **§ 11512. Authority to exempt**

39 The Administrator may grant an exemption from a regulation prescribed
40 in carrying out this chapter if the Administrator determines that the exemp-
41 tion is in the public interest.

1 **§ 11513. Nondisclosure of security activities**

2 (a) IN GENERAL.—Notwithstanding section 552 of title 5, the Adminis-
3 trator shall prescribe regulations prohibiting the disclosure of information
4 obtained or developed in carrying out security under authority of chapter
5 409 of this title or the Aviation and Transportation Security Act (Public
6 Law 107–71, 115 Stat. 597) if the Administrator decides that disclosing the
7 information would—

- 8 (1) be an unwarranted invasion of personal privacy;
9 (2) reveal a trade secret or privileged or confidential commercial or
10 financial information; or
11 (3) be detrimental to the security of transportation.

12 (b) AVAILABILITY OF INFORMATION TO CONGRESS.—Subsection (a) does
13 not authorize information to be withheld from a committee of Congress au-
14 thorized to have the information.

15 (c) LIMITATION ON TRANSFERABILITY OF DUTIES.—Except as otherwise
16 provided by law, the Administrator may not transfer a duty or power under
17 this section to another department, agency, or instrumentality of the United
18 States.

19 (d) LIMITATIONS.—Nothing in this section, or any other provision of law,
20 shall be construed to authorize the designation of information as sensitive
21 security information (as defined in section 1520.5 of title 49, Code of Fed-
22 eral Regulations)—

- 23 (1) to conceal a violation of law, inefficiency, or administrative error;
24 (2) to prevent embarrassment to a person, organization, or agency;
25 (3) to restrain competition; or
26 (4) to prevent or delay the release of information that does not re-
27 quire protection in the interest of transportation security, including
28 basic scientific research information not clearly related to transpor-
29 tation security.

30 **§ 11514. Transportation security strategic planning**

31 (a) IN GENERAL.—The Secretary shall develop, prepare, implement, and
32 update, as needed—

- 33 (1) a National Strategy for Transportation Security; and
34 (2) transportation modal security plans addressing security risks, in-
35 cluding threats, vulnerabilities, and consequences, for aviation, railroad,
36 ferry, highway, maritime, pipeline, public transportation, over-the-road
37 bus, and other transportation infrastructure assets.

38 (b) ROLE OF SECRETARY OF TRANSPORTATION.—The Secretary shall
39 work jointly with the Secretary of Transportation in developing, revising,
40 and updating the documents required by paragraph (1).

1 (c) CONTENTS OF NATIONAL STRATEGY FOR TRANSPORTATION SECUR-
2 RITY.—The National Strategy for Transportation Security shall include the
3 following:

4 (1) An identification and evaluation of the transportation assets in
5 the United States that, in the interests of national security and com-
6 merce, must be protected from attack or disruption by terrorist or
7 other hostile forces, including modal security plans for aviation, bridge
8 and tunnel, commuter rail and ferry, highway, maritime, pipeline, rail,
9 mass transit, over-the-road bus, and other public transportation infra-
10 structure assets that could be at risk of attack or disruption.

11 (2) The development of risk-based priorities, based on risk assess-
12 ments conducted or received by the Secretary (including assessments
13 conducted under the Implementing Recommendations of the 9/11 Com-
14 mission Act of 2007 (Public Law 110–53, 121 Stat. 266)), across all
15 transportation modes and realistic deadlines for addressing security
16 needs associated with those assets referred to in paragraph (1).

17 (3) The most appropriate, practical, and cost-effective means of de-
18 fending those assets against threats to their security.

19 (4) A forward-looking strategic plan that sets forth the agreed-on
20 roles and missions of Federal, State, regional, local, and tribal authori-
21 ties and establishes mechanisms for encouraging cooperation and par-
22 ticipation by private-sector entities, including nonprofit employee labor
23 organizations, in the implementation of the plan.

24 (5) A comprehensive delineation of prevention, response, and recov-
25 ery responsibilities and issues regarding threatened and executed acts
26 of terrorism within the United States and threatened and executed acts
27 of terrorism outside the United States to the extent the acts affect
28 United States transportation systems.

29 (6) A prioritization of research and development objectives that sup-
30 port transportation security needs, giving a higher priority to research
31 and development directed toward protecting vital transportation assets.
32 Transportation security research and development projects shall be
33 based, to the extent practicable, on the prioritization. Nothing in the
34 preceding sentence shall be construed to require the termination of a
35 research or development project initiated by the Secretary or the Sec-
36 retary of Transportation before August 3, 2007.

37 (7) A 3- and 10-year budget for Federal transportation security pro-
38 grams that will achieve the priorities of the National Strategy for
39 Transportation Security.

1 (8) Methods for linking the individual transportation modal security
2 plans and the programs contained therein, and a plan for addressing
3 the security needs of intermodal transportation.

4 (9) Transportation modal security plans described in subsection
5 (a)(2), including operational recovery plans to expedite, to the max-
6 imum extent practicable, the return to operation of an adversely af-
7 fected transportation system following a major terrorist attack on that
8 system or other incident. These plans shall be coordinated with the re-
9 sumption of trade protocols required under section 30502 of this title
10 and the National Maritime Transportation Security Plan required
11 under section 70103(a) of title 46.

12 (d) SUBMISSIONS OF PLANS.—

13 (1) DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEES.—

14 In this subsection, the term “appropriate congressional committees”
15 means the Committee on Transportation and Infrastructure and the
16 Committee on Homeland Security of the House of Representatives and
17 the Committee on Commerce, Science, and Transportation, the Com-
18 mittee on Homeland Security and Governmental Affairs, and the Com-
19 mittee on Banking, Housing, and Urban Affairs of the Senate.

20 (2) BIENNIAL STRATEGY REPORT.—The Secretary shall submit the
21 National Strategy for Transportation Security, including the transpor-
22 tation modal security plans and any revisions to the National Strategy
23 for Transportation Security and the transportation modal security
24 plans, to appropriate congressional committees not less frequently than
25 April 1 of each even-numbered year.

26 (3) PERIODIC PROGRESS REPORT.—

27 (A) REQUIREMENT FOR REPORT.—Each year, in conjunction
28 with the submission of the budget to Congress under section
29 1105(a) of title 31, the Secretary shall submit to the appropriate
30 congressional committees an assessment of the progress made on
31 implementing the National Strategy for Transportation Security,
32 including the transportation modal security plans.

33 (B) CONTENT.—Each progress report submitted under this
34 paragraph shall include, at a minimum, the following:

35 (i) Recommendations for improving and implementing the
36 National Strategy for Transportation Security and the trans-
37 portation modal and intermodal security plans that the Sec-
38 retary of Homeland Security, in consultation with the Sec-
39 retary of Transportation, considers appropriate.

40 (ii) An accounting of all grants for transportation security,
41 including grants and contracts for research and development,

1 awarded by the Secretary in the most recent fiscal year and
2 a description of how the grants accomplished the goals of the
3 National Strategy for Transportation Security.

4 (iii) An accounting of all—

5 (I) funds requested in the President's budget sub-
6 mitted pursuant to section 1105 of title 31 for the most
7 recent fiscal year for transportation security, by mode;

8 (II) personnel working on transportation security by
9 mode, including the number of contractors; and

10 (III) information on the turnover in the previous year
11 among senior staff of the Department, including compo-
12 nent agencies, working on transportation security issues.
13 The information shall include the number of employees
14 who have permanently left the office, agency, or area in
15 which they worked, and the amount of time that they
16 worked for the Department.

17 (C) WRITTEN EXPLANATION OF TRANSPORTATION SECURITY
18 ACTIVITIES NOT DELINEATED IN THE NATIONAL STRATEGY FOR
19 TRANSPORTATION SECURITY.—At the end of each fiscal year, the
20 Secretary shall submit to the appropriate congressional committees
21 a written explanation of any Federal transportation security activ-
22 ity that is inconsistent with the National Strategy for Transpor-
23 tation Security, including the amount of funds to be expended for
24 the activity and the number of personnel involved.

25 (4) CLASSIFIED MATERIAL.—Any part of the National Strategy for
26 Transportation Security, or any part of the transportation modal secu-
27 rity plans, that involves information that is properly classified under
28 criteria established by Executive order shall be submitted to the appro-
29 priate congressional committees separately in a classified format.

30 (e) PRIORITY STATUS.—

31 (1) IN GENERAL.—The National Strategy for Transportation Secu-
32 rity shall be the governing document for Federal transportation secu-
33 rity efforts.

34 (2) OTHER PLANS AND REPORTS.—The National Strategy for Trans-
35 portation Security shall include, as an integral part or as an appen-
36 dix—

37 (A) the current National Maritime Transportation Security Plan
38 under section 70103 of title 46;

39 (B) the report required by section 40958 of this title;

40 (C) transportation modal security plans required under this
41 chapter;

1 (D) the transportation-sector-specific plan required under
2 Homeland Security Presidential Directive–7; and

3 (E) any other transportation security plan or report that the
4 Secretary determines appropriate for inclusion.

5 (f) COORDINATION.—In carrying out the responsibilities under this sec-
6 tion, the Secretary, in coordination with the Secretary of Transportation,
7 shall consult, as appropriate, with Federal, State, and local agencies, tribal
8 governments, private-sector entities (including nonprofit employee labor or-
9 ganizations), institutions of higher learning, and other entities.

10 (g) PLAN DISTRIBUTION.—The Secretary shall make available and appro-
11 priately publicize an unclassified version of the National Strategy for Trans-
12 portation Security, including its component transportation modal security
13 plans, to Federal, State, regional, local and tribal authorities, transportation
14 system owners or operators, private-sector stakeholders, including nonprofit
15 employee labor organizations representing transportation employees, institu-
16 tions of higher learning, and other appropriate entities.

17 **§ 11515. Risk scenarios**

18 (a) ANNUAL DEVELOPMENT OF RISK-BASED PRIORITIES.—The Adminis-
19 trator shall annually develop, consistent with the transportation modal secu-
20 rity plans required under section 11514 of this title, risk-based priorities
21 based on risk assessments conducted or received by the Secretary across all
22 transportation modes that consider threats, vulnerabilities, and con-
23 sequences.

24 (b) ANALYSIS OF SCENARIOS.—The Administrator shall ensure that the
25 risk-based priorities identified under subsection (a) are informed by an anal-
26 ysis of terrorist attack scenarios for each transportation mode, including
27 cyberattack scenarios and intelligence and open source information about
28 current and evolving threats.

29 (c) REPORT.—Not later than 120 days after the date the annual risk-
30 based priorities are developed under subsection (a), the Administrator shall
31 submit to the Committees on Commerce, Science, and Transportation and
32 Homeland Security and Governmental Affairs of the Senate and Committee
33 on Homeland Security of the House of Representatives a report that in-
34 cludes the following:

35 (1) Copies of the risk assessments for each transportation mode.

36 (2) A summary that ranks the risks within and across modes.

37 (3) A description of the risk-based priorities for securing the trans-
38 portation sector that identifies and prioritizes the greatest security
39 needs of the transportation sector, both across and within modes, in
40 the order in which the priorities should be addressed.

1 (4) Information on the underlying methodologies used to assess risks
2 across and within each transportation mode and the basis for assump-
3 tions regarding threats, vulnerabilities, and consequences made in as-
4 sessing and prioritizing risks within each mode and across modes.

5 (d) SUBMISSION OF INFORMATION.—Information provided under sub-
6 section (c) may be submitted in a classified format or unclassified format,
7 as the Administrator considers appropriate.

8 **§ 11516. Transportation Security Information Sharing Plan**

9 (a) DEFINITIONS.—In this section:

10 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
11 priate congressional committees” has the meaning given the term in
12 section 11514 of this title.

13 (2) PLAN.—The term “Plan” means the Transportation Security In-
14 formation Sharing Plan established under subsection (b).

15 (3) PUBLIC AND PRIVATE STAKEHOLDERS.—The term “public and
16 private stakeholders” means Federal, State, and local agencies, tribal
17 governments, and appropriate private entities, including nonprofit em-
18 ployee labor organizations representing transportation employees.

19 (4) TRANSPORTATION SECURITY INFORMATION.—The term “trans-
20 portation security information” means information relating to the risks
21 to transportation modes, including aviation, public transportation, rail-
22 road, ferry, highway, maritime, pipeline, and over-the-road bus trans-
23 portation, and may include specific and general intelligence products,
24 as appropriate.

25 (b) ESTABLISHMENT OF PLAN.—The Secretary, in consultation with the
26 program manager of the information sharing environment established under
27 section 11908 of this title, the Secretary of Transportation, and public and
28 private stakeholders, shall establish a Transportation Security Information
29 Sharing Plan. In establishing the Plan, the Secretary shall gather input on
30 the development of the Plan from private and public stakeholders and the
31 program manager of the information sharing environment established under
32 section 11908 of this title.

33 (c) PURPOSE OF PLAN.—The Plan shall promote the sharing of transpor-
34 tation security information between the Department of Homeland Security
35 and public and private stakeholders.

36 (d) CONTENT OF PLAN.—The Plan shall include—

37 (1) a description of how intelligence analysts in the Department will
38 coordinate their activities in the Department and with other Federal,
39 State, and local agencies, and tribal governments, including coordina-
40 tion with existing modal information sharing centers and the center de-
41 scribed in section 40509 of this title;

1 (2) the establishment of a point of contact, which may be a single
2 point of contact in the Department, for each mode of transportation
3 for the sharing of transportation security information with public and
4 private stakeholders, including an explanation and justification to the
5 appropriate congressional committees if the point of contact established
6 under this paragraph differs from the agency in the Department that
7 has the primary authority, or has been delegated the authority by the
8 Secretary, to regulate the security of that transportation mode;

9 (3) a reasonable deadline by which the Plan will be implemented; and

10 (4) a description of resource needs for fulfilling the Plan.

11 (e) COORDINATION WITH INFORMATION SHARING.—The Plan shall be—

12 (1) implemented in coordination, as appropriate, with the program
13 manager for the information sharing environment established under
14 section 11908 of this title; and

15 (2) consistent with the establishment of the information sharing en-
16 vironment and policies, guidelines, procedures, instructions, or stand-
17 ards established by the President or the program manager for the im-
18 plementation and management of the information sharing environment.

19 (f) REPORTS TO CONGRESS.—The Secretary shall annually submit to the
20 appropriate congressional committees a report containing the Plan.

21 (g) SECURITY CLEARANCES.—The Secretary shall, to the greatest extent
22 practicable, take steps to expedite the security clearances needed for des-
23 ignated public and private stakeholders to receive and obtain access to clas-
24 sified information distributed under this section, as appropriate.

25 (h) CLASSIFICATION OF MATERIAL.—The Secretary, to the greatest ex-
26 tent practicable, shall provide designated public and private stakeholders
27 with transportation security information in an unclassified format.

28 (i) STAKEHOLDER SEMIANNUAL REPORT.—

29 (1) IN GENERAL.—Except as provided in paragraph (2), the Sec-
30 retary shall provide a semiannual report to the appropriate congres-
31 sional committees that includes—

32 (A) the number of public and private stakeholders who were
33 provided with each report on the Plan;

34 (B) a description of the measures the Secretary has taken to
35 ensure proper treatment and security for classified information to
36 be shared with the public and private stakeholders under the Plan;
37 and

38 (C) an explanation of the reason for the denial of transportation
39 security information to a stakeholder who had previously received
40 the information.

1 (2) WHEN REPORT NOT REQUIRED.—The Secretary is not required
2 to provide a semiannual report under paragraph (1) if no stakeholders
3 have been added to or removed from the group of persons with whom
4 transportation security information is shared under the Plan since the
5 end of the period covered by the last preceding semiannual report.

6 **§ 11517. Public area security**

7 (a) DEFINITIONS.—In this section:

8 (1) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appro-
9 priate committees of Congress” means—

10 (A) the Committee on Commerce, Science, and Transportation
11 of the Senate;

12 (B) the Committee on Homeland Security and Governmental
13 Affairs of the Senate; and

14 (C) the Committee on Homeland Security of the House of Rep-
15 resentatives.

16 (2) PUBLIC AND PRIVATE STAKEHOLDERS.—The term “public and
17 private stakeholders” has the meaning given the term in section 11516
18 of this title.

19 (3) SURFACE TRANSPORTATION ASSET.—The term “surface trans-
20 portation asset” includes—

21 (A) facilities, equipment, or systems used to provide transpor-
22 tation services by—

23 (i) a public transportation agency (as defined in section
24 40501 of this title);

25 (ii) a railroad carrier (as defined in section 20102 of title
26 49); or

27 (iii) an owner or operator of—

28 (I) an entity offering scheduled, fixed-route transpor-
29 tation services by over-the road bus (as defined in sec-
30 tion 40701 of this title); or

31 (II) a bus terminal; or

32 (B) other transportation facilities, equipment, or systems, as de-
33 termined by the Secretary.

34 (b) WORKING GROUP.—

35 (1) ESTABLISHMENT.—The Administrator, in coordination with the
36 Cybersecurity and Infrastructure Security Agency, shall establish a
37 working group to promote collaborative engagement between the Trans-
38 portation Security Administration and public and private stakeholders
39 to develop non-binding recommendations for enhancing security in pub-
40 lic areas of transportation facilities (including facilities that are surface

1 transportation assets), including recommendations regarding the fol-
2 lowing:

3 (A) Information sharing and interoperable communication capa-
4 bilities among the Transportation Security Administration and
5 public and private stakeholders with respect to terrorist or other
6 threats.

7 (B) Coordinated incident response procedures.

8 (C) The prevention of terrorist attacks and other incidents
9 through strategic planning, security training, exercises and drills,
10 law enforcement patrols, worker vetting, and suspicious activity re-
11 porting.

12 (D) Infrastructure protection through effective construction de-
13 sign barriers and installation of advanced surveillance and other
14 security technologies.

15 (2) ANNUAL REPORT.—

16 (A) SUBMISSION.—Not later than 1 year after the date the
17 working group is established under paragraph (1), the Adminis-
18 trator shall submit to the appropriate committees of Congress a
19 report, covering the 12-month period preceding the date of the re-
20 port, on—

21 (i) the organization of the working group;

22 (ii) the activities of the working group;

23 (iii) the participation of the Transportation Security Ad-
24 ministration and public and private stakeholders in the activi-
25 ties of the working group;

26 (iv) the findings of the working group, including any rec-
27 ommendations.

28 (B) PUBLICATION.—The Administrator may publish a public
29 version of the report that describes the activities of the working
30 group and such related matters as would be informative to the
31 public, consistent with section 552(b) of title 5.

32 (3) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of
33 title 5 shall not apply to the working group established under para-
34 graph (1) or any subcommittee of the working group.

35 (c) TECHNICAL ASSISTANCE.—The Secretary shall—

36 (1) inform owners and operators of surface transportation assets
37 about the availability of technical assistance, including vulnerability as-
38 sessment tools and cybersecurity guidelines, to help protect and en-
39 hance the resilience of public areas of the assets; and

1 (2) on request, and subject to the availability of appropriations, pro-
2 vide the technical assistance to owners and operators of surface trans-
3 portation assets.

4 (d) BEST PRACTICES.—

5 (1) SECRETARY.—Not later than 1 year after October 5, 2018, and
6 periodically thereafter, the Secretary shall publish on the Department
7 website and widely disseminate, as appropriate, current best practices
8 for protecting and enhancing the resilience of public areas of transpor-
9 tation facilities (including facilities that are surface transportation as-
10 sets), including associated frameworks or templates for implementation.

11 (2) ADMINISTRATOR.—The Administrator shall, in accordance with
12 law, periodically submit information, as received or developed, on best
13 practices developed by the Transportation Security Administration or
14 appropriate transportation stakeholders related to protecting the public
15 spaces of transportation infrastructure from emerging threats, to the
16 following:

17 (A) Federal Security Directors at airports.

18 (B) Appropriate security directors for other modes of transpor-
19 tation.

20 (C) Other appropriate transportation security stakeholders.

21 (e) INFORMATION SHARING.—The Administrator shall, in accordance
22 with law—

23 (1) in coordination with the Office of the Director of National Intel-
24 ligence and industry partners, implement improvements to the Air Do-
25 main Intelligence and Analysis Center to encourage increased participa-
26 tion from stakeholders and enhance government and industry security
27 information sharing on transportation security threats, including on cy-
28 bersecurity threat awareness;

29 (2) improve and expand the City and Airport Threat Assessment or
30 similar program to public and private stakeholders to capture, quantify,
31 communicate, and apply applicable intelligence to inform transportation
32 infrastructure mitigation measures, such as—

33 (A) quantifying levels of risk by airport that can be used to de-
34 termine risk-based security mitigation measures at each location;
35 and

36 (B) determining random and surge employee inspection oper-
37 ations based on changing levels of risk;

38 (3) continue to disseminate Transportation Intelligence Notes, tear-
39 lines, and related intelligence products to appropriate transportation se-
40 curity stakeholders on a regular basis; and

1 (4) continue to regularly conduct routine and threat-specific classi-
2 fied briefings between the Transportation Security Administration and
3 appropriate transportation sector stakeholders on an individual or
4 group basis to provide greater information sharing between public and
5 private sectors.

6 (f) MASS NOTIFICATION.—The Administrator shall encourage security
7 stakeholders to utilize mass notification systems, including the Integrated
8 Public Alert Warning System of the Federal Emergency Management Agen-
9 cy and social media platforms, to disseminate information to transportation
10 community employees, travelers, and the general public, as appropriate.

11 (g) PUBLIC AWARENESS PROGRAMS.—The Secretary, in coordination
12 with the Administrator, shall expand public programs of the Department
13 and the Transportation Security Administration that increase security
14 threat awareness, education, and training to include transportation network
15 public area employees, including airport and transportation vendors, local
16 hotels, cab and limousine companies, ridesharing companies, cleaning com-
17 panies, gas station attendants, cargo operators, and general aviation mem-
18 bers.

19 (h) REVIEW.—

20 (1) IN GENERAL.—Not later than 1 year after October 5, 2018, the
21 Administrator shall—

22 (A) review regulations, directives, policies, and procedures
23 issued by the Administrator regarding the transportation of a fire-
24 arm and ammunition; and

25 (B) submit to the appropriate committees of Congress a report
26 on the findings of the review under subparagraph (A), including,
27 as appropriate, information on plans to modify a regulation, direc-
28 tive, policy, or procedure based on the review.

29 (2) CONSULTATION.—In preparing the report under paragraph (1),
30 the Administrator shall consult with—

31 (A) the Aviation Security Advisory Committee;

32 (B) the Surface Transportation Security Advisory Committee
33 under section 40722 of this title; and

34 (C) appropriate public and private stakeholders.

35 **§ 11518. Best practices to secure against vehicle-based at-**
36 **tacks**

37 The Administrator shall disseminate best practices to public and private
38 stakeholders regarding how to enhance transportation security against the
39 threat of a vehicle-based terrorist attack.

1 **§ 11519. Enforcement of certain regulations and orders of**
2 **the Secretary**

3 (a) DEFINITIONS.—In this section:

4 (1) PERSON.—The term “person” does not include—

5 (A) the United States Postal Service; or

6 (B) the Department of Defense.

7 (2) SMALL BUSINESS CONCERN.—The term “small business concern”
8 has the meaning given the term in section 3 of the Small Business Act
9 (15 U.S.C. 632).

10 (b) APPLICABILITY OF SECTION.—

11 (1) IN GENERAL.—This section applies to the enforcement of regula-
12 tions prescribed, and orders issued, by the Secretary under a provision
13 of chapter 701 of title 46 or under a provision of title 49 other than
14 a provision of former chapter 449 (in this section referred to as an
15 “applicable provision of title 49”).

16 (2) VIOLATIONS OF FORMER CHAPTER 449 OF TITLE 49.—The pen-
17 alties under part B of subchapter V of chapter 409 of this title apply
18 to violations of regulations prescribed and orders issued by the Sec-
19 retary or the Administrator under former chapter 449 of title 49.

20 (3) NON-APPLICABILITY TO CERTAIN VIOLATIONS.—

21 (A) IN GENERAL.—Subsections (c) through (f) do not apply to
22 violations of regulations prescribed, and orders issued, by the Sec-
23 retary under a provision of title 49—

24 (i) involving the transportation of personnel or shipments
25 of materials by contractors where the Department of Defense
26 has assumed control and responsibility;

27 (ii) by a member of the armed forces of the United States
28 when performing official duties; or

29 (iii) by a civilian employee of the Department of Defense
30 when performing official duties.

31 (B) ALTERNATIVE PENALTIES.—Violations described in clause
32 (i), (ii), or (iii) of subparagraph (A) shall be subject to penalties
33 as determined by the Secretary of Defense or the designee of the
34 Secretary of Defense.

35 (c) CIVIL PENALTY.—

36 (1) IN GENERAL.—A person is liable to the United States Govern-
37 ment for a civil penalty of not more than \$10,000 for a violation of
38 a regulation prescribed, or order issued, by the Secretary under an ap-
39 plicable provision of title 49.

40 (2) REPEAT VIOLATIONS.—A separate violation occurs under this
41 subsection for each day the violation continues.

1 (d) ADMINISTRATIVE IMPOSITION OF CIVIL PENALTIES.—

2 (1) IN GENERAL.—The Secretary may impose a civil penalty for a
3 violation of a regulation prescribed, or order issued, under an applica-
4 ble provision of title 49. The Secretary shall give written notice of the
5 finding of a violation and the penalty.

6 (2) SCOPE OF CIVIL ACTION.—In a civil action to collect a civil pen-
7 alty imposed by the Secretary under this section, a court may not re-
8 examine issues of liability or the amount of the penalty.

9 (3) JURISDICTION.—The district courts of the United States shall
10 have exclusive jurisdiction of civil actions to collect a civil penalty im-
11 posed by the Secretary under this section if—

12 (A) the amount in controversy is more than—

13 (i) \$400,000, if the violation was committed by a person
14 other than an individual or small business concern; or

15 (ii) \$50,000 if the violation was committed by an individual
16 or small business concern;

17 (B) the action is in rem or another action in rem based on the
18 same violation has been brought; or

19 (C) another action has been brought for an injunction based on
20 the same violation.

21 (4) MAXIMUM PENALTY.—The maximum civil penalty the Secretary
22 administratively may impose under this subsection is—

23 (A) \$400,000, if the violation was committed by a person other
24 than an individual or small business concern; or

25 (B) \$50,000, if the violation was committed by an individual or
26 small business concern.

27 (5) NOTICE AND OPPORTUNITY TO REQUEST HEARING.—Before im-
28 posing a penalty under this chapter, the Secretary shall provide to the
29 person against whom the penalty is to be imposed—

30 (A) written notice of the proposed penalty; and

31 (B) the opportunity to request a hearing on the proposed pen-
32 alty, if the Secretary receives the request not later than 30 days
33 after the date on which the person receives notice.

34 (e) COMPROMISE AND SETOFF.—

35 (1) COMPROMISE.—The Secretary may compromise the amount of a
36 civil penalty imposed under this section.

37 (2) SETOFF.—The United States Government may deduct the
38 amount of a civil penalty imposed or compromised under this section
39 from amounts it owes the person liable for the penalty.

40 (f) INVESTIGATIONS AND PROCEEDINGS.—Subchapter V of chapter 409
41 of this title applies to investigations and proceedings brought under this sec-

1 tion to the same extent that chapter 461 of title 49 applies to investigations
2 and proceedings brought with respect to aviation security duties designated
3 to be carried out by the Secretary.

4 (g) ENFORCEMENT TRANSPARENCY.—

5 (1) IN GENERAL.—The Secretary shall—

6 (A) provide an annual summary to the public of all enforcement
7 actions taken by the Secretary under this section; and

8 (B) include in each summary the docket number of each en-
9 forcement action, the type of alleged violation, the penalty or pen-
10 alties proposed, and the final assessment amount of each penalty.

11 (2) ELECTRONIC AVAILABILITY.—Each summary under this sub-
12 section shall be made available to the public by electronic means.

13 (3) RELATIONSHIP TO FREEDOM OF INFORMATION ACT AND PRIVACY
14 ACT.—Nothing in this subsection shall be construed to require disclo-
15 sure of information or records that are exempt from disclosure under
16 section 552 or 552a of title 5.

17 **§ 11520. Registered traveler fee**

18 Notwithstanding section 553 of title 5, the Secretary shall impose a fee
19 for a registered traveler program undertaken by the Department by notice
20 in the Federal Register, and may modify the fee from time to time by notice
21 in the Federal Register. Fees shall not exceed the aggregate costs associated
22 with the program, shall be credited to the Transportation Security Adminis-
23 tration registered traveler fee account, and are available until expended.

24 **§ 11521. Enhanced security measures**

25 (a) IN GENERAL.—The Administrator may take the following actions:

26 (1) Require effective 911 emergency call capability for telephones
27 serving passenger aircraft and passenger trains.

28 (2) Establish a uniform system of identification for all State and
29 local law enforcement personnel for use in obtaining permission to
30 carry weapons in aircraft cabins and in obtaining access to a secured
31 area of an airport, if otherwise authorized to carry the weapons.

32 (3) Establish requirements to implement trusted passenger programs
33 and use available technologies to expedite the security screening of pas-
34 sengers who participate in the programs, thereby allowing security
35 screening personnel to focus on those passengers who should be subject
36 to more extensive screening.

37 (4) In consultation with the Commissioner of the Food and Drug
38 Administration, develop alternative security procedures under which a
39 medical product to be transported on a flight of an air carrier would
40 not be subject to an inspection that would irreversibly damage the
41 product.

1 (5) Provide for the use of technologies, including wireless and wire
2 line data technologies, to enable the private and secure communication
3 of threats to aid in the screening of passengers and other individuals
4 on airport property who are identified on any State or Federal security-
5 related data base for the purpose of having an integrated response co-
6 ordination of various authorized airport security forces.

7 (6) In consultation with the Administrator of the Federal Aviation
8 Administration, consider whether to require all pilot licenses to incor-
9 porate a photograph of the license holder and appropriate biometric im-
10 prints.

11 (7) Provide for the use of voice stress analysis, biometric, or other
12 technologies to prevent a person who might pose a danger to air safety
13 or security from boarding the aircraft of an air carrier or foreign air
14 carrier in air transportation or intrastate air transportation.

15 (8) Provide for the use of technology that will permit enhanced in-
16 stant communications and information between airborne passenger air-
17 craft and appropriate individuals or facilities on the ground.

18 (9) Require that air carriers provide flight attendants with a dis-
19 creet, hands-free, wireless method of communicating with the pilots.

20 (b) ANNUAL REPORT.—Until the Administrator has implemented or de-
21 cided not to take each of the actions specified in subsection (a), the Admin-
22 istrator shall transmit to Congress by May 19 each year a report on the
23 progress of the Administrator in evaluating and taking the actions, includ-
24 ing legislative recommendations that the Secretary may have for enhancing
25 transportation security.

26 **§ 11522. Performance management system**

27 (a) ESTABLISHING A FAIR AND EQUITABLE SYSTEM FOR MEASURING
28 STAFF PERFORMANCE.—The Administrator shall establish a performance
29 management system that strengthens the organization's effectiveness by
30 providing for the establishment of goals and objectives for managers, em-
31 ployees, and organizational performance consistent with the performance
32 plan.

33 (b) ESTABLISHING MANAGEMENT ACCOUNTABILITY FOR MEETING PER-
34 FORMANCE GOALS.—

35 (1) ADMINISTRATOR.—Each year, the Secretary and the Adminis-
36 trator shall enter into an annual performance agreement that shall set
37 forth organizational and individual performance goals for the Adminis-
38 trator.

39 (2) SENIOR MANAGERS.—Each year, the Administrator and each
40 senior manager who reports to the Administrator shall enter into an
41 annual performance agreement that sets forth organization and indi-

1 vidual goals for those managers. All other employees hired under the
2 authority of the Administrator shall enter into an annual performance
3 agreement that sets forth organization and individual goals for those
4 employees.

5 (c) PERFORMANCE-BASED SERVICE CONTRACTING.—To the extent con-
6 tracts are used to implement the Aviation and Transportation Security Act
7 (Public Law 107–71, 115 Stat. 597), the Administrator shall, to the extent
8 practical, maximize the use of performance-based service contracts. These
9 contracts should be consistent with guidelines published by the Office of
10 Federal Procurement Policy.

11 **§ 11523. Voluntary provision of emergency services**

12 (a) PROGRAM FOR PROVISION OF VOLUNTARY SERVICES.—

13 (1) PROGRAM.—The Administrator shall carry out a program to per-
14 mit qualified law enforcement officers, firefighters, and emergency med-
15 ical technicians to provide emergency services on commercial air flights
16 during emergencies.

17 (2) REQUIREMENTS.—The Administrator shall establish require-
18 ments for qualifications of providers of voluntary services under the
19 program under paragraph (1), including training requirements, that
20 the Administrator considers appropriate.

21 (3) CONFIDENTIALITY OF REGISTRY.—If as part of the program
22 under paragraph (1), the Administrator requires or permits registra-
23 tion of law enforcement officers, firefighters, or emergency medical
24 technicians who are willing to provide emergency services on commer-
25 cial flights during emergencies, the Administrator shall take appro-
26 priate actions to ensure that the registry is available only to appro-
27 priate airline personnel and otherwise remains confidential.

28 (4) CONSULTATION.—The Administrator shall consult with the Ad-
29 ministrator of the Federal Aviation Administration, appropriate rep-
30 representatives of the commercial airline industry, and organizations rep-
31 representing community-based law enforcement, firefighters, and emer-
32 gency medical technicians, in carrying out the program under para-
33 graph (1), including the actions taken under paragraph (3).

34 (b) EXEMPTION FROM LIABILITY.—An individual is not liable for dam-
35 ages in an action brought in a Federal or State court that arises from an
36 act or omission of the individual in providing, or attempting to provide, as-
37 sistance in the case of an in-flight emergency in an aircraft of an air carrier
38 if the individual meets qualifications as the Administrator prescribes for
39 purposes of this section.

40 (c) EXCEPTION.—The exemption under subsection (b) shall not apply in
41 a case in which an individual provides, or attempts to provide, assistance

1 described in subsection (b) in a manner that constitutes gross negligence
2 or willful misconduct.

3 **§ 11524. Disposition of unclaimed money and clothing**

4 (a) IN GENERAL.—

5 (1) DISPOSITION OF UNCLAIMED MONEY.—Notwithstanding section
6 3302 of title 31, unclaimed money recovered at an airport security
7 checkpoint—

8 (A) shall be retained by the Transportation Security Adminis-
9 tration; and

10 (B) shall remain available until expended for the purpose of pro-
11 viding civil aviation security as required in this chapter.

12 (2) DISPOSITION OF UNCLAIMED CLOTHING.—

13 (A) IN GENERAL.—In disposing of unclaimed clothing recovered
14 at any airport security checkpoint, the Administrator shall make
15 every reasonable effort, in consultation with the Secretary of Vet-
16 erans Affairs, to transfer the clothing to the local airport authority
17 or other local authorities for donation to charity, including local
18 veterans organizations or other local charitable organizations for
19 distribution to homeless or needy veterans and veteran families.

20 (B) AGREEMENTS.—In implementing subparagraph (A), the
21 Administrator may enter into agreements with airport authorities.

22 (C) OTHER CHARITABLE ARRANGEMENTS.—Nothing in this
23 subsection prevents an airport or the Transportation Security Ad-
24 ministration from donating unclaimed clothing to a charitable or-
25 ganization of their choosing.

26 (D) LIMITATION.—Nothing in this subsection creates a cost to
27 the Government.

28 (b) ANNUAL REPORT.—Not later than 180 days after October 18, 2004,
29 and annually thereafter, the Administrator shall transmit annually to the
30 Committee on Transportation and Infrastructure of the House of Rep-
31 resentatives; the Committee on Appropriations of the House of Representa-
32 tives; the Committee on Commerce, Science and Transportation of the Sen-
33 ate; and the Committee on Appropriations of the Senate, a report that con-
34 tains a detailed description of the amount of unclaimed money recovered in
35 total and at each individual airport, and specifies how the unclaimed money
36 is being used to provide civil aviation security.

37 **§ 11525. Transmittals to Congress**

38 The Administrator shall transmit directly to the appropriate committee
39 of Congress each report, legislative proposal, or other communication of the
40 executive branch relating to the Transportation Security Administration and

1 required to be submitted to Congress or the appropriate committee of Con-
2 gress.

3 **§ 11526. Transportation security preparedness plan for com-**
4 **municable disease outbreak**

5 (a) DEVELOPMENT.—Not later than December 27, 2023, the Secretary,
6 acting through the Administrator, in coordination with the Chief Medical
7 Officer of the Department, and in consultation with the partners identified
8 under subparagraphs (A) through (D) of subsection (c)(1), shall develop a
9 transportation security preparedness plan to address the event of a commu-
10 nicable disease outbreak. The Secretary, acting through the Administrator,
11 shall ensure the plan aligns with relevant Federal plans and strategies for
12 communicable disease outbreaks.

13 (b) CONSIDERATIONS.—In developing the plan required under subsection
14 (a), the Secretary, acting through the Administrator, shall consider each of
15 the following:

16 (1) The findings of the survey required under section 6411 of the
17 National Defense Authorization Act for Fiscal Year 2022 (Public Law
18 117–81, div. F, 135 Stat. 2409).

19 (2) The findings of the analysis required under section 6414 of the
20 National Defense Authorization Act for Fiscal Year 2022 (Public Law
21 117–81, div. F, 135 Stat. 2412).

22 (3) The plan required under section 6415 of the National Defense
23 Authorization Act for Fiscal Year 2022 (Public Law 117–81, div. F,
24 135 Stat. 2413).

25 (4) All relevant reports and recommendations regarding the Adminis-
26 tration’s response to the COVID19 pandemic, including any reports
27 and recommendations issued by the Comptroller General and the In-
28 spector General of the Department.

29 (5) Lessons learned from Federal interagency efforts during the
30 COVID19 pandemic.

31 (c) CONTENTS.—The plan developed under subsection (a) shall include
32 each of the following:

33 (1) Plans for communicating and collaborating in the event of a com-
34 municable disease outbreak with the following partners:

35 (A) Appropriate Federal departments and agencies, including
36 the Department of Health and Human Services, the Centers for
37 Disease Control and Prevention, the Department of Transpor-
38 tation, the Department of Labor, and appropriate interagency task
39 forces.

40 (B) The workforce of the Transportation Security Administra-
41 tion, including through the labor organization certified as the ex-

1 clusive representative of full- and part-time non-supervisory Trans-
2 portation Security Administration personnel carrying out screening
3 functions undersection 40911 of this title.

4 (C) International partners, including the International Civil
5 Aviation Organization and foreign governments, airports, and air
6 carriers.

7 (D) Public and private stakeholders, as the term is defined
8 under section 11516(a) of this title.

9 (E) The traveling public.

10 (2) Plans for protecting the safety of the Transportation Security
11 Administration workforce, including—

12 (A) reducing the risk of communicable disease transmission at
13 screening checkpoints and within the Transportation Security Ad-
14 ministration’s workforce related to the Administration’s transpor-
15 tation security operations and mission;

16 (B) ensuring the safety and hygiene of screening checkpoints
17 and other workstations;

18 (C) supporting equitable and appropriate access to relevant vac-
19 cines, prescriptions, and other medical care; and

20 (D) tracking rates of employee illness, recovery, and death.

21 (3) Criteria for determining the conditions that may warrant the in-
22 tegration of additional actions in the aviation screening system in re-
23 sponse to the communicable disease outbreak and a range of potential
24 roles and responsibilities that align with the conditions.

25 (4) Contingency plans for temporarily adjusting checkpoint oper-
26 ations to provide for passenger and employee safety while maintaining
27 security during the communicable disease outbreak.

28 (5) Provisions setting forth criteria for establishing an interagency
29 task force or other standing engagement platform with other appro-
30 priate Federal departments and agencies, including the Department of
31 Health and Human Services and the Department of Transportation, to
32 address the communicable disease outbreak.

33 (6) A description of scenarios in which the Administrator should con-
34 sider exercising authorities provided under section 11502 of this title
35 and for what purposes.

36 (7) Considerations for assessing the appropriateness of issuing secu-
37 rity directives and emergency amendments to regulated parties in var-
38 ious modes of transportation, including surface transportation, and
39 plans for ensuring compliance with the measures.

40 (8) A description of any potential obstacles, including funding con-
41 straints and limitations to authorities, that could restrict the ability of

1 the Administration to respond appropriately to a communicable disease
2 outbreak.

3 (d) DISSEMINATION.—On development of the plan required under sub-
4 section (a), the Administrator shall disseminate the plan to the partners
5 identified under subsection (c)(1) and to the Committee on Homeland Secu-
6 rity of the House of Representatives and the Committee on Homeland Secu-
7 rity and Governmental Affairs and the Committee on Commerce, Science,
8 and Transportation of the Senate.

9 (e) REVIEW.—Not later than two years after the date on which the plan
10 is disseminated under subsection (d), and biennially thereafter, the Sec-
11 retary, acting through the Administrator and in coordination with the Chief
12 Medical Officer of the Department, shall review the plan and, after con-
13 sultation with the partners identified under subparagraphs (A) through (D)
14 of subsection (c)(1), update the plan as appropriate.

15 **§ 11527. Aviation security directives and emergency amend-**
16 **ments**

17 (a) IN GENERAL.—The Administrator shall develop and implement guide-
18 lines with respect to domestic and last point of departure airports to—

19 (1) ensure the inclusion, as appropriate, of air carriers, domestic air-
20 port operators, and other transportation security stakeholders in the
21 development and implementation of security directives and emergency
22 amendments;

23 (2) document input provided by air carriers, domestic airport opera-
24 tors, and other transportation security stakeholders during the security
25 directive and emergency amendment, development, and implementation
26 processes;

27 (3) define a process, including timeframes, and with the inclusion of
28 feedback from air carriers, domestic airport operators, and other trans-
29 portation security stakeholders, for cancelling or incorporating security
30 directives and emergency amendments into security programs;

31 (4) conduct engagement with foreign partners on the implementation
32 of security directives and emergency amendments, as appropriate, in-
33 cluding recognition if existing security measures at a last point of de-
34 parture airport are found to provide commensurate security as intended
35 by potential new security directives and emergency amendments; and

36 (5) ensure that new security directives and emergency amendments
37 are focused on defined security outcomes.

38 (b) BRIEFING TO CONGRESS.—The Administrator shall brief the Com-
39 mittee on Homeland Security of the House of Representatives and the Com-
40 mittee on Commerce, Science, and Transportation of the Senate on the
41 guidelines described in paragraph (1).

1 (c) DECISIONS NOT SUBJECT TO JUDICIAL REVIEW.—Notwithstanding
2 any other provision of law, any action of the Administrator under paragraph
3 (1) is not subject to judicial review.

4 **Subchapter II—Acquisition Improvements**

5 **§ 11541. Definitions**

6 In this subchapter:

7 (1) PLAN.—The term “Plan” means the strategic 5-year technology
8 investment plan the Administrator develops under section 11542 of this
9 title.

10 (2) SECURITY-RELATED TECHNOLOGY.—The term “security-related
11 technology” means any technology that assists the Transportation Se-
12 curity Administration in the prevention of, or defense against, threats
13 to United States transportation systems, including threats to people,
14 property, and information.

15 **§ 11542. Technology investment plan**

16 (a) IN GENERAL.—The Administrator—

17 (1) shall develop and submit to Congress a strategic 5-year tech-
18 nology investment plan that may include a classified addendum to re-
19 port sensitive transportation security risks, technology vulnerabilities,
20 or other sensitive security information; and

21 (2) to the extent possible, shall publish the Plan in an unclassified
22 format in the public domain after it is approved by the Secretary.

23 (b) CONSULTATION.—The Administrator shall develop the Plan in con-
24 sultation with—

25 (1) the Under Secretary for Management;

26 (2) the Under Secretary for Science and Technology;

27 (3) the Chief Information Officer; and

28 (4) the aviation stakeholder advisory committee established by the
29 Administrator.

30 (c) CONTENTS.—The Plan shall include—

31 (1) an analysis of transportation security risks and the associated ca-
32 pability gaps that would be best addressed by security-related tech-
33 nology, including consideration of the most recent quadrennial home-
34 land security review under section 11706 of this title;

35 (2) a set of security-related technology acquisition needs that—

36 (A) is prioritized based on risk and associated capability gaps
37 identified under paragraph (1); and

38 (B) includes planned technology programs and projects with de-
39 fined objectives, goals, timelines, and measures;

40 (3) an analysis of current and forecast trends in domestic and inter-
41 national passenger travel;

1 (4) an identification of currently deployed security-related tech-
2 nologies that are at or near the end of their lifecycles;

3 (5) an identification of test, evaluation, modeling, and simulation ca-
4 pabilities, including target methodologies, rationales, and timelines nec-
5 essary to support the acquisition of the security-related technologies ex-
6 pected to meet the needs under paragraph (2);

7 (6) an identification of opportunities for public-private partnerships,
8 small and disadvantaged company participation, intragovernment col-
9 laboration, university centers of excellence, and national laboratory
10 technology transfer;

11 (7) an identification of the Transportation Security Administration's
12 acquisition workforce needs for the management of planned security-
13 related technology acquisitions, including consideration of leveraging
14 acquisition expertise of other Federal agencies;

15 (8) an identification of the security resources, including information
16 security resources, that will be required to protect security-related tech-
17 nology from physical or cyber theft, diversion, sabotage, or attack;

18 (9) an identification of initiatives to streamline the Transportation
19 Security Administration's acquisition process and provide greater pre-
20 dictability and clarity to small, medium, and large businesses, including
21 the timelines for testing and evaluation;

22 (10) an assessment of the impact on commercial aviation passengers;

23 (11) a strategy for consulting airport management, air carrier rep-
24 resentatives, and Federal security directors when an acquisition will
25 lead to the removal of equipment at airports, and how the strategy for
26 consulting with those officials of the relevant airports will address po-
27 tential negative impacts on commercial passengers or airport oper-
28 ations; and

29 (12) in consultation with the National Institute of Standards and
30 Technology, an identification of security-related technology interface
31 standards, in existence or if implemented, that could promote more
32 interoperable passenger, baggage, and cargo screening systems.

33 (d) LEVERAGING THE PRIVATE SECTOR.—To the extent practicable, and
34 in a manner that is consistent with fair and equitable practices, the Plan
35 shall—

36 (1) leverage emerging technology trends and research and develop-
37 ment investment trends in the public and private sectors;

38 (2) incorporate private-sector input, including from the aviation in-
39 dustry stakeholder advisory committee established by the Adminis-
40 trator, through requests for information, industry days, and other inno-
41 vative means consistent with the Federal Acquisition Regulation; and

1 (3) in consultation with the Under Secretary for Science and Tech-
2 nology, identify technologies in existence or in development that, with
3 or without adaptation, are expected to be suitable in meeting mission
4 needs.

5 (e) DISCLOSURE.—The Administrator shall include with the Plan a list
6 of nongovernment persons that contributed to the writing of the Plan.

7 (f) UPDATE AND REPORT.—The Administrator shall, in collaboration
8 with relevant industry and government stakeholders, annually submit to
9 Congress in an appendix to the budget request and publish in an unclassi-
10 fied format in the public domain—

11 (1) an update of the Plan;

12 (2) a report on the extent to which each security-related technology
13 the Transportation Security Administration has acquired since the last
14 issuance or update of the Plan is consistent with the planned tech-
15 nology programs and projects identified under subsection (c)(2) for
16 that security-related technology; and

17 (3) information about acquisitions completed during the fiscal year
18 preceding the fiscal year during which the report is submitted.

19 (g) ADDITIONAL UPDATE REQUIREMENTS.—Updates and reports under
20 subsection (f) shall—

21 (1) be prepared in consultation with—

22 (A) the individuals described in subsection (b); and

23 (B) the Surface Transportation Security Advisory Committee
24 established under section 40722 of this title; and

25 (2) include—

26 (A) information relating to technology investments by the
27 Transportation Security Administration and the private sector
28 that the Department supports with research, development, testing,
29 and evaluation for aviation, including air cargo, and surface trans-
30 portation security;

31 (B) information about acquisitions completed during the fiscal
32 year preceding the fiscal year during which the report is sub-
33 mitted;

34 (C) information relating to equipment of the Transportation Se-
35 curity Administration that is in operation after the end of the life-
36 cycle of the equipment specified by the manufacturer of the equip-
37 ment; and

38 (D) to the extent practicable, a classified addendum to report
39 sensitive transportation security risks and associated capability
40 gaps that would be best addressed by security-related technology
41 described in subparagraph (A).

1 (h) NOTICE OF COVERED CHANGES TO PLAN.—

2 (1) DEFINITION OF COVERED CHANGE.—In this subsection, the term
3 “covered change” means—

4 (A) an increase or decrease in the dollar amount allocated to
5 the procurement of a technology; or

6 (B) an increase or decrease in the number of a technology.

7 (2) NOTICE REQUIRED.—The Administrator shall submit to the
8 Committee on Commerce, Science, and Transportation of the Senate
9 and the Committee on Homeland Security of the House of Representa-
10 tives notice of a covered change to the Plan not later than 90 days
11 after the date that the covered change is made.

12 **§ 11543. Acquisition justification and reports and certifi-**
13 **cation**

14 (a) ACQUISITION JUSTIFICATION.—Before the Transportation Security
15 Administration implements any security-related technology acquisition, the
16 Administrator, in accordance with the Department’s policies and directives,
17 shall determine whether the acquisition is justified by conducting an anal-
18 ysis that includes—

19 (1) an identification of the scenarios and level of risk to transpor-
20 tation security from those scenarios that would be addressed by the se-
21 curity-related technology acquisition;

22 (2) an assessment of how the proposed acquisition aligns with the
23 Plan;

24 (3) a comparison of the total expected lifecycle cost against the total
25 expected quantitative and qualitative benefits to transportation secu-
26 rity;

27 (4) an analysis of alternative security solutions, including policy or
28 procedure solutions, to determine if the proposed security-related tech-
29 nology acquisition is the most effective and cost-efficient solution based
30 on cost-benefit considerations;

31 (5) an assessment of the potential privacy and civil liberties implica-
32 tions of the proposed acquisition that includes, to the extent prac-
33 ticable, consultation with organizations that advocate for the protection
34 of privacy and civil liberties;

35 (6) a determination that the proposed acquisition is consistent with
36 fair information practice principles issued by the Privacy Officer of the
37 Department;

38 (7) confirmation that there are no significant risks to human health
39 or safety posed by the proposed acquisition; and

40 (8) an estimate of the benefits to commercial aviation passengers.

41 (b) REPORTS AND CERTIFICATION.—

1 (1) IN GENERAL.—Not later than the end of the 30-day period pre-
2 ceding the award by the Transportation Security Administration of a
3 contract for any security-related technology acquisition exceeding
4 \$30,000,000, the Administrator shall submit to the Committee on
5 Commerce, Science, and Transportation of the Senate and the Com-
6 mittee on Homeland Security of the House of Representatives—

7 (A) the results of the comprehensive acquisition justification
8 under subsection (a); and

9 (B) a certification by the Administrator that the benefits to
10 transportation security justify the contract cost.

11 (2) REDUCTION DUE TO IMMINENT TERRORIST THREAT.—If there is
12 a known or suspected imminent threat to transportation security, the
13 Administrator—

14 (A) may reduce the 30-day period under paragraph (1) to 5
15 days to rapidly respond to the threat; and

16 (B) shall immediately notify the Committee on Commerce,
17 Science, and Transportation of the Senate and the Committee on
18 Homeland Security of the House of Representatives of the known
19 or suspected imminent threat.

20 **§ 11544. Baseline establishment and reports**

21 (a) BASELINE REQUIREMENTS.—

22 (1) IN GENERAL.—Before the Transportation Security Administra-
23 tion implements any security-related technology acquisition, the appro-
24 priate acquisition official of the Department shall establish and docu-
25 ment a set of formal baseline requirements. The requirements shall—

26 (A) include the estimated costs (including lifecycle costs), sched-
27 ule, and performance milestones for the planned duration of the
28 acquisition;

29 (B) identify the acquisition risks and a plan for mitigating those
30 risks; and

31 (C) assess the personnel necessary to manage the acquisition
32 process, manage the ongoing program, and support training and
33 other operations as necessary.

34 (2) FEASIBILITY.—In establishing the performance milestones under
35 paragraph (1)(A), the appropriate acquisition official of the Depart-
36 ment, to the extent possible and in consultation with the Under Sec-
37 retary for Science and Technology, shall ensure that achieving those
38 milestones is technologically feasible.

39 (3) TEST AND EVALUATION PLAN.—The Administrator, in consulta-
40 tion with the Under Secretary for Science and Technology, shall de-
41 velop a test and evaluation plan that describes—

1 (A) the activities that are expected to be required to assess ac-
2 quired technologies against the performance milestones established
3 under paragraph (1)(A);

4 (B) the necessary and cost-effective combination of laboratory
5 testing, field testing, modeling, simulation, and supporting analysis
6 to ensure that the technologies meet the Transportation Security
7 Administration's mission needs;

8 (C) an efficient planning schedule to ensure that test and eval-
9 uation activities are completed without undue delay; and

10 (D) if commercial aviation passengers are expected to interact
11 with the security-related technology, methods that could be used
12 to ensure passenger acceptance of and familiarization with the se-
13 curity-related technology.

14 (4) VERIFICATION AND VALIDATION.—The appropriate acquisition
15 official of the Department—

16 (A) subject to subparagraph (B), shall utilize independent re-
17 views to verify and validate the performance milestones and cost
18 estimates developed under paragraph (1) for a security-related
19 technology that pursuant to section 11542(c)(2) of this title has
20 been identified as a high priority need in the most recent Plan;
21 and

22 (B) shall ensure that the use of independent reviewers does not
23 unduly delay the schedule of any acquisition.

24 (5) STREAMLINING ACCESS FOR INTERESTED VENDORS.—The Ad-
25 ministrator shall establish a streamlined process for an interested ven-
26 dor of a security-related technology to request and receive appropriate
27 access to the baseline requirements and test and evaluation plans that
28 are necessary for the vendor to participate in the acquisition process
29 for that technology.

30 (b) REVIEW OF BASELINE REQUIREMENTS AND DEVIATION; REPORT.—

31 (1) REVIEW.—

32 (A) IN GENERAL.—The appropriate acquisition official of the
33 Department shall review and assess each implemented acquisition
34 to determine if the acquisition is meeting the baseline require-
35 ments established under subsection (a).

36 (B) ASSESSMENT.—The review shall include an assessment of
37 whether—

38 (i) the planned testing and evaluation activities have been
39 completed; and

40 (ii) the results of that testing and evaluation demonstrate
41 that the performance milestones are technologically feasible.

1 (2) REPORT.—Not later than 30 days after making a finding de-
2 scribed in clause (i), (ii), or (iii) of subparagraph (A), the Adminis-
3 trator shall submit a report to the Committee on Commerce, Science,
4 and Transportation of the Senate and the Committee on Homeland Se-
5 curity of the House of Representatives that includes—

6 (A) the results of any assessment that finds that—

7 (i) the actual or planned costs exceed the baseline costs by
8 more than 10 percent;

9 (ii) the actual or planned schedule for delivery has been de-
10 layed by more than 180 days; or

11 (iii) there is a failure to meet any performance milestone
12 that directly impacts security effectiveness;

13 (B) the cause for the excessive costs, delay, or failure; and

14 (C) a plan for corrective action.

15 **§ 11545. Inventory utilization**

16 (a) USE OF EXISTING INVENTORY.—Before the procurement of addi-
17 tional quantities of equipment to fulfill a mission need, the Administrator,
18 to the extent practicable, shall utilize any existing units in the Transpor-
19 tation Security Administration’s inventory to meet that need.

20 (b) TRACKING OF INVENTORY.—

21 (1) IN GENERAL.—The Administrator shall establish a process for
22 tracking—

23 (A) the location of security-related technology in the inventory
24 under subsection (a);

25 (B) the utilization status of security-related technology in the
26 inventory under subsection (a); and

27 (C) the quality of security-related equipment in the inventory
28 under subsection (a).

29 (2) INTERNAL CONTROLS.—The Administrator shall implement in-
30 ternal controls to ensure up-to-date accurate data on security-related
31 technology owned, deployed, and in use.

32 (c) LOGISTICS MANAGEMENT.—

33 (1) IN GENERAL.—The Administrator shall establish logistics prin-
34 ciples for managing inventory in an effective and efficient manner.

35 (2) LIMITATION ON JUST-IN-TIME LOGISTICS.—The Administrator
36 may not use just-in-time logistics if doing so—

37 (A) would inhibit necessary planning for large-scale delivery of
38 equipment to airports or other facilities; or

39 (B) would unduly diminish surge capacity for response to a ter-
40 rorist threat.

1 **§ 11546. Small business contracting goals**

2 Not later than March 18 of each year, the Administrator shall submit to
3 the Committee on Commerce, Science, and Transportation of the Senate
4 and the Committee on Homeland Security of the House of Representatives
5 a report that includes—

6 (1) the Transportation Security Administration’s performance record
7 with respect to meeting its published small-business contracting goals
8 during the preceding fiscal year;

9 (2) if the goals described in paragraph (1) were not met or the
10 Transportation Security Administration’s performance was below the
11 published small-business contracting goals of the Department—

12 (A) a list of challenges, including deviations from the Transpor-
13 tation Security Administration’s subcontracting plans, and factors
14 that contributed to the level of performance during the preceding
15 fiscal year;

16 (B) an action plan, with benchmarks, for addressing each of the
17 challenges identified in subparagraph (A) that—

18 (i) is prepared after consultation with the Secretary of De-
19 fense and the heads of Federal departments and agencies
20 that achieved their published goals for prime contracting with
21 small and minority-owned businesses, including small and dis-
22 advantaged businesses, in prior fiscal years; and

23 (ii) identifies policies and procedures that could be incor-
24 porated by the Transportation Security Administration in fur-
25 therance of achieving the Administration’s published goal for
26 the contracting; and

27 (3) a status report on the implementation of the action plan that was
28 developed in the preceding fiscal year in accordance with paragraph
29 (2)(B), if the plan was required.

30 **§ 11547. Consistency with Federal Acquisition Regulation**
31 **and Department policies and directives**

32 The Administration shall execute the responsibilities set forth in this sub-
33 chapter in a manner consistent with, and not duplicative of, the Federal Ac-
34 quisition Regulation and the Department’s policies and directives.

35 **§ 11548. Diversified security technology industry market-**
36 **place**

37 (a) DEFINITIONS.—In this section:

38 (1) INTELLIGENCE COMMUNITY.—The term “intelligence commu-
39 nity” has the meaning given the term in section 3 of the National Se-
40 curity Act of 1947 (50 U.S.C. 3003).

1 (2) SMALL BUSINESS CONCERN.—The term “small business concern”
2 has the meaning described under section 3 of the Small Business Act
3 (15 U.S.C. 632).

4 (3) SMALL BUSINESS INNOVATOR.—The term “small business inno-
5 vator” means a small business concern that has an advanced transpor-
6 tation security technology or capability.

7 (b) DEVELOPMENT OF STRATEGY.—Not later than 120 days after Octo-
8 ber 5, 2018, the Administrator shall develop and submit to the Committee
9 on Commerce, Science, and Transportation of the Senate and the Com-
10 mittee on Homeland Security of the House of Representatives a strategy to
11 promote a diverse security technology industry marketplace on which the
12 Administrator can rely to acquire advanced transportation security tech-
13 nologies or capabilities, including by increased participation of small busi-
14 ness innovators.

15 (c) CONTENTS OF STRATEGY.—The strategy required under subsection
16 (b) shall include the following:

17 (1) Information on how existing Transportation Security Administra-
18 tion solicitation, testing, evaluation, piloting, acquisition, and procure-
19 ment processes impact the Administrator’s ability to acquire from the
20 security technology industry marketplace, including small business
21 innovators that have not previously provided technology to the Trans-
22 portation Security Administration, innovative technologies or capabili-
23 ties with the potential to enhance transportation security.

24 (2) Specific actions that the Administrator will take, including modi-
25 fications to the processes described in paragraph (1), to foster diver-
26 sification in the security technology industry marketplace.

27 (3) Projected timelines for implementing the actions described in
28 paragraph (2).

29 (4) Plans for how the Administrator could, to the extent practicable,
30 assist a small business innovator periodically during the processes, in-
31 cluding when a small business innovator lacks adequate resources to
32 participate in the processes, to facilitate an advanced transportation se-
33 curity technology or capability being developed and acquired by the Ad-
34 ministrator.

35 (5) An assessment of the feasibility of partnering with an organiza-
36 tion described in section 501(c)(3) of the Internal Revenue Code of
37 1986 (26 U.S.C. 501(c)(3)) and exempt from tax under section 501(a)
38 of the Internal Revenue Code of 1986 (26 U.S.C. 501(a)) to provide
39 venture capital to businesses, particularly small business innovators, for
40 commercialization of innovative transportation security technologies

1 that are expected to be ready for commercialization in the near term
2 and within 36 months.

3 (d) FEASIBILITY ASSESSMENT.—In conducting the feasibility assessment
4 under subsection (c)(5), the Administrator shall consider the following:

5 (1) Establishing an organization described in section 501(c)(3) of the
6 Internal Revenue Code of 1986 (26 U.S.C. 501(c)(3)) and exempt from
7 tax under section 501(a) of the Internal Revenue Code of 1986 (26
8 U.S.C. 501(a)) as a venture capital partnership between the private
9 sector and the intelligence community to help businesses, particularly
10 small business innovators, commercialize innovative security-related
11 technologies.

12 (2) Enhanced engagement through the Science and Technology Di-
13 rectorate of the Department.

14 (e) RULE OF CONSTRUCTION.—Nothing in this section may be construed
15 as requiring changes to the Transportation Security Administration stand-
16 ards for security technology.

17 **§ 11549. Third party testing and verification of screening**
18 **technology**

19 (a) IN GENERAL.—In carrying out the responsibilities under section
20 11501(e)(9) of this title, the Administrator shall develop and implement, not
21 later than 1 year after October 5, 2018, a program to enable a vendor of
22 related security screening technology to obtain testing and verification, in-
23 cluding as an alternative to the Transportation Security Administration’s
24 test and evaluation process, by an appropriate third party, of the technology
25 before procurement or deployment.

26 (b) DETECTION TESTING.—

27 (1) IN GENERAL.—The third party testing and verification program
28 authorized under subsection (a) shall include detection testing to evalu-
29 ate the performance of the security screening technology system re-
30 garding the probability of false alarm and other indicators that the sys-
31 tem is able to meet the Transportation Security Administration’s mis-
32 sion needs.

33 (2) RESULTS.—The results of the third party detection testing under
34 paragraph (1) shall be considered final if the results are approved by
35 the Administration in accordance with approval standards developed by
36 the Administrator.

37 (3) COORDINATION WITH FINAL TESTING.—To the extent prac-
38 ticable, but without compromising the integrity of the Transportation
39 Security Administration test and evaluation process, the Administrator
40 shall coordinate the third party detection testing under paragraph (1)
41 with any subsequent, final Federal Government testing.

1 (4) INTERNATIONAL TESTING.—To the extent practicable and per-
2 missible under law and considering the national security interest of the
3 United States, the Administrator shall—

4 (A) share detection testing information and standards with ap-
5 propriate international partners; and

6 (B) coordinate with appropriate international partners to align
7 Transportation Security Administration testing and evaluation
8 with relevant international standards to maximize the capability to
9 detect explosives and other threats.

10 (c) OPERATIONAL TESTING.—

11 (1) IN GENERAL.—Subject to paragraph (2), the third party testing
12 and verification program authorized under subsection (a) shall include
13 operation testing.

14 (2) LIMITATION.—Third party operational testing under paragraph
15 (1) may not exceed 1 year.

16 (d) THIRD PARTY TESTING AS AN ALTERNATIVE.—Third party testing
17 under subsection (a) shall replace as an alternative, at the discretion of the
18 Administrator, the testing at the Transportation Security Administration
19 Systems Integration Facility, including testing for—

20 (1) health and safety factors;

21 (2) operator interface;

22 (3) human factors;

23 (4) environmental factors;

24 (5) throughput;

25 (6) reliability, maintainability, and availability factors; and

26 (7) interoperability.

27 (e) TESTING AND VERIFICATION FRAMEWORK.—

28 (1) IN GENERAL.—The Administrator shall—

29 (A) establish a framework for third party testing and for
30 verifying a security technology is operationally effective and able
31 to meet the Transportation Security Administration's mission
32 needs before it may enter or re-enter, as applicable, the oper-
33 ational context at an airport or other transportation facility;

34 (B) use phased implementation to allow the Transportation Se-
35 curity Administration and the third party to establish best prac-
36 tices; and

37 (C) oversee the third party testing and evaluation framework.

38 (2) RECOMMENDATIONS.—The Administrator shall request the Avia-
39 tion Security Advisory Committee's Security Technology Subcommittee,
40 in consultation with representatives of the security manufacturers in-

1 industry, to develop and submit to the Administrator recommendations
2 for the third party testing and verification framework.

3 (f) FIELD TESTING.—The Administrator shall prioritize the field testing
4 and evaluation, including by third parties, of security technology and equip-
5 ment at airports and on site at security technology manufacturers when pos-
6 sible as an alternative to the Transportation Security Administration Sys-
7 tems Integration Facility.

8 (g) APPROPRIATE THIRD PARTIES.—

9 (1) CITIZENSHIP REQUIREMENT.—An appropriate third party under
10 subsection (a) shall be—

11 (A) if an individual, a citizen of the United States; or

12 (B) if an entity, owned and controlled by a citizen of the United
13 States.

14 (2) WAIVER.—The Administrator may waive the requirement under
15 paragraph (1)(B) of a parent company that has implemented a foreign
16 ownership, control, or influence mitigation plan that has been approved
17 by the Defense Security Service of the Department of Defense before
18 applying to provide third party testing. The Administrator may reject
19 an application to provide third party testing under subsection (a) sub-
20 mitted by an entity that requires a waiver under this paragraph.

21 (3) ENSURING NO CONFLICT OF INTEREST.—The Administrator
22 shall ensure, to the extent possible, that an entity providing third party
23 testing under this section does not have a contractual, business, or
24 other pecuniary interest (exclusive of the testing) in—

25 (A) the security screening technology subject to the testing; or

26 (B) the vendor of the technology.

27 (h) REVIEW BY COMPTROLLER GENERAL.—

28 (1) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In
29 this subsection, the term “appropriate congressional committees”
30 means—

31 (A) the Committee on Commerce, Science, and Transportation
32 of the Senate;

33 (B) the Committee on Homeland Security and Governmental
34 Affairs of the Senate; and

35 (C) the Committee on Homeland Security of the House of Rep-
36 resentatives.

37 (2) IN GENERAL.—Not later than 2 years after October 5, 2018, the
38 Comptroller General shall submit to the appropriate committees of
39 Congress a study on the third party testing program developed under
40 this section.

1 (3) REVIEW.—The study under paragraph (2) shall include the fol-
2 lowing:

3 (A) Efficiencies or gains in effectiveness achieved in Transpor-
4 tation Security Administration operations, including technology ac-
5 quisition or screening operations, as a result of the program.

6 (B) The degree to which the Transportation Security Adminis-
7 tration conducts timely and regular oversight of the appropriate
8 third parties engaged in the testing.

9 (C) The effect of the program on the following:

10 (i) The introduction of innovative detection technologies
11 into security screening operations.

12 (ii) The availability of testing for technologies developed by
13 small to medium sized businesses.

14 (D) Vulnerabilities associated with the program, including with
15 respect to the following:

16 (i) National security.

17 (ii) Conflicts of interest between the appropriate third par-
18 ties engaged in the testing and the entities providing the tech-
19 nologies to be tested.

20 (iii) Waste, fraud, and abuse.

21 **§ 11550. Transportation Security Administration Systems In-**
22 **tegration Facility**

23 (a) IN GENERAL.—The Administrator shall continue to operate the
24 Transportation Security Administration Systems Integration Facility (in
25 this section referred to as the “TSIF”) for the purposes of testing and eval-
26 uating advanced transportation security screening technologies related to
27 the mission of the Transportation Security Administration.

28 (b) REQUIREMENTS.—The TSIF shall—

29 (1) evaluate the technologies described in subsection (a) to enhance
30 the security of transportation systems through screening and threat
31 mitigation and detection;

32 (2) test the technologies described in subsection (a) to support iden-
33 tified mission needs of the Transportation Security Administration and
34 to meet requirements for acquisitions and procurement;

35 (3) to the extent practicable, provide original equipment manufactur-
36 ers with test plans to minimize requirement interpretation disputes and
37 adhere to provided test plans;

38 (4) collaborate with other technical laboratories and facilities for pur-
39 poses of augmenting the capabilities of TSIF;

1 (5) deliver advanced transportation security screening technologies
2 that enhance the overall security of domestic transportation systems;
3 and

4 (6) to the extent practicable, provide funding and promote efforts to
5 enable participation by a small business concern (as the term is de-
6 scribed under section 3 of the Small Business Act (15 U.S.C. 632))
7 that—

8 (A) has an advanced technology or capability; but

9 (B) does not have adequate resources to participate in testing
10 and evaluation processes.

11 (c) STAFFING AND RESOURCE ALLOCATION.—The Administrator shall
12 ensure adequate staffing and resource allocations for the TSIF in a manner
13 that—

14 (1) prevents unnecessary delays in the testing and evaluation of ad-
15 vanced transportation security screening technologies for acquisitions
16 and procurement determinations;

17 (2) ensures the issuance of final paperwork certification no later
18 than 45 days after the date the testing and evaluation has concluded;
19 and

20 (3) ensures collaboration with technology stakeholders to close capa-
21 bilities gaps in transportation security.

22 (d) NOTIFICATION OF TESTING AND EVALUATION EXCEEDING 180
23 DAYS.—

24 (1) DEFINITIONS.—In this subsection:

25 (A) APPROPRIATE COMMITTEES OF CONGRESS.—The term “ap-
26 propriate committees of Congress” means—

27 (i) the Committee on Commerce, Science, and Transpor-
28 tation of the Senate;

29 (ii) the Committee on Homeland Security and Govern-
30 mental Affairs of the Senate; and

31 (iii) the Committee on Homeland Security of the House of
32 Representatives.

33 (B) DELIVERY DATE.—The term “delivery date” means the
34 date that the owner of an advanced transportation security screen-
35 ing technology—

36 (i) after installation, delivers the technology to the Trans-
37 portation Security Administration for testing and evaluation;
38 and

39 (ii) submits to the Administrator, in such form and manner
40 as the Administrator prescribes, a signed notification of the
41 delivery described in clause (i).

1 (2) IN GENERAL.—The Administrator shall notify the appropriate
2 committees of Congress if testing and evaluation by the TSIF of an
3 advance transportation security screening technology under this section
4 exceeds 180 days from the delivery date.

5 (3) NOTIFICATION.—The notification under paragraph (2) shall in-
6 clude—

7 (A) information relating to the delivery date;

8 (B) a justification for why the testing and evaluation process
9 has exceeded 180 days; and

10 (C) the estimated date for completion of the testing and evalua-
11 tion.

12 (e) RETESTING AND EVALUATION.—Advanced transportation security
13 screening technology that fails testing and evaluation by the TSIF may be
14 retested and evaluated at the discretion of the Administrator.

15 (f) RULE OF CONSTRUCTION.—Nothing in this section may be construed
16 to affect the authority or responsibility of an officer of the Department, or
17 an officer of another Federal department or agency, with respect to re-
18 search, development, testing, and evaluation of technologies, including the
19 authorities or responsibilities of the Under Secretary for Science and Tech-
20 nology and the Assistant Secretary of the Countering Weapons of Mass De-
21 struction Office.

22 **Subchapter III—Maintenance of Security-** 23 **Related Technology**

24 **§ 11561. Preventive maintenance validation process for se-** 25 **curity-related technology deployed to airports**

26 (a) IN GENERAL.—Not later than 180 days after October 5, 2018, the
27 Administrator shall develop and implement a preventive maintenance valida-
28 tion process for security-related technology deployed to airports.

29 (b) MAINTENANCE BY TRANSPORTATION SECURITY ADMINISTRATION
30 PERSONNEL AT AIRPORTS.—For maintenance to be carried out by Trans-
31 portation Security Administration personnel at airports, the process referred
32 to in subsection (a) shall include the following:

33 (1) Guidance to Transportation Security Administration personnel at
34 airports specifying how to conduct and document preventive mainte-
35 nance actions.

36 (2) Mechanisms for the Transportation Security Administration to
37 verify compliance with the guidance issued pursuant to paragraph (1).

38 (c) MAINTENANCE BY CONTRACTORS AT AIRPORTS.—For maintenance to
39 be carried out by a contractor at airports, the process referred to in sub-
40 section (a) shall require the following:

1 (1) Provision of monthly preventative maintenance schedules to ap-
2 propriate Transportation Security Administration personnel at each
3 airport that includes information on each action to be completed by a
4 contractor.

5 (2) Notification to appropriate Transportation Security Administra-
6 tion personnel at each airport when maintenance action is completed
7 by a contractor.

8 (3) A process for independent validation by a third party of con-
9 tractor maintenance.

10 (d) PENALTIES FOR NONCOMPLIANCE.—The Administrator shall require
11 maintenance for contracts entered into 60 days after October 5, 2018, or
12 later for security-related technology deployed to airports to include penalties
13 for noncompliance when it is determined that either preventive or corrective
14 maintenance has not been completed according to contractual requirements
15 and manufacturers' specifications.

16 **Chapter 117—Management**

Sec.

11701. Under Secretary for Management.

11702. Chief Financial Officer.

11703. Chief Information Officer.

11704. Chief Human Capital Officer.

11705. Officer for Civil Rights and Civil Liberties.

11706. Quadrennial homeland security review.

11707. Interoperable communications.

11708. Joint Task Forces.

11709. Office of Strategy, Policy, and Plans.

11710. Employee engagement.

11711. Acquisition professional career program.

17 **§ 11701. Under Secretary for Management**

18 (a) DEFINITION OF INTEROPERABLE COMMUNICATIONS.—In this section,
19 the term “interoperable communications” has the same meaning given that
20 term in section 10912(a) of this title.

21 (b) IN GENERAL.—The Under Secretary for Management serves as the
22 Chief Management Officer and principal advisor to the Secretary on matters
23 relating to the management of the Department, including management inte-
24 gration and transformation in support of homeland security operations and
25 programs. The Secretary, acting through the Under Secretary for Manage-
26 ment, is responsible for the management and administration of the Depart-
27 ment, including the following:

28 (1) The budget, appropriations, expenditures of funds, accounting,
29 and finance.

30 (2) Procurement.

31 (3) Human resources and personnel.

1 (4) Information technology and communications systems, including
2 policies and directives to achieve and maintain interoperable commu-
3 nications among the components of the Department.

4 (5) Facilities, property, equipment, and other material resources.

5 (6) Security for personnel, information technology and communica-
6 tions systems, facilities, property, equipment, and other material re-
7 sources.

8 (7) Strategic management planning and annual performance plan-
9 ning and identification and tracking of performance measures relating
10 to the responsibilities of the Department.

11 (8) Grants and other assistance management programs.

12 (9) The management integration and transformation in each func-
13 tional management discipline of the Department, including information
14 technology, financial management, acquisition management, and human
15 capital management, to ensure an efficient and orderly consolidation of
16 functions and personnel in the Department, including—

17 (A) the development of centralized data sources and connectivity
18 of information systems to the greatest extent practicable to en-
19 hance program visibility, transparency, and operational effective-
20 ness and coordination;

21 (B) the development of standardized and automated manage-
22 ment information to manage and oversee programs and make in-
23 formed decisions to improve the efficiency of the Department;

24 (C) the development of effective program management and reg-
25 ular oversight mechanisms, including clear roles and processes for
26 program governance, sharing of best practices, and access to time-
27 ly, reliable, and evaluated data on all acquisitions and investments;
28 and

29 (D) the overall supervision, including the conduct of internal au-
30 dits and management analyses, of the programs and activities of
31 the Department, including establishment of oversight procedures
32 to ensure a full and effective review of the efforts by components
33 of the Department to implement policies and procedures of the
34 Department for management integration and transformation.

35 (10) The development of a transition and succession plan, before De-
36 cember 1 of each year in which a Presidential election is held, to guide
37 the transition of Department functions to a new Presidential adminis-
38 tration, and making the plan available to the next Secretary and Under
39 Secretary for Management and to the congressional homeland security
40 committees.

1 (11) Reporting to the Government Accountability Office every 6
2 months to demonstrate measurable, sustainable progress made in im-
3 plementing the corrective action plans of the Department to address
4 the designation of the management functions of the Department on the
5 bi-annual high-risk list of the Government Accountability Office, until
6 the Comptroller General of the United States submits to the appro-
7 priate congressional committees written notification of removal of the
8 high-risk designation.

9 (12) The conduct of internal audits and management analyses of the
10 programs and activities of the Department.

11 (13) Any other management duties that the Secretary may des-
12 ignate.

13 (e) WAIVERS FOR CONDUCTING BUSINESS WITH SUSPENDED OR
14 DEBARRED CONTRACTORS.—Not later than 5 days after the date on which
15 the Chief Procurement Officer or Chief Financial Officer of the Department
16 issues a waiver of the requirement that an agency not engage in business
17 with a contractor or other recipient of funds listed as a party suspended
18 or debarred from receiving contracts, grants, or other types of Federal as-
19 sistance in the System for Award Management maintained by the General
20 Services Administration, or any successor, the Under Secretary for Manage-
21 ment shall submit to the congressional homeland security committees and
22 the Inspector General of the Department notice of the waiver and an expla-
23 nation of the finding by the Under Secretary that a compelling reason exists
24 for the waiver.

25 (d) VEHICLE FLEETS.—

26 (1) DEFINITIONS.—In this subsection:

27 (A) COMPONENT HEAD.—The term “component head” means
28 the head of a component of the Department with a vehicle fleet.

29 (B) EXCESS VEHICLE.—The term “excess vehicle” means a ve-
30 hicle that is not essential to support mission requirements of a
31 component.

32 (C) OPTIMAL FLEET SIZE.—The term “optimal fleet size”
33 means, with respect to a particular component, the appropriate
34 number of vehicles to support mission requirements of the compo-
35 nent.

36 (D) VEHICLE FLEET.—The term “vehicle fleet” means all
37 owned, commercially leased, or Government-leased vehicles of the
38 Department or of a component of the Department, including vehi-
39 cles used for law enforcement and other purposes.

40 (2) IN GENERAL.—In carrying out responsibilities regarding vehicle
41 fleets pursuant to subsection (b)(5), the Under Secretary for Manage-

1 ment shall be responsible for overseeing and managing vehicle fleets
2 throughout the Department. The Under Secretary shall also be respon-
3 sible for the following:

4 (A) Ensuring that components are in compliance with Federal
5 law, Federal regulations, executive branch guidance, and Depart-
6 ment policy (including associated guidance) relating to fleet man-
7 agement and use of vehicles from home to work.

8 (B) Developing and distributing a standardized vehicle alloca-
9 tion methodology and fleet management plan for components to
10 use to determine optimal fleet size in accordance with paragraph
11 (5).

12 (C) Ensuring that components formally document fleet manage-
13 ment decisions.

14 (D) Approving component fleet management plans, vehicle
15 leases, and vehicle acquisitions.

16 (3) COMPONENT RESPONSIBILITIES.—

17 (A) IN GENERAL.—Component heads—

18 (i) shall—

19 (I) comply with Federal law, Federal regulations, execu-
20 tive branch guidance, and Department policy (including
21 associated guidance) relating to fleet management and
22 use of vehicles from home to work;

23 (II) ensure that data related to fleet management is
24 accurate and reliable;

25 (III) use the data to develop a vehicle allocation tool
26 derived by using the standardized vehicle allocation
27 methodology provided by the Under Secretary for Man-
28 agement to determine the optimal fleet size for the next
29 fiscal year and a fleet management plan; and

30 (IV) use vehicle allocation methodologies and fleet
31 management plans to develop annual requests for fund-
32 ing to support vehicle fleets pursuant to paragraph (7);
33 and

34 (ii) may not, except as provided in subparagraph (B), lease
35 or acquire new vehicles or replace existing vehicles without
36 prior approval from the Under Secretary for Management
37 pursuant to paragraph (6)(B).

38 (B) EXCEPTION REGARDING CERTAIN LEASING AND ACQUISI-
39 TIONS.—If exigent circumstances warrant, a component head may
40 lease or acquire a new vehicle or replace an existing vehicle with-
41 out prior approval from the Under Secretary for Management. If

1 under the exigent circumstances a component head leases, ac-
2 quires, or replaces a vehicle, the component head shall provide to
3 the Under Secretary an explanation of the circumstances.

4 (4) ONGOING OVERSIGHT.—

5 (A) QUARTERLY MONITORING.—In accordance with paragraph
6 (5), the Under Secretary for Management shall collect, on a quar-
7 terly basis, information regarding component vehicle fleets, includ-
8 ing information on fleet size, composition, cost, and vehicle utiliza-
9 tion.

10 (B) AUTOMATED INFORMATION.—The Under Secretary for
11 Management shall seek to achieve a capability to collect, on a
12 quarterly basis, automated information regarding component vehi-
13 cle fleets, including the number of trips, miles driven, hours and
14 days used, and the associated costs of the mileage for leased vehi-
15 cles.

16 (C) MONITORING.—The Under Secretary for Management shall
17 track and monitor component information provided pursuant to
18 subparagraph (A) and, as appropriate, subparagraph (B), to en-
19 sure that component vehicle fleets are the optimal fleet size and
20 cost effective. The Under Secretary shall use the information to
21 inform the annual component fleet analyses referred to in para-
22 graph (5).

23 (5) ANNUAL REVIEW OF COMPONENT FLEET ANALYSIS.—

24 (A) IN GENERAL.—To determine the optimal fleet size and as-
25 sociated resources needed for each fiscal year, component heads
26 shall annually submit to the Under Secretary for Management a
27 vehicle allocation tool and fleet management plan using informa-
28 tion described in paragraph (4)(A). The tools and plans may be
29 submitted in classified form if a component head determines that
30 it is necessary to protect operations or mission requirements.

31 (B) VEHICLE ALLOCATION TOOL.—Component heads shall de-
32 velop a vehicle allocation tool in accordance with subclause (III)
33 of paragraph (3)(A)(i) that includes an analysis of the following:

34 (i) Vehicle utilization data, including the number of trips,
35 miles driven, hours and days used, and the associated costs
36 of the mileage for leased vehicles, in accordance with para-
37 graph (3)(A)(i).

38 (ii) The role of vehicle fleets in supporting mission require-
39 ments for each component.

40 (iii) Any other information determined relevant by the com-
41 ponent heads.

1 (C) FLEET MANAGEMENT PLANS.—Component heads shall use
2 information described in subparagraph (B) to develop a fleet man-
3 agement plan for each component. The fleet management plans
4 shall include the following:

5 (i) A plan for how each component may achieve optimal
6 fleet size determined by the vehicle allocation tool required
7 under subparagraph (B), including the elimination of excess
8 vehicles in accordance with paragraph (6), if applicable.

9 (ii) A cost-benefit analysis supporting the plan.

10 (iii) A schedule each component will follow to obtain opti-
11 mal fleet size.

12 (iv) Any other information determined relevant by compo-
13 nent heads.

14 (D) REVIEW.—The Under Secretary for Management shall re-
15 view and make a determination on the results of each component's
16 vehicle allocation tool and fleet management plan under this para-
17 graph to ensure each component's vehicle fleets are the optimal
18 fleet size and that components are in compliance with applicable
19 Federal law, Federal regulations, executive branch guidance, and
20 Department policy (including associated guidance) pursuant to
21 paragraph (3) relating to fleet management and use of vehicles
22 from home to work. The Under Secretary shall use the tools and
23 plans when reviewing annual component requests for vehicle fleet
24 funding in accordance with paragraph (7).

25 (6) GUIDANCE TO DEVELOP FLEET MANAGEMENT PLANS.—The
26 Under Secretary for Management shall provide guidance, pursuant to
27 paragraph (2)(B) on how component heads may achieve optimal fleet
28 size in accordance with paragraph (5), including processes for the fol-
29 lowing:

30 (A) Leasing or acquiring additional vehicles or replacing exist-
31 ing vehicles, if determined necessary.

32 (B) Disposing of excess vehicles that the Under Secretary deter-
33 mines should not be reallocated under subparagraph (C).

34 (C) Reallocating excess vehicles to other components that may
35 need temporary or long-term use of additional vehicles.

36 (7) ANNUAL REVIEW OF VEHICLE FLEET FUNDING REQUESTS.—As
37 part of the annual budget process, the Under Secretary for Manage-
38 ment shall review and make determinations regarding annual compo-
39 nent requests for funding for vehicle fleets. If component heads have
40 not taken steps in furtherance of achieving optimal fleet size in the
41 prior fiscal year pursuant to paragraphs (5) and (6), the Under Sec-

1 retary shall provide rescission recommendations to the Committee on
2 Appropriations and the Committee on Homeland Security of the House
3 of Representatives and the Committee on Appropriations and the Com-
4 mittee on Homeland Security and Governmental Affairs of the Senate
5 regarding the component vehicle fleets.

6 (8) ACCOUNTABILITY FOR VEHICLE FLEET MANAGEMENT.—

7 (A) PROHIBITION ON VEHICLE LEASES, ACQUISITIONS, OR RE-
8 PLACEMENTS.—The Under Secretary for Management and compo-
9 nent heads may not approve in a fiscal year a vehicle lease, acqui-
10 sition, or replacement request if the component heads did not com-
11 ply in the prior fiscal year with paragraph (5).

12 (B) PROHIBITION ON PERFORMANCE COMPENSATION.—No De-
13 partment official with vehicle fleet management responsibilities
14 may receive annual performance compensation in pay in a fiscal
15 year if the official did not comply in the prior fiscal year with
16 paragraph (5).

17 (C) PROHIBITION ON CAR SERVICES.—No senior executive serv-
18 ice official of the Department whose office has a vehicle fleet may
19 receive access to a car service in a fiscal year if the official did
20 not comply in the prior fiscal year with paragraph (5).

21 (9) MOTOR POOL.—

22 (A) IN GENERAL.—The Under Secretary for Management may
23 determine the feasibility of operating a vehicle motor pool to per-
24 mit components to share vehicles as necessary to support mission
25 requirements to reduce the number of excess vehicles in the De-
26 partment.

27 (B) REQUIREMENTS.—The determination of feasibility of oper-
28 ating a vehicle motor pool under subparagraph (A) shall—

29 (i) include—

30 (I) regions in the United States in which multiple
31 components with vehicle fleets are located in proximity to
32 one another, or a significant number of employees with
33 authorization to use vehicles are located; and

34 (II) law enforcement vehicles;

35 (ii) cover the National Capital Region; and

36 (iii) take into account different mission requirements.

37 (C) REPORT.—The Secretary shall include in the Department's
38 next annual performance report required under current law the re-
39 sults of the determination under this paragraph.

40 (e) APPOINTMENT AND EVALUATION.—The Under Secretary for Manage-
41 ment—

1 (1) is appointed by the President, by and with the advice and con-
2 sent of the Senate, from among individuals who have—

3 (A) extensive executive level leadership and management experi-
4 ence in the public or private sector;

5 (B) strong leadership skills;

6 (C) a demonstrated ability to manage large and complex organi-
7 zations; and

8 (D) a proven record in achieving positive operational results;

9 (2) shall enter into an annual performance agreement with the Sec-
10 retary that shall set forth measurable individual and organizational
11 goals; and

12 (3) is subject to an annual performance evaluation by the Secretary,
13 who shall determine as part of each evaluation whether the Under Sec-
14 retary for Management has made satisfactory progress toward achiev-
15 ing the goals set out in the performance agreement required under
16 paragraph (2).

17 (f) SYSTEM FOR AWARD MANAGEMENT CONSULTATION.—The Under
18 Secretary for Management shall require that all Department contracting
19 and grant officials consult the System for Award Management (or successor
20 system) as maintained by the General Services Administration prior to
21 awarding a contract or grant or entering into other transactions to ascertain
22 whether the selected contractor is excluded from receiving Federal contracts,
23 certain subcontracts, and certain types of Federal financial and non-finan-
24 cial assistance and benefits.

25 (g) WORKFORCE HEALTH AND MEDICAL SUPPORT.—

26 (1) IN GENERAL.—The Under Secretary for Management shall be re-
27 sponsible for workforce-focused health and medical activities of the De-
28 partment. The Under Secretary for Management may further delegate
29 responsibility for those activities, as appropriate.

30 (2) RESPONSIBILITIES.—The Under Secretary for Management, in
31 coordination with the Chief Medical Officer, shall—

32 (A) provide oversight and coordinate the medical and health ac-
33 tivities of the Department for the human and animal personnel of
34 the Department;

35 (B) establish medical, health, veterinary, and occupational
36 health exposure policy, guidance, strategies, and initiatives for the
37 human and animal personnel of the Department;

38 (C) as considered appropriate by the Under Secretary for Man-
39 agement, provide medical liaisons to the components of the De-
40 partment, on a reimbursable basis, to provide subject matter ex-
41 pertise on occupational and public health issues;

1 (D) serve as the primary representative for the Department on
2 agreements regarding the detail of Commissioned Corps officers of
3 the Public Health Service of the Department of Health and
4 Human Services to the Department, except that components of the
5 Department shall retain authority for funding, determination of
6 specific duties, and supervision of the detailed Commissioned
7 Corps officers; and

8 (E) perform other duties relating to the responsibilities de-
9 scribed in this paragraph as the Secretary may require.

10 **§ 11702. Chief Financial Officer**

11 (a) IN GENERAL.—The Chief Financial Officer shall—

12 (1) perform functions as specified in chapter 9 of title 31; and

13 (2) report to the Under Secretary for Management with respect to
14 those functions described in paragraph (1) and other responsibilities
15 that may be assigned.

16 (b) PROGRAM ANALYSIS AND EVALUATION FUNCTION.—

17 (1) ESTABLISHMENT OF OFFICE OF PROGRAM ANALYSIS AND EVAL-
18 UATION.—The Secretary shall establish an Office of Program Analysis
19 and Evaluation (in this section referred to as the “Office”) in the De-
20 partment.

21 (2) RESPONSIBILITIES.—The Office shall—

22 (A) analyze and evaluate plans, programs, and budgets of the
23 Department in relation to United States homeland security objec-
24 tives, projected threats, vulnerability assessments, estimated costs,
25 resource constraints, and the most recent homeland security strat-
26 egy developed under section 10396(b)(2) of this title;

27 (B) develop and perform analyses and evaluations of alternative
28 plans, programs, personnel levels, and budget submissions for the
29 Department in relation to United States homeland security objec-
30 tives, projected threats, vulnerability assessments, estimated costs,
31 resource constraints, and the most recent homeland security strat-
32 egy developed under section 10396(b)(2) of this title;

33 (C) establish policies for, and oversee the integration of, the
34 planning, programming, and budgeting system of the Department;

35 (D) review and ensure that the Department meets performance-
36 based budget requirements established by the Office of Manage-
37 ment and Budget;

38 (E) provide guidance for, and oversee the development of, the
39 Future Years Homeland Security Program of the Department, as
40 specified under section 10396 of this title;

1 (F) ensure that the costs of Department programs, including
2 classified programs, are presented accurately and completely;

3 (G) oversee the preparation of the annual performance plan for
4 the Department and the program and performance section of the
5 annual report on program performance for the Department, con-
6 sistent with sections 1115 and 1116, respectively, of title 31;

7 (H) provide leadership in developing and promoting improved
8 analytical tools and methods for analyzing homeland security plan-
9 ning and the allocation of resources; and

10 (I) perform other responsibilities delegated by the Secretary
11 consistent with an effective program analysis and evaluation func-
12 tion.

13 (3) DIRECTOR OF PROGRAM ANALYSIS AND EVALUATION.—There is
14 a Director of Program Analysis and Evaluation. The Director—

15 (A) is a principal staff assistant to the Chief Financial Officer
16 of the Department for program analysis and evaluation; and

17 (B) shall report to an official no lower than the Chief Financial
18 Officer.

19 (4) REORGANIZATION.—

20 (A) IN GENERAL.—The Secretary may allocate or reallocate the
21 functions of the Office, or discontinue the Office, under section
22 10341(b)(1) of this title.

23 (B) EXEMPTION FROM LIMITATIONS.—Section 10341(b)(2) of
24 this title does not apply to an action by the Secretary under this
25 paragraph.

26 (c) NOTIFICATION REGARDING TRANSFER OR REPROGRAMMING OF
27 FUNDS.—In a case in which appropriations available to the Department or
28 an officer of the Department are transferred or reprogrammed and notice
29 of the transfer or reprogramming is submitted to Congress (including an
30 officer, office, or committee of Congress), the Chief Financial Officer shall
31 simultaneously submit the notice to the Committee on Homeland Security
32 and the Committee on Oversight and Government Reform of the House of
33 Representatives, and to the Committee on Homeland Security and Govern-
34 mental Affairs of the Senate.

35 **§ 11703. Chief Information Officer**

36 (a) IN GENERAL.—The Chief Information Officer shall report to the Sec-
37 retary, or to another official of the Department, as the Secretary may di-
38 rect.

39 (b) GEOSPATIAL INFORMATION FUNCTIONS.—

40 (1) DEFINITIONS.—In this subsection:

1 (A) GEOSPATIAL INFORMATION.—The term “geospatial infor-
2 mation” means graphical or digital data depicting natural or man-
3 made physical features, phenomena, or boundaries of the earth
4 and information related thereto, including surveys, maps, charts,
5 remote sensing data, and images.

6 (B) GEOSPATIAL TECHNOLOGY.—The term “geospatial tech-
7 nology” means technology utilized by analysts, specialists, sur-
8 veyors, photogrammetrists, hydrographers, geodesists, cartog-
9 raphers, architects, or engineers for the collection, storage, re-
10 trieval, or dissemination of geospatial information, including—

- 11 (i) global satellite surveillance systems;
- 12 (ii) global position systems;
- 13 (iii) geographic information systems;
- 14 (iv) mapping equipment;
- 15 (v) geocoding technology; and
- 16 (vi) remote sensing devices.

17 (2) OFFICE OF GEOSPATIAL MANAGEMENT.—

18 (A) ESTABLISHMENT.—There is in the Office of the Chief In-
19 formation Officer the Office of Geospatial Management.

20 (B) GEOSPATIAL INFORMATION OFFICER.—

21 (i) IN GENERAL.—The Geospatial Information Officer ad-
22 ministers the Office of Geospatial Management. The
23 Geospatial Information Officer is appointed by the Secretary.
24 The Geospatial Information Officer serves under the direction
25 of the Chief Information Officer.

26 (ii) ASSISTS CHIEF INFORMATION OFFICER.—The
27 Geospatial Information Officer assists the Chief Information
28 Officer in carrying out all functions under this section and in
29 coordinating the geospatial information needs of the Depart-
30 ment.

31 (C) COORDINATION OF GEOSPATIAL INFORMATION.—The Chief
32 Information Officer shall establish and carry out a program to
33 provide for the efficient use of geospatial information, which shall
34 include—

- 35 (i) providing necessary geospatial information to implement
36 the critical infrastructure protection programs;
- 37 (ii) providing leadership and coordination in meeting the
38 geospatial information requirements of those responsible for
39 planning, prevention, mitigation, assessment, and response to
40 emergencies, critical infrastructure protection, and other
41 functions of the Department; and

1 (iii) coordinating with users of geospatial information with-
2 in the Department to ensure interoperability and prevent un-
3 necessary duplication.

4 (D) RESPONSIBILITIES.—In carrying out this subsection, the
5 responsibilities of the Chief Information Officer include—

6 (i) coordinating the geospatial information needs and ac-
7 tivities of the Department;

8 (ii) implementing standards, as adopted by the Director of
9 the Office of Management and Budget under the processes
10 established under section 216 of the E-Government Act of
11 2002 (Public Law 107-347, 44 U.S.C. 3501 note), to facili-
12 tate the interoperability of geospatial information pertaining
13 to homeland security among all users of the information in—

14 (I) the Department;

15 (II) State and local government; and

16 (III) the private sector;

17 (iii) coordinating with the Federal Geographic Data Com-
18 mittee and carrying out the responsibilities of the Department
19 pursuant to Office of Management and Budget Circular A-16
20 and Executive Order 12906 (59 Fed. Reg. 17671, 43 U.S.C.
21 1457 note); and

22 (iv) making recommendations to the Secretary and the Ex-
23 ecutive Director of the Office for State and Local Government
24 Coordination and Preparedness on awarding grants to—

25 (I) fund the creation of geospatial data; and

26 (II) execute information sharing agreements regarding
27 geospatial data with State, local, and tribal governments.

28 **§ 11704. Chief Human Capital Officer**

29 (a) REPORTING AUTHORITY.—The Chief Human Capital Officer of the
30 Department shall report directly to the Under Secretary for Management.

31 (b) RESPONSIBILITIES.—In addition to the responsibilities set forth in
32 chapter 14 of title 5 and other applicable law, the Chief Human Capital Of-
33 ficer of the Department shall—

34 (1) develop and implement strategic workforce planning policies, in-
35 cluding with respect to leader development and employee engagement,
36 that are consistent with Government-wide leading principles, in line
37 with Department strategic human capital goals and priorities, and in-
38 formed by best practices within the Federal Government and the pri-
39 vate sector, taking into account the special requirements of members of
40 the armed forces serving in the Coast Guard;

1 (2) use performance measures to evaluate, on an ongoing
2 basis, Department-wide strategic workforce planning efforts;

3 (3) develop, improve, and implement policies that, to the extent prac-
4 ticable, are informed by employee feedback, including compensation
5 flexibilities available to Federal agencies where appropriate, to recruit,
6 hire, train, and retain the workforce of the Department, in coordination
7 with all components of the Department;

8 (4) identify methods for managing and overseeing human capital
9 programs and initiatives, including leader development and employee
10 engagement programs, in coordination with the head of each compo-
11 nent of the Department;

12 (5) develop a career path framework and create opportunities for
13 leader development in coordination with all components of the Depart-
14 ment that is informed by an assessment, carried out by the Chief
15 Human Capital Officer, of the learning and developmental needs of em-
16 ployees in supervisory and nonsupervisory roles across the Department
17 and appropriate workforce planning initiatives;

18 (6) lead the efforts of the Department for managing employee re-
19 sources, including training and development opportunities, in coordina-
20 tion with each component of the Department;

21 (7) work to ensure the Department is implementing human capital
22 programs and initiatives and effectively educating each component of
23 the Department about these programs and initiatives;

24 (8) identify and eliminate unnecessary and duplicative human capital
25 policies and guidance;

26 (9) maintain a catalogue of available employee development opportu-
27 nities, including the Homeland Security Rotation Program pursuant
28 to section 10366 of this title, departmental leadership development pro-
29 grams, interagency development programs, and other rotational pro-
30 grams;

31 (10) ensure that employee discipline and adverse action programs
32 comply with the requirements of all pertinent laws, rules, regulations,
33 and Federal guidance, and ensure due process for employees;

34 (11) analyze each Department or Government-wide Federal work-
35 force satisfaction or morale survey not later than 90 days after the
36 date of the publication of each survey and submit to the Secretary
37 analysis, including, as appropriate, recommendations to improve work-
38 force satisfaction or morale in the Department;

39 (12) review and approve all component employee engagement action
40 plans to ensure the plans include initiatives responsive to the root cause

1 of employee engagement challenges, as well as outcome-based perform-
2 ance measures and targets to track the progress of the initiatives;

3 (13) provide input concerning the hiring and performance of the
4 Chief Human Capital Officer or comparable official in each component
5 of the Department; and

6 (14) ensure that all employees of the Department are informed of
7 their rights and remedies under chapters 12 and 23 of title 5.

8 (c) COMPONENT STRATEGIES.—

9 (1) IN GENERAL.—Each component of the Department shall, in co-
10 ordination with the Chief Human Capital Officer of the Department,
11 develop a 5-year workforce strategy for the component that will support
12 the goals, objectives, and performance measures of the Department for
13 determining the proper balance of Federal employees and private labor
14 resources.

15 (2) STRATEGY REQUIREMENTS.—In developing the strategy required
16 under paragraph (1), each component shall consider the effect on
17 human resources associated with creating additional Federal full-time
18 equivalent positions, converting private contractors to Federal employ-
19 ees, or relying on the private sector for goods and services.

20 (d) CHIEF LEARNING AND ENGAGEMENT OFFICER.—The Chief Human
21 Capital Officer may designate an employee of the Department to serve as
22 a Chief Learning and Engagement Officer to assist the Chief Human Cap-
23 ital Officer in carrying out this section.

24 (e) ANNUAL SUBMISSION.—Not later than 90 days after the date on
25 which the Secretary submits the annual budget justification for the Depart-
26 ment, the Secretary shall submit to the congressional homeland security
27 committees a report that includes a table, delineated by component with ac-
28 tual and enacted amounts, including—

29 (1) information on the progress in the Department of fulfilling the
30 workforce strategies developed under subsection (c);

31 (2) information on employee development opportunities catalogued
32 pursuant to subsection (b)(9) and any available data on participation
33 rates, attrition rates, and impacts on retention and employee satisfac-
34 tion;

35 (3) information on the progress of Departmentwide strategic work-
36 force planning efforts as determined under subsection (b)(2);

37 (4) information on the activities of the steering committee estab-
38 lished pursuant to section 11710(a) of this title, including the number
39 of meetings, types of materials developed and distributed, and rec-
40 ommendations made to the Secretary;

1 (5) the number of on-board staffing for Federal employees from the
2 prior fiscal year;

3 (6) the total contract hours submitted by each prime contractor as
4 part of the service contract inventory required under section 743 of the
5 Financial Services and General Government Appropriations Act, 2010
6 (Public Law 111–117, div. C, 31 U.S.C. 501 note); and

7 (7) the number of full-time equivalent personnel identified under the
8 Intergovernmental Personnel Act of 1970 (42 U.S.C. 4701 et seq.).

9 (f) LIMITATION.—Nothing in this section overrides or otherwise affects
10 the requirements specified in section 10312 of this title.

11 **§ 11705. Officer for Civil Rights and Civil Liberties**

12 (a) IN GENERAL.—The Officer for Civil Rights and Civil Liberties, who
13 shall report directly to the Secretary, shall—

14 (1) review and assess information concerning abuses of civil rights,
15 civil liberties, and profiling on the basis of race, ethnicity, or religion,
16 by employees and officials of the Department;

17 (2) make public through the Internet, radio, television, or newspaper
18 advertisements information on the responsibilities and functions of, and
19 how to contact, the Officer;

20 (3) assist the Secretary, directorates, and offices of the Department
21 to develop, implement, and periodically review Department policies and
22 procedures to ensure that the protection of civil rights and civil liberties
23 is appropriately incorporated into Department programs and activities;

24 (4) oversee compliance with constitutional, statutory, regulatory, pol-
25 icy, and other requirements relating to the civil rights and civil liberties
26 of individuals affected by the programs and activities of the Depart-
27 ment;

28 (5) coordinate with the Privacy Officer to ensure that—

29 (A) programs, policies, and procedures involving civil rights,
30 civil liberties, and privacy considerations are addressed in an inte-
31 grated and comprehensive manner; and

32 (B) Congress receives appropriate reports regarding the pro-
33 grams, policies, and procedures; and

34 (6) investigate complaints and information indicating possible abuses
35 of civil rights or civil liberties, unless the Inspector General of the De-
36 partment determines that the complaint or information should be inves-
37 tigated by the Inspector General.

38 (b) REPORT.—The Secretary shall submit to the President of the Senate,
39 the Speaker of the House of Representatives, and the appropriate commit-
40 tees and subcommittees of Congress on an annual basis a report—

1 (1) on the implementation of this section, including the use of funds
2 appropriated to carry out this section; and

3 (2) detailing allegations of abuses described under subsection (a)(1)
4 and actions taken by the Department in response to the allegations.

5 **§ 11706. Quadrennial homeland security review**

6 (a) REQUIREMENT.—

7 (1) QUADRENNIAL REVIEWS REQUIRED.—In fiscal year 2025, and
8 every 4 years thereafter, the Secretary shall conduct a review of the
9 homeland security of the Nation (in this section referred to as a “quad-
10 rennial homeland security review”).

11 (2) SCOPE OF REVIEW.—Each quadrennial homeland security review
12 shall be a comprehensive examination of the homeland security strategy
13 of the Nation, including recommendations regarding the long-term
14 strategy and priorities of the Nation for homeland security and guid-
15 ance on the programs, assets, capabilities, budget, policies, and authori-
16 ties of the Department.

17 (3) CONSULTATION.—The Secretary shall conduct each quadrennial
18 homeland security review under this subsection in consultation with—

19 (A) the heads of other Federal agencies, including the Attorney
20 General, the Secretary of State, the Secretary of Defense, the Sec-
21 retary of Health and Human Services, the Secretary of the Treas-
22 ury, the Secretary of Agriculture, the Secretary of Energy, and
23 the Director of National Intelligence;

24 (B) key officials of the Department, including the Under Sec-
25 retary for Strategy, Policy, and Plans;

26 (C) representatives from appropriation advisory committees es-
27 tablished pursuant to section 10391 of this title, including the
28 Homeland Security Advisory Council and the Homeland Security
29 Science and Technology Advisory Council, or otherwise estab-
30 lished, including the Aviation Security Advisory Committee estab-
31 lished pursuant to section 40963 of this title; and

32 (D) other relevant governmental and nongovernmental entities,
33 including State, local, and tribal government officials, members of
34 Congress, private-sector representatives, academics, and other pol-
35 icy experts.

36 (4) RELATIONSHIP WITH FUTURE YEARS HOMELAND SECURITY PRO-
37 GRAM.—The Secretary shall ensure that each review conducted under
38 this section is coordinated with the Future Years Homeland Security
39 Program required under section 10396 of this title.

40 (b) CONTENTS OF REVIEW.—In each quadrennial homeland security re-
41 view, the Secretary shall—

1 (1) delineate and update, as appropriate, the national homeland se-
2 curity strategy, consistent with appropriate national and Department
3 strategies, strategic plans, and Homeland Security Presidential Direc-
4 tives, including the National Strategy for Homeland Security, the Na-
5 tional Response Plan, and the Department Security Strategic Plan;

6 (2) outline and prioritize the full range of the critical homeland secu-
7 rity mission areas of the Nation, based on the risk assessment required
8 pursuant to subsection (e)(2)(B);

9 (3) describe, to the extent practicable, the interagency cooperation,
10 preparedness of Federal response assets, infrastructure, resources re-
11 quired, and other elements of the homeland security program and poli-
12 cies of the Nation associated with the national homeland security strat-
13 egy, required to execute successfully the full range of missions called
14 for in the national homeland security strategy described in paragraph
15 (1) and the homeland security mission areas outlined under paragraph
16 (2);

17 (4) identify, to the extent practicable, resources required to execute
18 the full range of missions called for in the national homeland security
19 strategy described in paragraph (1) and the homeland security mission
20 areas outlined under paragraph (2), including any resources identified
21 from redundant, wasteful, or unnecessary capabilities or capacities that
22 may be redirected to better support other existing capabilities or capac-
23 ities, as the case may be; and

24 (5) include an assessment of the organizational alignment of the De-
25 partment with the national homeland security strategy referred to in
26 paragraph (1) and the homeland security mission areas outlined under
27 paragraph (2).

28 (e) REPORTING.—

29 (1) IN GENERAL.—Not later than 60 days after the date of the
30 President's budget for the fiscal year after the fiscal year in which a
31 quadrennial homeland security review is conducted, the Secretary shall
32 submit to Congress a report regarding that quadrennial homeland secu-
33 rity review.

34 (2) CONTENTS OF REPORT.—Each report submitted under para-
35 graph (1) shall include—

36 (A) the results of the quadrennial homeland security review;

37 (B) a risk assessment of the assumed or defined national home-
38 land security interests of the Nation that were examined for the
39 purposes of that review or for purposes of the quadrennial EMP
40 and GMD risk assessment under section 10918(d)(2)(E) of this
41 title;

1 (C) the national homeland security strategy, including a
2 prioritized list of the critical homeland security missions of the
3 Nation, as required under subsection (b)(2);

4 (D) to the extent practicable, a description of the interagency
5 cooperation, preparedness of Federal response assets, infrastruc-
6 ture, resources required, and other elements of the homeland secu-
7 rity program and policies of the Nation associated with the na-
8 tional homeland security strategy, required to execute successfully
9 the full range of missions called for in the applicable national
10 homeland security strategy referred to in subsection (b)(1) and the
11 homeland security mission areas outlined under subsection (b)(2);

12 (E) an assessment of the organizational alignment of the De-
13 partment with the applicable national homeland security strategy
14 referred to in subsection (b)(1) and the homeland security mission
15 areas outlined under subsection (b)(2), including the Department's
16 organizational structure, management systems, budget and ac-
17 counting systems, human resources systems, procurement systems,
18 and physical and technical infrastructure;

19 (F) to the extent practicable, a discussion of cooperation among
20 Federal agencies in the effort to promote national homeland secu-
21 rity;

22 (G) to the extent practicable, a discussion of cooperation be-
23 tween the Federal Government and State, local, and tribal govern-
24 ments in preventing terrorist attacks and preparing for emergency
25 response to threats and risks to national homeland security; and

26 (H) any other matter the Secretary considers appropriate.

27 (3) DOCUMENTATION.—The Secretary shall retain and on request
28 provided to Congress the following documentation regarding each quad-
29 rennial homeland security review:

30 (A) Records regarding the consultation carried out pursuant to
31 subsection (a)(3), including the following:

32 (i) All written communications, including communications
33 sent out by the Secretary and feedback submitted to the Sec-
34 retary through technology, online communications tools, in-
35 person discussions, and the interagency process.

36 (ii) Information on how feedback received by the Secretary
37 informed each quadrennial homeland security review.

38 (B) Information regarding the risk assessment required pursu-
39 ant subsection (c)(2)(B), including the following:

40 (i) The risk model utilized to generate the risk assessment.

1 (ii) Information, including data used in the risk model uti-
2 lized to generate the risk assessment.

3 (iii) Sources of information, including other risk assess-
4 ments, utilized to generate the risk assessment.

5 (iv) Information on assumptions, weighing factors, and subjec-
6 tive judgments utilized to generate the risk assessment, together
7 with information on the rationale or basis of the assumptions,
8 weighing factors, and subjective judgments.

9 (4) PUBLIC AVAILABILITY.—The Secretary shall, consistent with the
10 protection of national security and other sensitive matters, make each
11 report submitted under paragraph (1) publicly available on the Internet
12 website of the Department.

13 (d) REVIEW.—Not later than 90 days after the submission of each report
14 required under subsection (c)(1), the Secretary shall provide to the Com-
15 mittee on Homeland Security of the House of Representatives and the Com-
16 mittee on Homeland Security and Governmental Affairs of the Senate infor-
17 mation on the degree to which the findings and recommendations developed
18 in the quadrennial homeland security review that is the subject of the report
19 were integrated into the acquisition strategy and expenditure plans for the
20 Department.

21 **§ 11707. Interoperable communications**

22 (a) DEFINITION OF INTEROPERABLE COMMUNICATIONS.—The term
23 “interoperable communications” has the same meaning given that term in
24 section 10912(a) of this title.

25 (b) APPLICATION.—Subsections (c) through (e) shall apply only with re-
26 spect to the interoperable communications capabilities in the Department
27 and components of the Department to communicate with the Department.

28 (c) STRATEGY FOR ACHIEVING AND MAINTAINING INTEROPERABLE COM-
29 MUNICATIONS AMONG THE COMPONENTS OF THE DEPARTMENT.—The
30 Under Secretary for Management shall submit to the Committee on Home-
31 land Security of the House of Representatives and the Committee on Home-
32 land Security and Governmental Affairs of the Senate a strategy, which
33 shall be updated as necessary, for achieving and sustaining interoperable
34 communications among the components of the Department, including for
35 daily operations, planned events, and emergencies, with corresponding mile-
36 stones, that includes the following:

37 (1) An assessment of interoperability gaps in radio communications
38 among the components of the Department, as of July 6, 2015.

39 (2) Information on efforts and activities, including current and
40 planned policies, directives, and training, of the Department since No-
41 vember 1, 2012, to achieve and maintain interoperable communications

1 among the components of the Department, and planned efforts and ac-
2 tivities of the Department to achieve and maintain the interoperable
3 communications.

4 (3) An assessment of obstacles and challenges to achieving and
5 maintaining interoperable communications among the components of
6 the Department.

7 (4) Information on, and an assessment of, the adequacy of mecha-
8 nisms available to the Under Secretary for Management to enforce and
9 compel compliance with interoperable communications policies and di-
10 rectives of the Department.

11 (5) Guidance provided to the components of the Department to im-
12 plement interoperable communications policies and directives of the De-
13 partment.

14 (6) The total amount of funds expended by the Department since
15 November 1, 2012, and projected future expenditures, to achieve inter-
16 operable communications, including on equipment, infrastructure, and
17 maintenance.

18 (7) Dates on which Department-wide interoperability is projected to
19 be achieved for voice, data, and video communications, respectively, and
20 interim milestones that correspond to the achievement of each of those
21 modes of communications.

22 (d) SUPPLEMENTARY MATERIAL.—Together with the strategy required
23 under subsection (c), the Under Secretary for Management shall submit to
24 the Committee on Homeland Security of the House of Representatives and
25 the Committee on Homeland Security and Governmental Affairs of the Sen-
26 ate information on—

27 (1) any intra-agency effort or task force that has been delegated cer-
28 tain responsibilities by the Under Secretary for Management relating
29 to achieving and maintaining interoperable communications among the
30 components of the Department by the dates referred to in subsection
31 (c)(7); and

32 (2) who in each component is responsible for implementing policies
33 and directives issued by the Under Secretary for Management to
34 achieve and maintain the interoperable communications.

35 (e) REPORT.—Not later than 100 days after the date on which the strat-
36 egy required under subsection (c) is submitted, and every 2 years afterwards
37 for 6 years, the Under Secretary for Management shall submit to the Com-
38 mittee on Homeland Security of the House of Representatives and the Com-
39 mittee on Homeland Security and Governmental Affairs of the Senate a re-
40 port on the status of efforts to implement the strategy required under sub-
41 section (c), including the following:

1 (1) Progress on each interim milestone referred to in subsection
2 (e)(7) toward achieving and maintaining interoperable communications
3 among the components of the Department.

4 (2) Information on any policies, directives, guidance, and training es-
5 tablished by the Under Secretary for Management.

6 (3) An assessment of the level of compliance, adoption, and partici-
7 pation among the components of the Department with the policies, di-
8 rectives, guidance, and training established by the Under Secretary for
9 Management to achieve and maintain interoperable communications
10 among the components.

11 (4) Information on any additional resources or authorities needed by
12 the Under Secretary for Management.

13 **§ 11708. Joint Task Forces**

14 (a) DEFINITION OF SITUATIONAL AWARENESS.—In this section, the term
15 “situational awareness” means knowledge and unified understanding of un-
16 lawful cross-border activity, including—

17 (1) threats and trends concerning illicit trafficking and unlawful
18 crossings;

19 (2) the ability to forecast future shifts in the threats and trends;

20 (3) the ability to evaluate the threats and trends at a level sufficient
21 to create actionable plans; and

22 (4) the operational capability to conduct continuous and integrated
23 surveillance of the air, land, and maritime borders of the United
24 States.

25 (b) ESTABLISHMENT.—The Secretary may establish and operate depart-
26 mental Joint Task Forces to conduct joint operations using personnel and
27 capabilities of the Department for the purposes specified in subsection (d).

28 (c) DIRECTOR, DEPUTY DIRECTOR, AND STAFF.—

29 (1) DIRECTOR.—

30 (A) APPOINTMENT.—Each Joint Task Force shall be headed by
31 a Director, appointed by the President, for a term of not more
32 than 2 years. The Secretary shall submit to the President rec-
33 ommendations for the appointment after consulting with the heads
34 of the components of the Department with membership on any
35 Joint Task Force. A Director shall be—

36 (i) a current senior official of the Department with not less
37 than 1 year of significant leadership experience at the De-
38 partment; or

39 (ii) if no suitable candidate is available at the Department,
40 an individual with—

1 (I) not less than 1 year of significant leadership experi-
2 ence in a Federal agency since the establishment of the
3 Department; and

4 (II) a demonstrated ability in, knowledge of, and sig-
5 nificant experience working on, the issues to be ad-
6 dressed by the Joint Task Force.

7 (B) EXTENSION.—The Secretary may extend the appointment
8 of a Director of a Joint Task Force for not more than 2 years
9 if the Secretary determines that the extension is in the best inter-
10 est of the Department.

11 (2) DEPUTY DIRECTOR.—For each Joint Task Force, the Secretary
12 shall appoint a Deputy Director, who shall be an official of a different
13 component or office of the Department than the Director.

14 (3) STAFF.—

15 (A) IN GENERAL.—Each Joint Task Force shall have a staff,
16 composed of personnel from relevant components and offices of the
17 Department, to assist the Director in carrying out the mission and
18 responsibilities of the Joint Task Force.

19 (B) INFORMATION TO BE INCLUDED IN REPORT.—The Sec-
20 retary shall include in the report submitted under subsection
21 (f)(6)—

22 (i) the number of personnel of each component or office
23 permanently assigned to each Joint Task force; and

24 (ii) the number of personnel of each component or office
25 assigned on a temporary basis to each Joint Task Force

26 (d) PURPOSES.—

27 (1) IN GENERAL.—Subject to paragraph (2), the purposes referred
28 to in subsection (b) are or relate to the following:

29 (A) Securing the land and maritime borders of the United
30 States.

31 (B) Addressing homeland security crises.

32 (C) Establishing regionally based operations.

33 (2) LIMITATION.—

34 (A) IN GENERAL.—The Secretary may not establish a Joint
35 Task Force for any major disaster or emergency declared under
36 the Robert T. Stafford Disaster Relief and Emergency Assistance
37 Act (42 U.S.C. 5121 et seq.) or an incident for which the Federal
38 Emergency Management Agency has primary responsibility for
39 management of the response under chapter 113 of this title, in-
40 cluding section 11303(a)(3)(A), unless the responsibilities of the
41 Joint Task Force—

1 (i) do not include operational functions relating to incident
2 management, including coordination of operations; and

3 (ii) are consistent with the requirements of paragraphs (1)
4 and (2)(A) of section 11302(b) and section 11309 of this title
5 and section 302 of the Robert T. Stafford Disaster Relief and
6 Emergency Assistance Act (42 U.S.C. 5143).

7 (B) RESPONSIBILITIES AND FUNCTIONS OF AGENCY AND AD-
8 MINISTRATOR NOT REDUCED.—Nothing in this section may be
9 construed to reduce the responsibilities or functions of the Federal
10 Emergency Management Agency or the Administrator of the Fed-
11 eral Emergency Management Agency under chapter 111 of this
12 title or any other provision of law, including the diversion of an
13 asset, function, or mission from the Federal Emergency Manage-
14 ment Agency or the Administrator of the Federal Emergency
15 Management Agency pursuant to section 11306 of this title.

16 (e) RESPONSIBILITIES.—The Director of a Joint Task Force, subject to
17 the oversight, direction, and guidance of the Secretary, shall—

18 (1) when the Joint Task Force is established for the purpose re-
19 ferred to in subsection (d)(1)(A), maintain situational awareness in the
20 areas of responsibility of the Joint Task Force, as determined by the
21 Secretary;

22 (2) provide operational plans and requirements for standard oper-
23 ating procedures and contingency operations in the areas of responsi-
24 bility of the Joint Task Force, as determined by the Secretary;

25 (3) plan and execute joint task force activities in the areas of respon-
26 sibility of the Joint Task Force, as determined by the Secretary;

27 (4) set and accomplish strategic objectives through integrated oper-
28 ational planning and execution;

29 (5) exercise operational direction over personnel and equipment from
30 components and offices of the Department allocated to the Joint Task
31 Force to accomplish the objectives of the Joint Task Force;

32 (6) when the Joint Task Force is established for the purpose re-
33 ferred to in subsection (d)(1)(A), establish operational and investigative
34 priorities in the areas of responsibility of the Joint Task Force, as de-
35 termined by the Secretary;

36 (7) coordinate with foreign governments and other Federal, State,
37 and local agencies, as appropriate, to carry out the mission of the Joint
38 Task Force; and

39 (8) carry out other duties and powers the Secretary determines ap-
40 propriate.

41 (f) PERSONNEL AND RESOURCES.—

1 (1) TEMPORARY ALLOCATION.—The Secretary, on request of the Di-
2 rector of a Joint Task Force and giving appropriate consideration of
3 risk to the other primary missions of the Department, may allocate to
4 the Joint Task Force on a temporary basis personnel and equipment
5 of components and offices of the Department.

6 (2) COST NEUTRALITY.—A Joint Task Force may not require more
7 resources than would have otherwise been required by the Department
8 to carry out the duties assigned to the Joint Task Force if the Joint
9 Task Force had not been established.

10 (3) LOCATION OF OPERATIONS.—In establishing a location of oper-
11 ations for a Joint Task Force, the Secretary shall, to the extent prac-
12 ticable, use existing facilities that integrate efforts of components of
13 the Department and State, local, tribal, or territorial law enforcement
14 or military entities.

15 (4) CONSIDERATION OF IMPACT.—When reviewing requests for allo-
16 cation of component personnel and equipment under paragraph (1), the
17 Secretary shall consider the impact of the allocation on the ability of
18 the donating component or office to carry out the primary missions of
19 the Department, and in the case of the Coast Guard, the missions spec-
20 ified in section 10312 of this title.

21 (5) LIMITATION.—Personnel and equipment of the Coast Guard allo-
22 cated under this subsection may be used only to carry out operations
23 and investigations relating to the missions specified in section 10312
24 of this title.

25 (6) REPORT.—The Secretary, at the time the budget of the Presi-
26 dent for a fiscal year is submitted to Congress under section 1105(a)
27 of title 31, shall submit to the Committee on Homeland Security and
28 the Committee on Transportation and Infrastructure of the House of
29 Representatives and the Committee on Homeland Security and Govern-
30 mental Affairs and the Committee on Commerce, Science, and Trans-
31 portation of the Senate a report on the total funding, personnel, and
32 other resources that each component or office of the Department allo-
33 cated under this subsection to each Joint Task Force to carry out the
34 mission of the Joint Task Force during the fiscal year immediately pre-
35 ceding each report, and a description of the degree to which the re-
36 sources drawn from each component or office impact the primary mis-
37 sion of the component or office.

38 (g) COMPONENT RESOURCE AUTHORITY.—As directed by the Secretary—

39 (1) each Director of a Joint Task Force shall be provided sufficient
40 resources from relevant components and offices of the Department and

1 the authority necessary to carry out the missions and responsibilities
2 of the Joint Task Force required under this section;

3 (2) the resources referred to in paragraph (1) shall be under the
4 operational authority, direction, and control of the Director of the Joint
5 Task Force to which the resources are assigned; and

6 (3) the personnel and equipment of each Joint Task Force shall re-
7 main under the administrative direction of the head of the component
8 or office of the Department that provided the personnel or equipment.

9 (h) MISSION; ESTABLISHMENT OF PERFORMANCE METRICS.—The Sec-
10 retary shall—

11 (1) using leading practices in performance management and lessons
12 learned by other law enforcement task forces and joint operations, es-
13 tablish—

14 (A) the mission, strategic goals, and objectives of each Joint
15 Task Force;

16 (B) the criteria for terminating each Joint Task Force; and

17 (C) outcome-based and other appropriate performance metrics
18 for evaluating the effectiveness of each Joint Task Force with re-
19 spect to the mission, strategic goals, and objectives established
20 pursuant to subparagraph (A), including—

21 (i) targets for each Joint Task Force to achieve by not
22 later than 1 and 3 years after the establishment under this
23 paragraph; and

24 (ii) a description of the methodology used to establish the
25 metrics.

26 (2) not later than 120 days after December 23, 2022, and 120 days
27 after the establishment of a new Joint Task Force, as appropriate, sub-
28 mit to the Committee on Homeland Security and the Committee on
29 Transportation and Infrastructure of the House of Representatives and
30 the Committee on Homeland Security and Governmental Affairs and
31 the Committee on Commerce, Science, and Transportation of the Sen-
32 ate the mission, strategic goals, objectives, and metrics established
33 under paragraph (1); and

34 (3) not later than December 23, 2023, and annually thereafter, sub-
35 mit to the committees specified in paragraph (2) a report that contains
36 information on the progress in implementing the outcome-based and
37 other appropriate performance metrics established pursuant to para-
38 graph (1)(C).

39 (i) JOINT DUTY TRAINING PROGRAM.—

40 (1) IN GENERAL.—The Secretary shall—

1 (A) establish a joint duty training program in the Department
2 for the purposes of—

- 3 (i) enhancing coordination in the Department; and
4 (ii) promoting workforce professional development; and

5 (B) tailor the joint duty training program to improve joint oper-
6 ations as part of the Joint Task Forces.

7 (2) ELEMENTS.—The joint duty training program established under
8 paragraph (1) shall address, at a minimum, the following topics:

- 9 (A) National security strategy.
10 (B) Strategic and contingency planning.
11 (C) Command and control of operations under joint command.
12 (D) International engagement.
13 (E) The homeland security enterprise.
14 (F) Interagency collaboration.
15 (G) Leadership.
16 (H) Specific subject matters relevant to the Joint Task Force,
17 including matters relating to the missions specified in section
18 10312 of this title, to which the joint duty training program is as-
19 signed.

20 (3) TRAINING REQUIRED.—

21 (A) DIRECTORS AND DEPUTY DIRECTORS.—Except as provided
22 in subparagraphs (C) and (D), an individual shall complete the
23 joint duty training program before being appointed Director or
24 Deputy Director of a Joint Task Force.

25 (B) STAFF.—Each official serving on the staff of a Joint Task
26 Force shall complete the joint duty training program in the 1st
27 year of assignment to the Joint Task Force.

28 (C) EXCEPTION.—Subparagraph (A) does not apply to the 1st
29 Director or Deputy Director appointed to a Joint Task Force on
30 or after December 23, 2016.

31 (D) WAIVER.—The Secretary may waive the application of sub-
32 paragraph (A) if the Secretary determines that the waiver is in
33 the interest of homeland security or necessary to carry out the
34 mission for which a Joint Task Force was established.

35 (j) NOTIFICATION OF JOINT TASK FORCE FORMATION OR TERMI-
36 NATION.—

37 (1) IN GENERAL.—Not later than 7 days after establishing or termi-
38 nating a Joint Task Force under this section, the Secretary shall sub-
39 mit to the majority leader of the Senate, the minority leader of the
40 Senate, The Speaker of the House of Representatives, the majority
41 leader of the House of Representatives, the minority leader of the

1 House of Representatives, the Committee on Homeland Security and
2 the Committee on Transportation and Infrastructure of the House of
3 Representatives, and the Committee on Homeland Security and Gov-
4 ernmental Affairs and the Committee on Commerce, Science, and
5 Transportation of the Senate a notification regarding the establishment
6 or termination. The contents of the notification shall include the fol-
7 lowing:

8 (A) The criteria and conditions required to establish or termi-
9 nate the Joint Task Force at issue.

10 (B) The primary mission, strategic goals, objectives, and plan
11 of operations of the Joint Task Force.

12 (C) If the notification is a notification of termination, informa-
13 tion on the effectiveness of the Joint Task Force as measured by
14 the outcome-based performance metrics and other appropriate per-
15 formance metrics established pursuant to subsection (h)(1)(C).

16 (D) The funding and resources required to establish or termi-
17 nate the Joint Task Force.

18 (E) The number of personnel of each component or office per-
19 manently assigned to the Joint Task Force.

20 (F) The number of personnel of each component and office as-
21 signed on a temporary basis to the Joint Task Force.

22 (G) If the notification is a notification of establishment, the an-
23 ticipated costs of establishing and operating the Joint Task Force.

24 (H) If the notification is a notification of termination, funding
25 allocated in the immediately preceding fiscal year to the Joint
26 Task Force for—

27 (i) operations, notwithstanding the termination; and

28 (ii) activities associated with the termination.

29 (I) The anticipated establishment or actual termination date of
30 the Joint Task Force, as the case may be.

31 (2) WAIVER AUTHORITY.—The Secretary may waive the requirement
32 under paragraph (1) in the event of an emergency circumstance that
33 imminently threatens the protection of human life or property.

34 (k) REVIEW.—Not later than December 23, 2023, the Comptroller Gen-
35 eral shall submit to the Committee on Homeland Security and the Com-
36 mittee on Transportation and Infrastructure of the House of Representa-
37 tives and the Committee on Homeland Security and Governmental Affairs
38 and the Committee on Commerce, Science, and Transportation of the Sen-
39 ate an assessment of the effectiveness of the Secretary's utilization of the
40 authority provided under this section for the purposes specified in sub-
41 section (d) as among the range of options available to the Secretary to con-

1 duct joint operations among department components and offices and a re-
2 view of the Joint Task Forces established under this section. The review
3 shall include—

4 (1) an assessment of methodology utilized to determine whether to
5 establish or determine each Joint Task Force; and

6 (2) an assessment of the effectiveness of oversight over each Joint
7 Task Force, with specificity regarding the Secretary's utilization of out-
8 come-based or other appropriate performance metrics (established pur-
9 suant to subsection (h)(1)(C)) to evaluate the effectiveness of each
10 Joint Task Force in measuring progress with respect to the mission,
11 strategic goals, and objectives (established pursuant to subsection
12 (h)(1)(A)) of the Joint Task Force.

13 (l) JOINT DUTY ASSIGNMENT PROGRAM.—After establishing the joint
14 duty training program under subsection (i), the Secretary shall establish a
15 joint duty assignment program in the Department for the purposes of en-
16 hancing coordination in the Department and promoting workforce profes-
17 sional development.

18 (m) SUNSET.—This section expires on September 30, 2024.

19 **§ 11709. Office of Strategy, Policy, and Plans**

20 (a) IN GENERAL.—The Under Secretary for Strategy, Policy, and Plans
21 is the principal policy advisor to the Secretary.

22 (b) FUNCTIONS.—The Under Secretary for Strategy, Policy, and Plans
23 shall—

24 (1) lead, conduct, and coordinate Department-wide policy develop-
25 ment and implementation and strategic planning;

26 (2) develop and coordinate policies to promote and ensure quality,
27 consistency, and integration for the programs, components, offices, and
28 activities across the Department;

29 (3) develop and coordinate strategic plans and long-term goals of the
30 Department with risk-based analysis and planning to improve oper-
31 ational mission effectiveness, including consultation with the Secretary
32 regarding the quadrennial homeland security review under section
33 11706 of this title;

34 (4) manage Department leadership councils and provide analytics
35 and support to the councils;

36 (5) manage international coordination and engagement for the De-
37 partment;

38 (6) review and incorporate, as appropriate, external stakeholder feed-
39 back into Department policy; and

40 (7) carry out such other responsibilities as the Secretary determines
41 appropriate.

1 (c) COORDINATION BY DEPARTMENT COMPONENTS.—To ensure consist-
2 ency with the policy priorities of the Department, the head of each compo-
3 nent of the Department shall coordinate with the Office of Strategy, Policy,
4 and Plans in establishing or modifying policies or strategic planning guid-
5 ance with respect to each component.

6 (d) HOMELAND SECURITY STATISTICS AND JOINT ANALYSIS.—

7 (1) HOMELAND SECURITY STATISTICS.—The Under Secretary for
8 Strategy, Policy, and Plans shall—

9 (A) establish standards of reliability and validity for statistical
10 data collected and analyzed by the Department;

11 (B) be provided by the heads of all components of the Depart-
12 ment with statistical data maintained by the Department regard-
13 ing the operations of the Department.

14 (C) conduct or oversee analysis and reporting of the data by the
15 Department as required by law or as directed by the Secretary;
16 and

17 (D) ensure the accuracy of metrics and statistical data provided
18 to Congress.

19 (2) TRANSFER OF RESPONSIBILITIES.—There shall be transferred to
20 the Under Secretary for Strategy, Policy, and Plans the maintenance
21 of all immigration statistical information of U.S. Customs and Border
22 Protection, U.S. Immigration and Customs Enforcement, and U.S.
23 Citizenship and Immigration Services, which shall include information
24 and statistics of the type contained in the publication entitled “Year-
25 book of Immigration Statistics” prepared by the Office of Immigration
26 Statistics, including region-by-region statistics on the aggregate num-
27 ber of applicants and petitions filed by an alien (or filed on behalf of
28 an alien) and denied, and the reasons for the denial, disaggregated by
29 category of denial and application or petition type.

30 (e) LIMITATION.—Nothing in this section overrides or otherwise affects
31 the requirements specified in section 10312 of this title.

32 **§ 11710. Employee engagement**

33 (a) STEERING COMMITTEE.—Not later than 120 days after December 27,
34 2021, the Secretary shall establish an employee engagement steering com-
35 mittee, including representatives from operational components, head-
36 quarters, and field personnel, including supervisory and nonsupervisory per-
37 sonnel, and employee labor organizations that represent Department em-
38 ployees, and chaired by the Under Secretary for Management, to carry out
39 the following activities:

40 (1) Identify factors that have a negative impact on employee engage-
41 ment, morale, and communications in the Department, such as percep-

1 tions about limitations on career progression, mobility, or development
2 opportunities, collected through employee feedback platforms, including
3 through annual employee surveys, questionnaires, and other commu-
4 nications, as appropriate.

5 (2) Identify, develop, and distribute initiatives and best practices to
6 improve employee engagement, morale, and communications in the De-
7 partment, including through annual employee surveys, questionnaires,
8 and other communications, as appropriate.

9 (3) Monitor efforts of each component to address employee engage-
10 ment, morale, and communications based on employee feedback pro-
11 vided through annual employee surveys, questionnaires, and other com-
12 munications, as appropriate.

13 (4) Advise the Secretary on efforts to improve employee engagement,
14 morale, and communications in specific components and across the De-
15 partment.

16 (5) Conduct regular meetings and report, not less than once per
17 quarter, to the Under Secretary for Management, the head of each
18 component, and the Secretary on Departmentwide efforts to improve
19 employee engagement, morale, and communications.

20 (b) ACTION PLAN; REPORTING.—The Secretary, acting through the Chief
21 Human Capital Officer, shall—

22 (1) not later than 120 days after the date of the establishment of
23 the employee engagement steering committee under subsection (a),
24 issue a Departmentwide employee engagement action plan, reflecting
25 input from the steering committee and employee feedback provided
26 through annual employee surveys, questionnaires, and other commu-
27 nications in accordance with subsection(a)(1), to execute strategies to
28 improve employee engagement, morale, and communications in the De-
29 partment; and

30 (2) require the head of each component to—

31 (A) develop and implement a component-specific employee en-
32 gagement plan to advance the action plan required under para-
33 graph (1) that includes performance measures and objectives, is
34 informed by employee feedback provided through annual employee
35 surveys, questionnaires, and other communications, as appropriate,
36 and sets forth how employees and, where applicable, their labor
37 representatives are to be integrated in developing programs and
38 initiatives;

39 (B) monitor progress on implementation of the action plan; and

1 (C) provide to the Chief Human Capital Officer and the steer-
2 ing committee quarterly reports on actions planned and progress
3 made under this paragraph.

4 (e) TERMINATION.—This section shall terminate on December 27, 2026.

5 **§ 11711. Acquisition professional career program**

6 (a) DEFINITIONS.—In this section:

7 (1) HISPANIC-SERVING INSTITUTION.— The term “Hispanic-serving
8 institution” has the meaning given that term in section 502 of the
9 Higher Education Act of 1965 (20 U.S.C. 1101a).

10 (2) HISTORICALLY BLACK COLLEGES AND UNIVERSITIES.—The term
11 “historically Black colleges and universities” has the meaning given the
12 term “part B institution” in section 322 of the Higher Education Act
13 of 1965 (20 U.S.C. 1061).

14 (3) INSTITUTION OF HIGHER EDUCATION.—The term “institution of
15 higher education” has the meaning given that term in section 101 of
16 the Higher Education Act of 1965 (20 U.S.C. 1001).

17 (b) ESTABLISHMENT.—There is in the Department an acquisition profes-
18 sional career program to develop a cadre of acquisition professionals within
19 the Department.

20 (c) ADMINISTRATION.—The Under Secretary for Management shall ad-
21 minister the acquisition professional career program established pursuant to
22 subsection (a).

23 (d) PROGRAM REQUIREMENTS.—The Under Secretary for Management
24 shall carry out the following with respect to the acquisition professional ca-
25 reer program:

26 (1) Designate the occupational series, grades, and number of acquisi-
27 tion positions throughout the Department to be included in the pro-
28 gram and manage centrally those positions.

29 (2) Establish and publish on the Department’s website eligibility cri-
30 teria for candidates to participate in the program.

31 (3) Carry out recruitment efforts to attract candidates—

32 (A) from institutions of higher education, including those insti-
33 tutions with established acquisition specialties and courses of
34 study, historically Black colleges and universities, and Hispanic-
35 serving institutions;

36 (B) with diverse work experience outside of the Federal Govern-
37 ment; or

38 (C) with military service.

39 (4) Hire eligible candidates for designated positions under the pro-
40 gram.

1 (5) Develop a structured program comprised of acquisition training,
 2 on-the-job experience, Department-wide rotations, mentorship, shad-
 3 owing, and other career development opportunities for program partici-
 4 pants.

5 (6) Provide, beyond required training established for program par-
 6 ticipants, additional specialized acquisition training, including small
 7 business contracting and innovative acquisition techniques training.

8 (e) REPORTS.—Not later than December 27, 2022, and annually there-
 9 after through 2027, the Secretary shall submit to the Committee on Home-
 10 land Security of the House of Representatives and the Committee on Home-
 11 land Security and Governmental Affairs of the Senate a report on the acqui-
 12 sition professional career program. Each report shall include the following
 13 information:

14 (1) The number of candidates approved for the program.

15 (2) The number of candidates who commenced participation in the
 16 program, including generalized information on the candidates' back-
 17 grounds with respect to education and prior work experience, but not
 18 including personally identifiable information.

19 (3) A breakdown of the number of participants hired under the pro-
 20 gram by type of acquisition position.

21 (4) A list of Department components and offices that participated
 22 in the program and information regarding length of time of each pro-
 23 gram participant in each rotation at the components or offices.

24 (5) Program attrition rates and post-program graduation retention
 25 data, including information on how the data compare to the prior
 26 year's data, as available.

27 (6) The Department's recruiting efforts for the program.

28 (7) The Department's efforts to promote retention of program par-
 29 ticipants.

30 **Chapter 119—Coordination With Other** 31 **Entities**

Sec.

11901. Responsibilities of Office for State and Local Government Coordination.

11902. Responsibilities of Office for National Capital Region Coordination.

11903. Joint Interagency Task Force.

11904. Coordination with Department of Health and Human Services under the Public
 Health Service Act.

11905. Aviation security.

11906. Investigation of violent acts, shootings, and mass killings.

11907. Facilitating homeland security information sharing procedures.

11908. Information sharing.

11909. Prohibition of Terrorism Information and Prevention System.

11910. Prevention of international child abduction.

11911. Limitation of liability.

11912. Transnational Criminal Investigative Units.

11913. Reciprocal information sharing with foreign government.

1 **§ 11901. Responsibilities of Office for State and Local Gov-**
2 **ernment Coordination**

3 The Office for State and Local Government Coordination oversees and co-
4 ordinates departmental programs for and relationships with State and local
5 governments. The Office shall—

6 (1) coordinate the activities of the Department relating to State and
7 local government;

8 (2) assess, and advocate for, the resources needed by State and local
9 government to implement the national strategy for combating ter-
10 rorism;

11 (3) provide State and local government with regular information, re-
12 search, and technical support to assist local efforts at securing the
13 homeland; and

14 (4) develop a process for receiving meaningful input from State and
15 local government to assist the development of the national strategy for
16 combating terrorism and other homeland security activities.

17 **§ 11902. Responsibilities of Office for National Capital Re-**
18 **gion Coordination**

19 (a) IN GENERAL.—The Office for National Capital Region Coordination
20 oversees and coordinates Federal programs for and relationships with State,
21 local, and regional authorities in the National Capital Region, as defined
22 under section 2674(f)(2) of title 10.

23 (b) COOPERATION WITH NATIONAL CAPITAL REGION OFFICIALS.—

24 (1) IN GENERAL.—The Secretary shall cooperate with the Mayor of
25 the District of Columbia, the Governors of Maryland and Virginia, and
26 other State, local, and regional officers in the National Capital Region
27 to integrate the District of Columbia, Maryland, and Virginia into the
28 planning, coordination, and execution of the activities of the Federal
29 Government for the enhancement of domestic preparedness against the
30 consequences of terrorist attacks.

31 (2) INCORPORATION OF GOVERNORS OF WEST VIRGINIA AND PENN-
32 SYLVANIA.—For purposes of planning, coordination, execution, and de-
33 cision making related to mass evacuation during a disaster, the Gov-
34 ernors of Pennsylvania, or their designees, shall be incorporated into
35 efforts to integrate the activities of Federal, State, and local govern-
36 ments in the National Capital Region.

37 (c) RESPONSIBILITIES.—The Office for National Capital Region Coordi-
38 nation shall—

39 (1) coordinate the activities of the Department relating to the Na-
40 tional Capital Region, including cooperation with the Office for State
41 and Local Government Coordination;

1 (2) assess, and advocate for, the resources needed by State, local,
2 and regional authorities in the National Capital Region to implement
3 efforts to secure the homeland;

4 (3) provide State, local, and regional authorities in the National Cap-
5 ital Region with regular information, research, and technical support
6 to assist the efforts of State, local, and regional authorities in the Na-
7 tional Capital Region in securing the homeland;

8 (4) develop a process for receiving meaningful input from State,
9 local, and regional authorities and the private sector in the National
10 Capital Region to assist in the development of the homeland security
11 plans and activities of the Federal Government;

12 (5) coordinate with Federal agencies in the National Capital Region
13 on terrorism preparedness, to ensure adequate planning, information
14 sharing, training, and execution of the Federal role in domestic pre-
15 paredness activities;

16 (6) coordinate with Federal, State, local, and regional agencies, and
17 the private sector in the National Capital Region on terrorism pre-
18 paredness to ensure adequate planning, information sharing, training,
19 and execution of domestic preparedness activities among these agencies
20 and entities; and

21 (7) serve as a liaison between the Federal Government and State,
22 local, and regional authorities, and private-sector entities in the Na-
23 tional Capital Region to facilitate access to Federal grants and other
24 programs.

25 (d) ANNUAL REPORT.—The Office for National Capital Region Coordina-
26 tion shall submit an annual report to Congress that includes—

27 (1) the identification of the resources required to fully implement
28 homeland security efforts in the National Capital Region;

29 (2) an assessment of the progress made by the National Capital Re-
30 gion in implementing homeland security efforts; and

31 (3) recommendations to Congress regarding the additional resources
32 needed to fully implement homeland security efforts in the National
33 Capital Region.

34 (e) LIMITATION.—Nothing contained in this section shall be construed as
35 limiting the power of State and local governments.

36 **§ 11903. Joint Interagency Task Force**

37 The Secretary may establish and operate a permanent Joint Interagency
38 Homeland Security Task Force composed of representatives from military
39 and civilian agencies of the United States Government for the purposes of
40 anticipating terrorist threats against the United States and taking appro-
41 priate actions to prevent harm to the United States.

1 **§ 11904. Coordination with Department of Health and**
2 **Human Services under the Public Health Service**
3 **Act**

4 (a) IN GENERAL.—The annual Federal response plan developed by the
5 Department shall be consistent with section 319 of the Public Health Service
6 Act (42 U.S.C. 247d).

7 (b) DISCLOSURES AMONG RELEVANT AGENCIES.—

8 (1) IN GENERAL.—Full disclosure among relevant agencies shall be
9 made under this subsection.

10 (2) PUBLIC HEALTH EMERGENCY.—During the period in which the
11 Secretary of Health and Human Services has declared the existence of
12 a public health emergency under section 319(a) of the Public Health
13 Service Act (42 U.S.C. 247d(a)), the Secretary of Health and Human
14 Services shall keep relevant agencies, including the Department, the
15 Department of Justice, and the Federal Bureau of Investigation, fully
16 and currently informed.

17 (3) POTENTIAL PUBLIC HEALTH EMERGENCY.—In cases involving,
18 or potentially involving, a public health emergency, but in which no de-
19 termination of an emergency by the Secretary of Health and Human
20 Services under section 319(a) of the Public Health Service Act (42
21 U.S.C. 247d(a)) has been made, all relevant agencies, including the De-
22 partment, the Department of Justice, and the Federal Bureau of Inves-
23 tigation, shall keep the Secretary of Health and Human Services and
24 the Director of the Centers for Disease Control and Prevention fully
25 and currently informed.

26 **§ 11905. Aviation security**

27 (a) CONSULTATION WITH FEDERAL AVIATION ADMINISTRATION.—The
28 Secretary and other officials in the Department shall consult with the Ad-
29 ministrator of the Federal Aviation Administration before taking an action
30 that might affect aviation safety, air carrier operations, aircraft airworthi-
31 ness, or the use of airspace. The Secretary shall establish a liaison office
32 in the Department to consult with the Administrator of the Federal Avia-
33 tion Administration.

34 (b) LIMITATIONS ON STATUTORY CONSTRUCTION.—

35 (1) GRANT OF AUTHORITY.—Nothing in this subtitle may be con-
36 strued to vest in the Secretary or another official in the Department
37 authority over transportation security that is not vested in the Admin-
38 istrator of the Transportation Security Administration, or that was not
39 vested in the Secretary of Transportation under chapter 449 of title
40 49 on November 24, 2002.

1 (2) OBLIGATION OF AIRPORT IMPROVEMENT PROGRAM FUNDS.—
2 Nothing in this subtitle may be construed to authorize the Secretary
3 or any other official in the Department to obligate amounts made avail-
4 able under section 48103 of title 49.

5 **§ 11906. Investigation of violent acts, shootings, and mass**
6 **killings**

7 (a) DEFINITIONS.—In this section:

8 (1) MASS KILLINGS.—The term “mass killings” means 3 or more
9 killings in a single incident.

10 (2) PLACE OF PUBLIC USE.—The term “place of public use” has the
11 meaning given the term under section 2332f(e)(6) of title 18.

12 (b) PROVIDING ASSISTANCE.—At the request of an appropriate law en-
13 forcement official of a State or political subdivision, the Secretary, through
14 deployment of the Secret Service or U.S. Immigration and Customs En-
15 forcement, may assist in the investigation of violent acts and shootings oc-
16 ccurring in a place of public use, and in the investigation of mass killings
17 and attempted mass killings. Any assistance provided by the Secretary
18 under this subsection shall be presumed to be within the scope of a Federal
19 office or of Federal employment.

20 **§ 11907. Facilitating homeland security information sharing**
21 **procedures**

22 (a) DEFINITIONS.—In this section:

23 (1) HOMELAND SECURITY INFORMATION.—The term “homeland se-
24 curity information” means information possessed by a Federal, State,
25 or local agency that—

26 (A) relates to the threat of terrorist activity;

27 (B) relates to the ability to prevent, interdict, or disrupt ter-
28 rorist activity;

29 (C) would improve the identification or investigation of a sus-
30 pected terrorist or terrorist organization; or

31 (D) would improve the response to a terrorist act.

32 (2) INTELLIGENCE COMMUNITY.—The term “intelligence commu-
33 nity” has the meaning given the term in section 3(4) of the National
34 Security Act of 1947 (50 U.S.C. 3003(4)).

35 (3) STATE AND LOCAL PERSONNEL.—The term “State and local per-
36 sonnel” means any of the following persons involved in the prevention
37 of, preparation for, or response to terrorist attack:

38 (A) State Governors, mayors, and other locally elected officials.

39 (B) State and local law enforcement personnel and firefighters.

40 (C) Public health and medical professionals.

1 (D) Regional, State, and local emergency management agency
2 personnel, including State adjutant generals.

3 (E) Other appropriate emergency response agency personnel.

4 (F) Employees of private-sector entities that affect critical in-
5 frastructure, cyber, economic, or public health security, as des-
6 ignated by the Federal Government in procedures developed under
7 this section.

8 (b) PROCEDURES FOR DETERMINING EXTENT OF SHARING OF HOME-
9 LAND SECURITY INFORMATION.—

10 (1) ESTABLISHMENT OF PROCEDURES.—The President shall pre-
11 scribe and implement procedures under which relevant Federal agen-
12 cies—

13 (A) share relevant and appropriate homeland security informa-
14 tion with other Federal agencies, including the Department, and
15 appropriate State and local personnel;

16 (B) identify and safeguard homeland security information that
17 is sensitive but unclassified; and

18 (C) to the extent the information is in classified form, determine
19 whether, how, and to what extent to remove classified information,
20 as appropriate, and with which personnel it may be shared after
21 the information is removed.

22 (2) APPLICABILITY.—The President shall ensure that the procedures
23 apply to all agencies of the Federal Government.

24 (3) NO CHANGE IN SUBSTANTIVE REQUIREMENTS.—The procedures
25 shall not change the substantive requirements for the classification and
26 safeguarding of classified information.

27 (4) NO CHANGE IN PROTECTIVE AUTHORITIES.—The procedures
28 shall not change the requirements and authorities to protect sources
29 and methods.

30 (c) PROCEDURES FOR SHARING OF HOMELAND SECURITY INFORMA-
31 TION.—

32 (1) IN GENERAL.—Under procedures prescribed by the President, all
33 appropriate agencies, including the intelligence community, shall,
34 through information sharing systems, share homeland security informa-
35 tion with Federal agencies and appropriate State and local personnel
36 to the extent the information may be shared, as determined under sub-
37 section (b), together with assessments of the credibility of the informa-
38 tion.

39 (2) SYSTEM CAPABILITIES.—Each information sharing system
40 through which information is shared under paragraph (1) shall—

1 (A) have the capability to transmit unclassified or classified in-
2 formation, though the procedures and recipients for each capa-
3 bility may differ;

4 (B) have the capability to restrict delivery of information to
5 specified subgroups by geographic location, type of organization,
6 position of a recipient within an organization, or a recipient's need
7 to know the information;

8 (C) be configured to allow the efficient and effective sharing of
9 information; and

10 (D) be accessible to appropriate State and local personnel.

11 (3) USE CONDITIONS.—The procedures prescribed under paragraph
12 (1) shall establish conditions on the use of information shared under
13 paragraph (1)—

14 (A) to limit the re-dissemination of the information to ensure
15 that the information is not used for an unauthorized purpose;

16 (B) to ensure the security and confidentiality of the informa-
17 tion;

18 (C) to protect the constitutional and statutory rights of individ-
19 uals who are subjects of the information; and

20 (D) to provide data integrity through the timely removal and
21 destruction of obsolete or erroneous names and information.

22 (4) INCLUSION OF EXISTING SYSTEMS.—The procedures prescribed
23 under paragraph (1) shall ensure, to the greatest extent practicable,
24 that the information sharing system through which information is
25 shared under that paragraph include existing information sharing sys-
26 tems, including the National Law Enforcement Telecommunications
27 System, the Regional Information Sharing System, and the Terrorist
28 Threat Warning System of the Federal Bureau of Investigation.

29 (5) AGENCY ACCESS.—Each appropriate Federal agency, as deter-
30 mined by the President, shall have access to each information sharing
31 system through which information is shared under paragraph (1), and
32 shall therefore have access to all information, as appropriate, shared
33 under that paragraph.

34 (6) SHARING INFORMATION.—The procedures prescribed under para-
35 graph (1) shall ensure that appropriate State and local personnel are
36 authorized to use the information sharing systems—

37 (A) to access information shared with the personnel; and

38 (B) to share, with others who have access to the information
39 sharing systems, the homeland security information of their own
40 jurisdictions, which shall be marked appropriately as pertaining to
41 potential terrorist activity.

1 (7) ASSESSMENT AND INTEGRATION OF INFORMATION.—Under pro-
2 cedures prescribed jointly by the Director of National Intelligence and
3 the Attorney General, each appropriate Federal agency, as determined
4 by the President, shall review and assess the information shared under
5 paragraph (6) and integrate the information with existing intelligence.

6 (d) SHARING OF CLASSIFIED INFORMATION AND SENSITIVE BUT UN-
7 CLASSIFIED INFORMATION WITH STATE AND LOCAL PERSONNEL.—

8 (1) IN GENERAL.—The President shall prescribe procedures under
9 which Federal agencies may, to the extent the President considers nec-
10 essary, share with appropriate State and local personnel homeland se-
11 curity information that remains classified or otherwise protected after
12 the determinations prescribed under the procedures set forth in sub-
13 section (b) are made.

14 (2) TRAINING PROGRAM.—

15 (A) ESTABLISHMENT.—The Secretary shall establish a program
16 to provide appropriate training to officials described in subpara-
17 graph (B) in order to assist the officials in—

18 (i) identifying sources of potential terrorist threats through
19 the methods the Secretary determines are appropriate;

20 (ii) reporting information relating to the potential terrorist
21 threats to the appropriate Federal agencies in the appropriate
22 form and manner;

23 (iii) assuring that all reported information is systematically
24 submitted to and passed on by the Department for use by ap-
25 propriate Federal agencies; and

26 (iv) understanding the mission and roles of the intelligence
27 community to promote more effective information sharing
28 among Federal, State, and local officials and representatives
29 of the private sector to prevent terrorist attacks against the
30 United States.

31 (B) TRAINING COVERAGE.—The officials referred to in subpara-
32 graph (A) are officials of State and local government agencies and
33 representatives of private-sector entities with responsibilities relat-
34 ing to the oversight and management of first responders, counter-
35 terrorism activities, or critical infrastructure.

36 (C) CONSULTATION WITH ATTORNEY GENERAL.—The Secretary
37 shall consult with the Attorney General to ensure that the training
38 program established in subparagraph (A) does not duplicate the
39 training program established in section 908 of the USA PA-
40 TRIOT Act (Public Law 107–56, 28 U.S.C. 509 note).

1 (D) OTHER CONSULTATION.—The Secretary shall carry out this
2 paragraph in consultation with the Director of National Intel-
3 ligence and the Attorney General.

4 (e) RESPONSIBLE OFFICIALS.—For each affected Federal agency, the
5 head of the agency shall designate an official to administer this subtitle with
6 respect to the agency.

7 (f) FEDERAL CONTROL OF INFORMATION.—Under procedures prescribed
8 under this section, information obtained by a State or local government
9 from a Federal agency under this section shall remain under the control of
10 the Federal agency, and a State or local law authorizing or requiring a gov-
11 ernment to disclose information shall not apply to the information.

12 (g) CONSTRUCTION.—Nothing in this subtitle shall be construed as au-
13 thORIZING a department, bureau, agency, officer, or employee of the Federal
14 Government to request, receive, or transmit to another Government entity
15 or any Government personnel, or transmit to a State or local entity or State
16 or local personnel otherwise authorized by the Homeland Security Act of
17 2002 (Public Law 107–296, 116 Stat. 2135) to receive homeland security
18 information, information collected by the Federal Government solely for sta-
19 tistical purposes in violation of any other provision of law relating to the
20 confidentiality of the information.

21 **§ 11908. Information sharing**

22 (a) DEFINITIONS.—In this section:

23 (1) HOMELAND SECURITY INFORMATION.—The term “homeland se-
24 curity information” has the meaning given the term in section
25 11907(a) of this title.

26 (2) INFORMATION SHARING COUNCIL.—The term “Information Shar-
27 ing Council” means the Information Sharing Council established by
28 Executive Order 13388 (Oct. 25, 2005, 70 F.R. 62023), or any suc-
29 cessor body designated by the President, and referred to under sub-
30 section (e).

31 (3) INFORMATION SHARING ENVIRONMENT; ISE.—The terms “infor-
32 mation sharing environment” and “ISE” mean an approach that facili-
33 tates the sharing of terrorism and homeland security information,
34 which may include any method determined necessary and appropriate
35 for carrying out this section.

36 (4) PROGRAM MANAGER.—The term “program manager” means the
37 program manager designated under subsection (d).

38 (5) TERRORISM INFORMATION.—The term “terrorism informa-
39 tion”—

1 (A) means all information, whether collected, produced, or dis-
2 tributed by intelligence, law enforcement, military, homeland secu-
3 rity, or other activities relating to—

4 (i) the existence, organization, capabilities, plans, inten-
5 tions, vulnerabilities, means of finance or material support, or
6 activities of foreign or international terrorist groups or indi-
7 viduals, or of domestic groups or individuals involved in
8 transnational terrorism;

9 (ii) threats posed by these groups or individuals to the
10 United States, United States persons, or United States inter-
11 ests, or to those of other nations;

12 (iii) communications of or by these groups or individuals;
13 or

14 (iv) other groups or individuals reasonably believed to be
15 assisting or associated with these groups or individuals; and

16 (B) includes weapons of mass destruction information.

17 (6) WEAPONS OF MASS DESTRUCTION INFORMATION.—The term
18 “weapons of mass destruction information” means information that
19 could reasonably be expected to assist in the development, proliferation,
20 or use of a weapon of mass destruction (including a chemical, biologi-
21 cal, radiological, or nuclear weapon) that could be used by a terrorist
22 or a terrorist organization against the United States, including infor-
23 mation about the location of a stockpile of nuclear materials that could
24 be exploited for use in a weapon that could be used by a terrorist or
25 a terrorist organization against the United States.

26 (b) INFORMATION SHARING ENVIRONMENT.—

27 (1) ESTABLISHMENT.—The President shall—

28 (A) create an information sharing environment for the sharing
29 of terrorism information in a manner consistent with national se-
30 curity and with applicable legal standards relating to privacy and
31 civil liberties;

32 (B) designate the organizational and management structures
33 that will be used to operate and manage the ISE; and

34 (C) determine and enforce the policies, directives, and rules that
35 will govern the content and usage of the ISE.

36 (2) ATTRIBUTES.—The President shall, through the structures de-
37 scribed in subparagraphs (B) and (C) of paragraph (1), ensure that
38 the ISE provides and facilitates the means for sharing terrorism infor-
39 mation among all appropriate Federal, State, local, and tribal entities,
40 and the private sector through the use of policy guidelines and tech-
41 nologies. The President shall, to the greatest extent practicable, ensure

1 that the ISE provides the functional equivalent of, or otherwise sup-
2 ports, a decentralized, distributed, and coordinated environment that—

3 (A) connects existing systems, where appropriate, provides no
4 single points of failure, and allows users to share information
5 among agencies, between levels of government, and, as appro-
6 priate, with the private sector;

7 (B) ensures direct and continuous online electronic access to in-
8 formation;

9 (C) facilitates the availability of information in a form and man-
10 ner that makes easier its use in analysis, investigations, and oper-
11 ations;

12 (D) builds upon existing systems capabilities currently in use
13 across the Government;

14 (E) employs an information access management approach that
15 controls access to data rather than just systems and networks,
16 without sacrificing security;

17 (F) facilitates the sharing of information at and across all levels
18 of security;

19 (G) provides directory services, or the functional equivalent, for
20 locating people and information;

21 (H) incorporates protections for individuals' privacy and civil
22 liberties;

23 (I) incorporates strong mechanisms to enhance accountability
24 and facilitate oversight, including audits, authentication, and ac-
25 cess controls;

26 (J) integrates the information within the scope of the informa-
27 tion sharing environment, including information in legacy tech-
28 nologies;

29 (K) integrates technologies, including all legacy technologies,
30 through Internet-based services, consistent with appropriate secu-
31 rity protocols and safeguards, to enable connectivity among re-
32 quired users at the Federal, State, and local levels;

33 (L) allows the full range of analytic and operational activities
34 without the need to centralize information within the scope of the
35 information sharing environment;

36 (M) permits analysts to collaborate both independently and in
37 a group (commonly known as "collective and noncollective collabo-
38 ration"), and across multiple levels of national security informa-
39 tion and controlled unclassified information;

40 (N) provides a resolution process that enables changes by au-
41 thorized officials regarding rules and policies for the access, use,

1 and retention of information within the scope of the information
2 sharing environment; and

3 (O) incorporates continuous, real-time, and immutable audit ca-
4 pabilities, to the maximum extent practicable.

5 (3) DELEGATION.—The President may delegate responsibility for
6 carrying out this subsection, except that the President may not dele-
7 gate that responsibility to the Director of National Intelligence.

8 (c) GUIDELINES AND REQUIREMENTS.—The President shall—

9 (1) leverage all ongoing efforts consistent with establishing the ISE
10 and issue guidelines for acquiring, accessing, sharing, and using infor-
11 mation, including guidelines to ensure that information is provided in
12 its most shareable form, such as by using tearlines to separate out data
13 from the sources and methods by which the data are obtained;

14 (2) in consultation with the Privacy and Civil Liberties Oversight
15 Board established under section 1061 of the Intelligence Reform and
16 Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee), issue guidelines
17 that—

18 (A) protect privacy and civil liberties in the development and
19 use of the ISE; and

20 (B) shall be made public, unless nondisclosure is clearly nec-
21 essary to protect national security; and

22 (3) require the heads of Federal departments and agencies to pro-
23 mote a culture of information sharing by—

24 (A) reducing disincentives to information sharing, including
25 over-classification of information and unnecessary requirements
26 for originator approval, consistent with applicable laws and regula-
27 tions; and

28 (B) providing affirmative incentives for information sharing.

29 (d) PROGRAM MANAGER.—

30 (1) DESIGNATION.—Each individual designated as the program man-
31 ager shall be appointed by the Director of National Intelligence. The
32 program manager, in consultation with the head of an affected depart-
33 ment or agency, shall have and exercise Government-wide authority
34 over the sharing of information within the scope of the information
35 sharing environment, including homeland security information, ter-
36 rorism information, and weapons of mass destruction information, by
37 all Federal departments, agencies, and components, irrespective of the
38 Federal department, agency, or component in which the program man-
39 ager may be administratively located, except as otherwise expressly pro-
40 vided by law.

41 (2) DUTIES AND RESPONSIBILITIES.—

1 (A) IN GENERAL.—The program manager shall, in consultation
2 with the Information Sharing Council—

3 (i) plan for and oversee the implementation of, and man-
4 age, the ISE;

5 (ii) assist in the development of policies, as appropriate, to
6 foster the development and proper operation of the ISE;

7 (iii) consistent with the direction and policies issued by the
8 President, the Director of National Intelligence, and the Di-
9 rector of the Office of Management and Budget, issue Gov-
10 ernment-wide procedures, guidelines, instructions, and func-
11 tional standards, as appropriate, for the management, devel-
12 opment, and proper operation of the ISE;

13 (iv) identify and resolve information sharing disputes be-
14 tween Federal departments, agencies, and components; and

15 (v) assist, monitor, and assess the implementation of the
16 ISE by Federal departments and agencies to ensure adequate
17 progress, technological consistency, and policy compliance;
18 and regularly report the findings to Congress.

19 (B) CONTENT OF POLICIES, PROCEDURES, GUIDELINES, IN-
20 STRUCTIONS, AND STANDARDS.—The policies, procedures, guide-
21 lines, instructions, and standards under clauses (ii) and (iii) of
22 subparagraph (A) shall—

23 (i) take into account the varying missions and security re-
24 quirements of agencies participating in the ISE;

25 (ii) address development, implementation, and oversight of
26 technical standards and requirements;

27 (iii) take into account ongoing and planned efforts that
28 support development, implementation, and management of
29 the ISE;

30 (iv) address and facilitate information sharing between and
31 among departments and agencies of the intelligence commu-
32 nity, the Department of Defense, the homeland security com-
33 munity, and the law enforcement community;

34 (v) address and facilitate information sharing between Fed-
35 eral departments and agencies and State, tribal, and local
36 governments;

37 (vi) address and facilitate, as appropriate, information
38 sharing between Federal departments and agencies and the
39 private sector;

1 (vii) address and facilitate, as appropriate, information
2 sharing between Federal departments and agencies with for-
3 eign partners and allies; and

4 (viii) ensure the protection of privacy and civil liberties.

5 (e) INFORMATION SHARING COUNCIL.—

6 (1) ESTABLISHMENT.—There is in the Department the Information
7 Sharing Council that assists the President and the program manager
8 in their duties under this section. The Information Sharing Council
9 serves until removed from service or replaced by the President (at the
10 sole discretion of the President) with a successor body.

11 (2) SPECIFIC DUTIES.—In assisting the President and the program
12 manager in their duties under this section, the Information Sharing
13 Council shall—

14 (A) advise the President and the program manager in devel-
15 oping policies, procedures, guidelines, instructions, and standards
16 necessary to establish, implement, and maintain the ISE;

17 (B) work to ensure coordination among the Federal depart-
18 ments and agencies participating in the ISE in the establishment,
19 implementation, and maintenance of the ISE;

20 (C) identify and, as appropriate, recommend the consolidation
21 and elimination of current programs, systems, and processes used
22 by Federal departments and agencies to share information, and
23 recommend, as appropriate, the redirection of existing resources to
24 support the ISE;

25 (D) identify gaps, if any, between existing technologies, pro-
26 grams, and systems used by Federal departments and agencies to
27 share information and the parameters of the proposed information
28 sharing environment;

29 (E) recommend solutions to address gaps identified under sub-
30 paragraph (D);

31 (F) recommend means by which the ISE can be extended to
32 allow interchange of information between Federal departments and
33 agencies and appropriate authorities of State and local govern-
34 ments;

35 (G) assist the program manager in identifying and resolving in-
36 formation sharing disputes between Federal departments, agen-
37 cies, and components;

38 (H) identify appropriate personnel for assignment to the pro-
39 gram manager to support staffing needs identified by the program
40 manager; and

1 (I) recommend whether or not, and by which means, the ISE
2 should be expanded so as to allow future expansion encompassing
3 other relevant categories of information.

4 (3) CONSULTATION.—In performing its duties, the Information
5 Sharing Council shall consider input from persons and entities outside
6 the Federal Government having significant experience and expertise in
7 policy, technical matters, and operational matters relating to the ISE.

8 (4) INAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—The Information
9 Sharing Council (including a subsidiary group of the Council) is not
10 subject to the requirements of chapter 10 of title 5.

11 (5) DETAILEES.—On a request by the Director of National Intel-
12 ligence, the departments and agencies represented on the Information
13 Sharing Council shall detail to the program manager, on a reimburs-
14 able basis, appropriate personnel identified under paragraph (2)(H).

15 (f) AGENCY RESPONSIBILITIES.—The head of each department or agency
16 that possesses or uses intelligence or terrorism information, operates a sys-
17 tem in the ISE, or otherwise participates (or expects to participate) in the
18 ISE shall—

19 (1) ensure full department or agency compliance with information
20 sharing policies, procedures, guidelines, rules, and standards estab-
21 lished under subsections (b) and (d);

22 (2) ensure the provision of adequate resources for systems and ac-
23 tivities supporting operation of and participation in the ISE;

24 (3) ensure full department or agency cooperation in the development
25 of the ISE to implement Government-wide information sharing; and

26 (4) submit, at the request of the President or the program manager,
27 reports on the implementation of the requirements of the ISE within
28 the department or agency.

29 (g) ADDITIONAL POSITIONS.—The program manager may hire not more
30 than 40 full-time employees to assist the program manager in—

31 (1) activities associated with the implementation of the information
32 sharing environment, including—

33 (A) implementing the requirements under subsection (b)(2); and

34 (B) any additional implementation initiatives to enhance and ex-
35 pedite the creation of the information sharing environment; and

36 (2) identifying and resolving information sharing disputes between
37 Federal departments, agencies, and components under subsection
38 (d)(2)(A)(iv).

1 **§ 11909. Prohibition of Terrorism Information and Preven-**
2 **tion System**

3 All activities of the Federal Government to implement the proposed com-
4 ponent program of the Citizen Corps Division known as Operation TIPS
5 (Terrorism Information and Prevention System) are prohibited.

6 **§ 11910. Prevention of international child abduction**

7 (a) PROGRAM ESTABLISHED.—The Secretary, through the Commissioner
8 of U.S. Customs and Border Protection, in coordination with the Secretary
9 of State, the Attorney General, and the Director of the Federal Bureau of
10 Investigation, shall establish a program that—

11 (1) seeks to prevent a child (as defined in section 1204(b)(1) of title
12 18) from departing from the territory of the United States if a parent
13 or legal guardian of the child presents a court order from a court of
14 competent jurisdiction prohibiting the removal of the child from the
15 United States to a U.S. Customs and Border Protection Officer in suf-
16 ficient time to prevent the departure for the duration of the court
17 order; and

18 (2) leverages other existing authorities and processes to address the
19 wrongful removal and return of a child.

20 (b) INTERAGENCY COORDINATION.—

21 (1) IN GENERAL.—The Secretary of State shall convene and chair
22 an interagency working group to prevent international parental child
23 abduction. The group shall be composed of presidentially appointed,
24 Senate-confirmed officials from—

25 (A) the Department of State;

26 (B) the Department of Homeland Security, including U.S. Cus-
27 toms and Border Protection and U.S. Immigration and Customs
28 Enforcement; and

29 (C) the Department of Justice, including the Federal Bureau of
30 Investigation.

31 (2) DEPARTMENT OF DEFENSE.—The Secretary of Defense shall
32 designate an official in the Department of Defense—

33 (A) to coordinate with the Department of State on international
34 child abduction issues; and

35 (B) to oversee activities designed to prevent or resolve inter-
36 national child abduction cases relating to active duty military serv-
37 ice members.

38 **§ 11911. Limitation of liability**

39 A person who has completed a security awareness training course ap-
40 proved by or operated under a cooperative agreement with the Department,
41 who is enrolled in a program recognized or acknowledged by an Information

1 Sharing and Analysis Center and who reports a situation, activity, or inci-
2 dent pursuant to that program to an appropriate authority, shall not be lia-
3 ble for damages in an action brought in a Federal or State court which re-
4 sult from an act or omission unless the person is guilty of gross negligence
5 or willful misconduct.

6 **§ 11912. Transnational Criminal Investigative Units**

7 (a) IN GENERAL.—The Secretary, with the concurrence of the Secretary
8 of State, shall operate Transnational Criminal Investigative Units within
9 Homeland Security Investigations.

10 (b) COMPOSITION.—Each Transnational Criminal Investigative Unit shall
11 be composed of trained foreign law enforcement officials who shall collabo-
12 rate with Homeland Security Investigations to investigate and prosecute in-
13 dividuals involved in transnational criminal activity.

14 (c) VETTING REQUIREMENT.—

15 (1) IN GENERAL.—Before entry into a Transnational Criminal Inves-
16 tigative Unit, and at periodic intervals while serving in a Transnational
17 Criminal Investigate Unit, foreign law enforcement officials shall be re-
18 quired to pass certain security evaluations, which may include a back-
19 ground check, a polygraph examination, a urinalysis test, or other
20 measures that the Secretary determines to be appropriate.

21 (2) LEAHY VETTING REQUIRED.—No member of a foreign law en-
22 forcement unit may join a Transnational Criminal Investigative Unit
23 if the Secretary, in coordination with the Secretary of State, has cred-
24 ible information that the foreign law enforcement unit has committed
25 a gross violation of human rights, consistent with the limitations set
26 forth in section 620M of the Foreign Assistance Act of 1961 (22 U.S.C.
27 2378d).

28 (3) APPROVAL AND CONCURRENCE.— The establishment and contin-
29 ued support of the Transnational Criminal Investigative Units that are
30 assigned under paragraph (1)—

31 (A) shall be performed with the approval of the chief of mission
32 to the foreign country to which the personnel are assigned;

33 (B) shall be consistent with the duties and powers of the Sec-
34 retary of State and the chief of mission for a foreign country
35 under section 103 of the Diplomatic Security Act (22 U.S.C. 4802)
36 and section 207 of the Foreign Service Act of 1980 (22 U.S.C.
37 3927), respectively; and

38 (C) shall not be established without the concurrence of the As-
39 sistant Secretary of State for International Narcotics and Law
40 Enforcement Affairs.

1 (4) REPORT.—The Executive Associate Director of Homeland Security
2 Investigations shall submit a report to the Committee on Foreign
3 Relations of the Senate, the Committee on Homeland Security and
4 Governmental Affairs of the Senate, the Committee on the Judiciary
5 of the Senate, the Committee on Foreign Affairs of the House of Rep-
6 representatives, the Committee on Homeland Security of the House of
7 Representatives, and the Committee on the Judiciary of the House of
8 Representatives that describes—

9 (A) the procedures used for vetting Transnational Criminal In-
10 vestigative Unit members to include compliance with the vetting
11 required under this subsection; and

12 (B) any additional measures that should be implemented to pre-
13 vent personnel in vetted units from being compromised by criminal
14 organizations.

15 (d) MONETARY STIPEND.—The Executive Associate Director of Home-
16 land Security Investigations may pay vetted members of a Transnational
17 Criminal Investigative Unit a monetary stipend in an amount associated
18 with their duties dedicated to unit activities.

19 (e) ANNUAL BRIEFING.—The Executive Associate Director of Homeland
20 Security Investigations, during the 5-year period beginning on December 23,
21 2022, shall provide an annual unclassified briefing to the congressional com-
22 mittees referred to in subsection (c)(4), which may include a classified ses-
23 sion, if necessary, that identifies—

24 (1) the number of vetted members of Transnational Criminal Inves-
25 tigative Unit in each country;

26 (2) the amount paid in stipends to the members, disaggregated by
27 country;

28 (3) relevant enforcement statistics, such as arrests and progress
29 made on joint investigations, in each country; and

30 (4) whether any vetted members of the Transnational Criminal In-
31 vestigative Unit in each country were involved in any unlawful activity,
32 including human rights abuses or significant acts of corruption.

33 **§ 11913. Reciprocal information sharing with foreign gov-**
34 **ernment**

35 Acting in accordance with a bilateral or multilateral arrangement, the
36 Secretary, in the Secretary's discretion and on the basis of reciprocity, may
37 provide information from the National Sex Offender Registry relating to a
38 conviction for a sex offense against a minor (as the terms are defined in
39 section 111 of the Sex Offender Registration and Notification Act (34
40 U.S.C. 20911) to a foreign government on the request of the foreign govern-

1 ment, and may receive comparable information from the foreign govern-
2 ment.

3 **Chapter 121—Homeland Security Council**

Sec.

12101. Establishment.

12102. Membership.

12103. Functions and activities.

12104. Staff.

12105. Joint meetings with National Security Council.

4 **§ 12101. Establishment**

5 There is in the Executive Office of the President the Homeland Security
6 Council to advise the President on homeland security matters.

7 **§ 12102. Membership**

8 (a) MEMBERS.—The members of the Homeland Security Council are the
9 following:

10 (1) The President.

11 (2) The Vice President.

12 (3) The Secretary.

13 (4) The Attorney General.

14 (5) The Secretary of Defense.

15 (6) Other individuals who may be designated by the President.

16 (b) ATTENDANCE OF CHAIRMAN OF JOINT CHIEFS OF STAFF AT MEET-
17 INGS.—The Chairman of the Joint Chiefs of Staff (or, in the absence of
18 the Chairman, the Vice Chairman of the Joint Chiefs of Staff) may, in the
19 role of the Chairman of the Joint Chiefs of Staff as principal military ad-
20 viser to the Homeland Security Council and subject to the direction of the
21 President, attend and participate in meetings of the Council.

22 **§ 12103. Functions and activities**

23 To effectively coordinate the policies and functions of the United States
24 Government relating to homeland security, the Homeland Security Council
25 shall—

26 (1) assess the objectives, commitments, and risks of the United
27 States in the interest of homeland security and make resulting rec-
28 ommendations to the President;

29 (2) oversee and review homeland security policies of the Federal Gov-
30 ernment and make resulting recommendations to the President; and

31 (3) perform other functions that the President may direct.

32 **§ 12104. Staff**

33 (a) HEADED BY EXECUTIVE SECRETARY.—The Homeland Security
34 Council has a staff, the head of which is a civilian Executive Secretary ap-
35 pointed by the President.

1 (b) PAY OF EXECUTIVE SECRETARY.—The President shall fix the pay of
 2 the Executive Secretary at a rate not to exceed the rate of pay payable to
 3 the Executive Secretary of the National Security Council.

4 **§ 12105. Joint meetings with National Security Council**

5 The President may convene joint meetings of the Homeland Security
 6 Council and the National Security Council with participation by members
 7 of either Council or as the President may otherwise direct.

8 **Chapter 123—Emergency Communications**

Sec.

12301. Definitions; rule of construction.

12302. Responsibilities of Executive Assistant Director for Emergency Communications.

12303. National Emergency Communications Plan.

12304. Assessments and reports.

12305. Coordination of Department emergency communications grant programs.

12306. Regional Emergency Communications Coordination.

12307. Emergency Communications Preparedness Center.

12308. Urban and other high-risk area communications capabilities.

12309. Interoperable Emergency Communications Grant Program.

12310. Border interoperability demonstration project.

9 **§ 12301. Definitions; rule of construction**

10 (a) DEFINITIONS OF INTEROPERABLE COMMUNICATIONS AND INTER-
 11 OPERABLE EMERGENCY COMMUNICATIONS.—In this chapter, the terms
 12 “interoperable communications” and “interoperable emergency communica-
 13 tions” have the meaning given the term “interoperable communications”
 14 under section 10912(a) of this title.

15 (b) RULE OF CONSTRUCTION.—Nothing in this chapter or in sections
 16 10913 or 10914 of this title shall be construed to transfer to the Office of
 17 Emergency Communications any function, personnel, asset, component, au-
 18 thority, grant program, or liability of the Federal Emergency Management
 19 Agency as constituted on June 1, 2006.

20 **§ 12302. Responsibilities of Executive Assistant Director for**
 21 **Emergency Communications**

22 (a) IN GENERAL.—The Executive Assistant Director for Emergency
 23 Communications shall—

24 (1) assist the Secretary in developing and implementing the program
 25 described in section 10912(b)(1) of this title, except as provided in sec-
 26 tion 10913 of this title;

27 (2) administer the Department’s responsibilities and authorities re-
 28 lating to the SAFECOM Program, excluding elements related to re-
 29 search, development, testing, and evaluation and standards;

30 (3) administer the Department’s responsibilities and authorities re-
 31 lating to the Integrated Wireless Network program;

32 (4) conduct extensive, nationwide outreach to support and promote
 33 the ability of emergency response providers and relevant government

1 officials to continue to communicate in the event of natural disasters,
2 acts of terrorism, and other man-made disasters;

3 (5) conduct extensive, nationwide outreach and foster the develop-
4 ment of interoperable emergency communications capabilities by State,
5 regional, local, and tribal governments and public safety agencies, and
6 by regional consortia thereof;

7 (6) provide technical assistance to State, regional, local, and tribal
8 government officials with respect to the use of interoperable emergency
9 communications capabilities;

10 (7) coordinate with the Regional Administrators regarding the activi-
11 ties of Regional Emergency Communications Coordination Working
12 Groups under section 12306 of this title;

13 (8) promote the development of standard operating procedures and
14 best practices with respect to use of interoperable emergency commu-
15 nications capabilities for incident response, and facilitate the sharing
16 of information on best practices for achieving, maintaining, and en-
17 hancing interoperable emergency communications capabilities for re-
18 sponse;

19 (9) coordinate, in cooperation with the National Communications
20 System, the establishment of a national response capability with initial
21 and ongoing planning, implementation, and training for the deployment
22 of communications equipment for relevant State, local, and tribal gov-
23 ernments and emergency response providers in the event of a cata-
24 strophic loss of local and regional emergency communications services;

25 (10) assist the President, the National Security Council, the Home-
26 land Security Council, and the Director of the Office of Management
27 and Budget in ensuring the continued operation of the telecommuni-
28 cations functions and responsibilities of the Federal Government, ex-
29 cluding spectrum management;

30 (11) establish, in coordination with the Director of the Office for
31 Interoperability and Compatibility, requirements for interoperable
32 emergency communications capabilities, which shall be nonproprietary
33 where standards for the capabilities exist, for all public safety radio
34 and data communications systems and equipment purchased using
35 homeland security assistance administered by the Department, exclud-
36 ing any alert and warning device, technology, or system;

37 (12) review, in consultation with the Assistant Secretary for Grants
38 and Training, all interoperable emergency communications plans of
39 Federal, State, local, and tribal governments, including statewide and
40 tactical interoperability plans, developed pursuant to homeland security

1 assistance administered by the Department, but excluding spectrum al-
2 location and management related to the plans;

3 (13) develop and update periodically, as appropriate, a National
4 Emergency Communications Plan under section 12303 of this title;

5 (14) perform other duties of the Department necessary to support
6 and promote the ability of emergency response providers and relevant
7 government officials to continue to communicate in the event of natural
8 disasters, acts of terrorism, and other man-made disasters;

9 (15) perform other duties of the Department necessary to achieve
10 the goal of, and maintain and enhance, interoperable emergency com-
11 munications capabilities; and

12 (16) fully participate in the mechanisms required under section
13 10702(a)(1)(G) of this title.

14 (b) PERFORMANCE OF PREVIOUSLY TRANSFERRED FUNCTIONS.—The
15 Secretary shall administer through the Executive Assistant Director for
16 Emergency Communications the following programs and responsibilities:

17 (1) The SAFECOM Program, excluding elements related to re-
18 search, development, testing, and evaluation and standards.

19 (2) The responsibilities of the Chief Information Officer related to
20 the implementation of the Integrated Wireless Network.

21 (3) The Interoperable Communications Technical Assistance Pro-
22 gram.

23 (c) COORDINATION.—The Executive Assistant Director for Emergency
24 Communications shall coordinate—

25 (1) as appropriate, with the Director of the Office for Interoper-
26 ability and Compatibility with respect to the responsibilities described
27 in section 10913 of this title; and

28 (2) with the Administrator of the Federal Emergency Management
29 Agency with respect to the responsibilities described in this chapter.

30 **§ 12303. National Emergency Communications Plan**

31 (a) IN GENERAL.—The Secretary, acting through the Assistant Director
32 for Emergency Communications, and in cooperation with the National Com-
33 munications System Office of the Department (as appropriate), shall, in co-
34 operation with State, local, and tribal governments, Federal departments
35 and agencies, emergency response providers, and the private sector, develop,
36 and periodically update, a National Emergency Communications Plan to
37 provide recommendations regarding how the United States should—

38 (1) support and promote the ability of emergency response providers
39 and relevant government officials to continue to communicate in the
40 event of natural disasters, acts of terrorism, and other man-made dis-
41 asters; and

1 (2) ensure, accelerate, and attain interoperable emergency commu-
2 nications nationwide.

3 (b) COORDINATION.—The Emergency Communications Preparedness
4 Center under section 12307 of this title shall coordinate the development
5 of the Federal aspects of the National Emergency Communications Plan.

6 (c) CONTENTS.—The National Emergency Communications Plan shall—

7 (1) include recommendations developed in consultation with the Fed-
8 eral Communications Commission and the National Institute of Stand-
9 ards and Technology for a process for expediting national voluntary
10 consensus standards for emergency communications equipment for the
11 purchase and use by public safety agencies of interoperable emergency
12 communications equipment and technologies;

13 (2) identify the appropriate capabilities necessary for emergency re-
14 sponse providers and relevant government officials to continue to com-
15 municate in the event of natural disasters, acts of terrorism, and other
16 man-made disasters;

17 (3) identify the appropriate interoperable emergency communications
18 capabilities necessary for Federal, State, local, and tribal governments
19 in the event of natural disasters, acts of terrorism, and other man-
20 made disasters;

21 (4) recommend both short-term and long-term solutions for ensuring
22 that emergency response providers and relevant government officials
23 can continue to communicate in the event of natural disasters, acts of
24 terrorism, and other man-made disasters;

25 (5) recommend both short-term and long-term solutions for deploy-
26 ing interoperable emergency communications systems for Federal,
27 State, local, and tribal governments throughout the Nation, including
28 through the provision of existing and emerging technologies;

29 (6) identify how Federal departments and agencies that respond to
30 natural disasters, acts of terrorism, and other man-made disasters can
31 work effectively with State, local, and tribal governments, in all States,
32 and with other entities;

33 (7) identify obstacles to deploying interoperable emergency commu-
34 nications capabilities nationwide and recommend short-term and long-
35 term measures to overcome those obstacles, including recommendations
36 for multijurisdictional coordination among Federal, State, local, and
37 tribal governments;

38 (8) recommend goals and time frames for the deployment of emer-
39 gency, command-level communications systems based on new and exist-
40 ing equipment across the United States and develop a timetable for the

1 deployment of interoperable emergency communications systems nation-
2 wide;

3 (9) recommend appropriate measures that emergency response pro-
4 viders should employ to ensure the continued operation of relevant gov-
5 ernmental communications infrastructure in the event of natural disas-
6 ters, acts of terrorism, or other man-made disasters; and

7 (10) set a date, including interim benchmarks, as appropriate, by
8 which State, local, and tribal governments, Federal departments and
9 agencies, and emergency response providers expect to achieve a baseline
10 level of national interoperable communications, as that term is defined
11 under section 10912(a) of this title.

12 **§ 12304. Assessments and reports**

13 (a) BASELINE ASSESSMENT.—The Secretary, acting through the Assist-
14 ant Director for Emergency Communications, shall conduct an assessment
15 of Federal, State, local, and tribal governments every 5 years, that—

16 (1) defines the range of capabilities needed by emergency response
17 providers and relevant government officials to continue to communicate
18 in the event of natural disasters, acts of terrorism, and other man-
19 made disasters;

20 (2) defines the range of interoperable emergency communications ca-
21 pabilities needed for specific events;

22 (3) assesses the currently available capabilities to meet the commu-
23 nications needs;

24 (4) identifies the gap between current capabilities and defined re-
25 quirements; and

26 (5) includes a national interoperable emergency communications in-
27 ventory to be completed by the Secretary, the Secretary of Commerce,
28 and the Chairman of the Federal Communications Commission that—

29 (A) identifies for each Federal department and agency—

30 (i) the channels and frequencies used;

31 (ii) the nomenclature used to refer to each channel or fre-
32 quency used; and

33 (iii) the types of communications systems and equipment
34 used; and

35 (B) identifies the interoperable emergency communications sys-
36 tems in use by public safety agencies in the United States.

37 (b) CLASSIFIED ANNEX.—The baseline assessment under this section
38 may include a classified annex, including information provided under sub-
39 section (a)(5)(A).

1 (c) SAVINGS CLAUSE.—In conducting the baseline assessment under this
2 section, the Secretary may incorporate findings from assessments conducted
3 before, or ongoing on, October 4, 2006.

4 (d) PROGRESS REPORTS.—Not later than 1 year after October 4, 2006,
5 and biennially thereafter, the Secretary, acting through the Assistant Direc-
6 tor for Emergency Communications, shall submit to Congress a report on
7 the progress of the Department in achieving the goals of, and carrying out
8 its responsibilities under, this chapter, including—

9 (1) a description of the findings of the most recent baseline assess-
10 ment conducted under subsection (a);

11 (2) a determination of the degree to which interoperable emergency
12 communications capabilities have been attained to date and the gaps
13 that remain for interoperability to be achieved;

14 (3) an evaluation of the ability to continue to communicate and to
15 provide and maintain interoperable emergency communications by
16 emergency managers, emergency response providers, and relevant gov-
17 ernment officials in the event of—

18 (A) natural disasters, acts of terrorism, or other man-made dis-
19 asters, including Incidents of National Significance declared by the
20 Secretary under the National Response Plan; and

21 (B) a catastrophic loss of local and regional communications
22 services;

23 (4) a list of best practices relating to the ability to continue to com-
24 municate and to provide and maintain interoperable emergency commu-
25 nications in the event of natural disasters, acts of terrorism, or other
26 man-made disasters; and

27 (5) an evaluation of the feasibility and desirability of the Depart-
28 ment's developing, on its own or in conjunction with the Department
29 of Defense, a mobile communications capability, modeled on the Army
30 Signal Corps, that could be deployed to support emergency communica-
31 tions at the site of natural disasters, acts of terrorism, or other man-
32 made disasters.

33 **§ 12305. Coordination of Department emergency commu-**
34 **nications grant programs**

35 (a) COORDINATION OF GRANTS AND STANDARDS PROGRAMS.—The Sec-
36 retary, acting through the Assistant Director for Emergency Communica-
37 tions, shall ensure that grant guidelines for the use of homeland security
38 assistance administered by the Department relating to interoperable emer-
39 gency communications are coordinated and consistent with the goals and
40 recommendations in the National Emergency Communications Plan under
41 section 12303 of this title.

1 (b) DENIAL OF ELIGIBILITY FOR GRANTS.—

2 (1) IN GENERAL.—The Secretary, acting through the Assistant Sec-
3 retary for Grants and Planning, and in consultation with the Assistant
4 Director for Emergency Communications, may prohibit any State,
5 local, or tribal government from using homeland security assistance ad-
6 ministered by the Department to achieve, maintain, or enhance emer-
7 gency communications capabilities, if—

8 (A) the government has not complied with the requirement to
9 submit an Interoperable Communications Plan as required by sec-
10 tion 10912(e) of this title;

11 (B) the government has proposed to upgrade or purchase new
12 equipment or systems that do not meet or exceed any applicable
13 national voluntary consensus standards and has not provided a
14 reasonable explanation of why the equipment or systems will serve
15 the needs of the applicant better than equipment or systems that
16 meet or exceed the standards; and

17 (C) as of the date that is 3 years after the date of the comple-
18 tion of the initial National Emergency Communications Plan
19 under section 12303 of this title, national voluntary consensus
20 standards for interoperable emergency communications capabilities
21 have not been developed and promulgated.

22 (2) STANDARDS.—The Secretary, in coordination with the Federal
23 Communications Commission, the National Institute of Standards and
24 Technology, and other Federal departments and agencies responsible
25 for standards, shall support the development, promulgation, and updat-
26 ing as necessary of national voluntary consensus standards for inter-
27 operable emergency communications.

28 **§ 12306. Regional Emergency Communications Coordination**

29 (a) IN GENERAL.—There is in each Regional Office a Regional Emer-
30 gency Communications Coordination Working Group (in this section re-
31 ferred to as an “RECC Working Group”). Each RECC Working Group
32 shall report to the relevant Regional Administrator and coordinate its activi-
33 ties with the relevant Regional Advisory Council.

34 (b) MEMBERSHIP.—Each RECC Working Group consists of the following:

35 (1) Organizations representing the interests of the following:

36 (A) State officials.

37 (B) Local government officials, including sheriffs.

38 (C) State police departments.

39 (D) Local police departments.

40 (E) Local fire departments.

41 (F) Public safety answering points (9-1-1 services).

1 (G) State emergency managers, homeland security directors, or
2 representatives of State administrative agencies.

3 (H) Local emergency managers or homeland security directors.

4 (I) Other emergency response providers as appropriate.

5 (2) Representatives from the Department, the Federal Communica-
6 tions Commission, and other Federal departments and agencies with
7 responsibility for coordinating interoperable emergency communications
8 with, or providing emergency support services to, State, local, and trib-
9 al governments.

10 (e) COORDINATION.—Each RECC Working Group shall coordinate its ac-
11 tivities with the following:

12 (1) Communications equipment manufacturers and vendors (includ-
13 ing broadband data service providers).

14 (2) Local exchange carriers.

15 (3) Local broadcast media.

16 (4) Wireless carriers.

17 (5) Satellite communications services.

18 (6) Cable operators.

19 (7) Hospitals.

20 (8) Public utility services.

21 (9) Emergency evacuation transit services.

22 (10) Ambulance services.

23 (11) HAM and amateur radio operators.

24 (12) Representatives from other private-sector entities and non-
25 governmental organizations as the Regional Administrator determines
26 appropriate.

27 (d) DUTIES.—The duties of each RECC Working Group include—

28 (1) assessing the survivability, sustainability, and interoperability of
29 local emergency communications systems to meet the goals of the Na-
30 tional Emergency Communications Plan;

31 (2) reporting annually to the relevant Regional Administrator, the
32 Assistant Director for Emergency Communications, the Chairman of
33 the Federal Communications Commission, and the Assistant Secretary
34 for Communications and Information of the Department of Commerce
35 on the status of its region in building robust and sustainable interoper-
36 able voice and data emergency communications networks and, not later
37 than 60 days after the completion of the initial National Emergency
38 Communications Plan under section 12303 of this title, on the progress
39 of the region in meeting the goals of the plan;

40 (3) ensuring a process for the coordination of effective multijuris-
41 dictional, multi-agency emergency communications networks for use

1 during natural disasters, acts of terrorism, and other man-made disas-
2 ters through the expanded use of emergency management and public
3 safety communications mutual aid agreements; and

4 (4) coordinating the establishment of Federal, State, local, and tribal
5 support services and networks designed to address the immediate and
6 critical human needs in responding to natural disasters, acts of ter-
7 rorism, and other man-made disasters.

8 **§ 12307. Emergency Communications Preparedness Center**

9 (a) ESTABLISHMENT.—There is the Emergency Communications Pre-
10 paredness Center.

11 (b) OPERATION.—The Secretary, the Chairman of the Federal Commu-
12 nications Commission, the Secretary of Defense, the Secretary of Commerce,
13 the Attorney General, and the heads of other Federal departments and
14 agencies or their designees shall jointly operate the Emergency Communica-
15 tions Preparedness Center in accordance with the Memorandum of Under-
16 standing entitled, “Emergency Communications Preparedness Center
17 (ECPC) Charter”.

18 (c) FUNCTIONS.—The Emergency Communications Preparedness Center
19 shall—

20 (1) serve as the focal point for interagency efforts and as a clearing-
21 house with respect to all relevant intergovernmental information to sup-
22 port and promote (including specifically by working to avoid duplica-
23 tion, hindrances, and counteractive efforts among the participating
24 Federal departments and agencies)—

25 (A) the ability of emergency response providers and relevant
26 government officials to continue to communicate in the event of
27 natural disasters, acts of terrorism, and other man-made disasters;
28 and

29 (B) interoperable emergency communications;

30 (2) prepare and submit to Congress annually a strategic assessment
31 regarding the coordination efforts of Federal departments and agencies
32 to advance—

33 (A) the ability of emergency response providers and relevant
34 government officials to continue to communicate in the event of
35 natural disasters, acts of terrorism, and other man-made disasters;
36 and

37 (B) interoperable emergency communications;

38 (3) consider, in preparing the strategic assessment under paragraph
39 (2), the goals stated in the National Emergency Communications Plan
40 under section 12303 of this title; and

1 (4) perform other functions provided in the ECPC Charter described
2 in subsection (b).

3 **§ 12308. Urban and other high-risk area communications ca-**
4 **pabilities**

5 (a) IN GENERAL.—The Secretary, in consultation with the Chairman of
6 the Federal Communications Commission and the Secretary of Defense, and
7 with appropriate State, local, and tribal government officials, shall provide
8 technical guidance, training, and other assistance, as appropriate, to sup-
9 port the rapid establishment of consistent, secure, and effective interoper-
10 able emergency communications capabilities in the event of an emergency
11 in urban and other areas determined by the Secretary to be at consistently
12 high levels of risk from natural disasters, acts of terrorism, and other man-
13 made disasters.

14 (b) MINIMUM CAPABILITIES.—The interoperable emergency communica-
15 tions capabilities established under subsection (a) shall ensure the ability of
16 all levels of government, emergency response providers, the private sector,
17 and other organizations with emergency response capabilities—

18 (1) to communicate with each other in the event of an emergency;

19 (2) to have appropriate and timely access to the information sharing
20 environment described in section 11908 of this title; and

21 (3) to be consistent with any applicable State or urban area home-
22 land strategy or plan.

23 **§ 12309. Interoperable Emergency Communications Grant**
24 **Program**

25 (a) ESTABLISHMENT.—The Secretary shall establish the Interoperable
26 Emergency Communications Grant Program to make grants to States to
27 carry out initiatives to improve local, tribal, statewide, regional, national,
28 and, where appropriate, international interoperable emergency communica-
29 tions, including communications in collective response to natural disasters,
30 acts of terrorism, and other man-made disasters.

31 (b) POLICY.—The Assistant Director for Emergency Communications
32 shall ensure that a grant awarded to a State under this section is consistent
33 with the policies established pursuant to the responsibilities and authorities
34 of the Emergency Communications Division under this chapter, including
35 ensuring that activities funded by the grant—

36 (1) comply with the statewide plan for that State required by section
37 10912(e) of this title; and

38 (2) comply with the National Emergency Communications Plan
39 under section 12303 of this title, when completed.

40 (c) ADMINISTRATION.—

1 (1) IN GENERAL.—The Administrator of the Federal Emergency
2 Management Agency shall administer the Interoperable Emergency
3 Communications Grant Program pursuant to the responsibilities and
4 authorities of the Administrator under chapter 113 of this title.

5 (2) GUIDANCE.—In administering the grant program, the Adminis-
6 trator shall ensure that the use of grants is consistent with guidance
7 established by the Assistant Director for Emergency Communications
8 under section 10912(b)(1)(H) of this title.

9 (d) USE OF FUNDS.—A State that receives a grant under this section
10 shall use the grant to implement that State’s Interoperable Communications
11 Plan required under section 10912(e) of this title and approved under sub-
12 section (e) of this section, and to assist with activities determined by the
13 Secretary to be integral to interoperable emergency communications.

14 (e) APPROVAL OF PLANS.—

15 (1) APPROVAL AS CONDITION OF GRANT.—Before a State may re-
16 ceive a grant under this section, the Assistant Director for Emergency
17 Communications shall approve the State’s Interoperable Communica-
18 tions Plan required under section 10912(e) of this title.

19 (2) PLAN REQUIREMENTS.—In approving a plan under this sub-
20 section, the Assistant Director for Emergency Communications shall
21 ensure that the plan—

22 (A) is designed to improve interoperability at the city, county,
23 regional, State, and interstate level;

24 (B) considers any applicable local or regional plan; and

25 (C) complies, to the maximum extent practicable, with the Na-
26 tional Emergency Communications Plan under section 12303 of
27 this title.

28 (3) APPROVAL OF REVISIONS.—The Assistant Director for Emer-
29 gency Communications may approve revisions to a State’s plan if the
30 Assistant Director for Emergency Communications determines that
31 doing so is likely to further interoperability.

32 (f) LIMITATIONS ON USES OF FUNDS.—

33 (1) IN GENERAL.—The recipient of a grant under this section may
34 not use the grant—

35 (A) to supplant State or local funds;

36 (B) for any State or local government cost-sharing contribution;

37 or

38 (C) for recreational or social purposes.

39 (2) PENALTIES.—In addition to other remedies currently available,
40 the Secretary may take necessary actions to ensure that recipients of

1 grant funds are using the funds for the purpose for which they were
2 intended.

3 (g) LIMITATIONS ON AWARD OF GRANTS.—

4 (1) NATIONAL EMERGENCY COMMUNICATIONS PLAN REQUIRED.—

5 The Secretary may not award a grant under this section before the
6 date on which the Secretary completes and submits to Congress the
7 National Emergency Communications Plan required under section
8 12303 of this title.

9 (2) VOLUNTARY CONSENSUS STANDARDS.—The Secretary may not
10 award a grant to a State under this section for the purchase of equip-
11 ment that does not meet applicable voluntary consensus standards, un-
12 less the State demonstrates that there are compelling reasons for the
13 purchase.

14 (h) AWARD OF GRANTS.—In approving applications and awarding grants
15 under this section, the Secretary shall consider—

16 (1) the risk posed to each State by natural disasters, acts of ter-
17 rorism, or other man-made disasters, including—

18 (A) the likely need of a jurisdiction within the State to respond
19 to the risk in nearby jurisdictions;

20 (B) the degree of threat, vulnerability, and consequences related
21 to critical infrastructure (from all critical infrastructure sectors)
22 or key resources identified by the Administrator or the State
23 homeland security and emergency management plans, including
24 threats to, vulnerabilities of, and consequences from damage to
25 critical infrastructure and key resources in nearby jurisdictions;

26 (C) the size of the population and density of the population of
27 the State, including appropriate consideration of military, tourist,
28 and commuter populations;

29 (D) whether the State is on or near an international border;

30 (E) whether the State encompasses an economically significant
31 border crossing; and

32 (F) whether the State has a coastline bordering an ocean, a
33 major waterway used for interstate commerce, or international
34 waters; and

35 (2) the anticipated effectiveness of the State's proposed use of grant
36 funds to improve interoperability.

37 (i) OPPORTUNITY TO AMEND APPLICATIONS.—In considering applications
38 for grants under this section, the Administrator shall provide applicants
39 with a reasonable opportunity to correct defects in the application, if any,
40 before making final awards.

41 (j) MINIMUM GRANT AMOUNTS.—

1 (1) STATES.—In awarding grants under this section, the Secretary
2 shall ensure that for each fiscal year, except as provided in paragraph
3 (2), no State receives a grant in an amount that is less than 0.35 per-
4 cent of the total amount appropriated for grants under this section for
5 that fiscal year.

6 (2) TERRITORIES.—In awarding grants under this section, the Sec-
7 retary shall ensure that for each fiscal year, American Samoa, the
8 Northern Mariana Islands, Guam, and the Virgin Islands each receive
9 grants in amounts that are not less than 0.08 percent of the total
10 amount appropriated for grants under this section for that fiscal year.

11 (k) CERTIFICATION.—Each State that receives a grant under this section
12 shall certify that the grant is used for the purpose for which the funds were
13 intended and in compliance with the State’s approved Interoperable Commu-
14 nications Plan.

15 (l) STATE RESPONSIBILITIES.—

16 (1) AVAILABILITY OF FUNDS TO LOCAL AND TRIBAL GOVERN-
17 MENTS.—Not later than 45 days after receiving grant funds, a State
18 that receives a grant under this section shall obligate or otherwise
19 make available to local and tribal governments—

20 (A) not less than 80 percent of the grant funds;

21 (B) with the consent of local and tribal governments, eligible ex-
22 penditures having a value of not less than 80 percent of the
23 amount of the grant; or

24 (C) grant funds combined with other eligible expenditures hav-
25 ing a total value of not less than 80 percent of the amount of the
26 grant.

27 (2) ALLOCATION OF FUNDS.—A State that receives a grant under
28 this section shall allocate grant funds to tribal governments in the
29 State to assist tribal communities in improving interoperable commu-
30 nications, in a manner consistent with the State’s Interoperable Com-
31 munications Plan. A State may not impose unreasonable or unduly
32 burdensome requirements on a tribal government as a condition of pro-
33 viding grant funds or resources to the tribal government.

34 (3) PENALTIES.—If a State violates the requirements of this sub-
35 section, in addition to other remedies available to the Secretary, the
36 Secretary may terminate or reduce the amount of the grant awarded
37 to that State or transfer grant funds previously awarded to the State
38 directly to the appropriate local or tribal government.

39 (m) REPORTS.—

40 (1) ANNUAL REPORTS BY STATE GRANT RECIPIENTS.—A State that
41 receives a grant under this section shall annually submit to the Assist-

1 ant Director for Emergency Communications a report on the progress
2 of the State in implementing that State’s Interoperable Communica-
3 tions Plan required under section 10912(e) of this title and achieving
4 interoperability at the city, county, regional, State, and interstate lev-
5 els. The Assistant Director for Emergency Communications shall make
6 the reports publicly available, including by making them available on
7 the Internet website of the Cybersecurity and Infrastructure Security
8 Agency, subject to any redactions that the Assistant Director for
9 Emergency Communications determines are necessary to protect classi-
10 fied or other sensitive information.

11 (2) ANNUAL REPORTS TO CONGRESS.—At least once each year, the
12 Assistant Director for Emergency Communications shall submit to
13 Congress a report on the use of grants awarded under this section and
14 any progress in implementing Statewide Interoperable Communications
15 Plans and improving interoperability at the city, county, regional,
16 State, and interstate level, as a result of the award of the grants.

17 (n) RULE OF CONSTRUCTION.—Nothing in this section shall be construed
18 or interpreted to preclude a State from using a grant awarded under this
19 section for interim or long-term Internet Protocol-based interoperable solu-
20 tions.

21 **§ 12310. Border interoperability demonstration project**

22 (a) IN GENERAL.—

23 (1) ESTABLISHMENT.—The Secretary, acting through the Assistant
24 Director for Emergency Communications, and in coordination with the
25 Federal Communications Commission and the Secretary of Commerce,
26 shall establish an International Border Community Interoperable Com-
27 munications Project (in this section referred to as the “demonstration
28 project”).

29 (2) MINIMUM NUMBER OF COMMUNITIES.—The Assistant Director
30 for Emergency Communications shall select no fewer than 6 commu-
31 nities to participate in the demonstration project.

32 (3) LOCATION OF COMMUNITIES.—No fewer than 3 of the commu-
33 nities selected under paragraph (2) shall be located on the northern
34 border of the United States and no fewer than 3 of the communities
35 selected under paragraph (2) shall be located on the southern border
36 of the United States.

37 (b) CONDITIONS.—The Assistant Director for Emergency Communica-
38 tions, in coordination with the Federal Communications Commission and
39 the Secretary of Commerce, shall ensure that the demonstration project is
40 carried out as soon as adequate spectrum is available as a result of the 800
41 megahertz rebanding process in border areas, and shall ensure that the bor-

1 der projects do not impair or impede the rebanding process, but under no
2 circumstances shall funds be distributed under this section unless the Fed-
3 eral Communications Commission and the Secretary of Commerce agree
4 that these conditions have been met.

5 (c) DEMONSTRATION PROJECT REQUIREMENTS.—Consistent with the re-
6 sponsibilities of the Emergency Communications Division under section
7 12302 of this title, the Assistant Director for Emergency Communications
8 shall foster local, tribal, State, and Federal interoperable emergency commu-
9 nications, as well as interoperable emergency communications with appro-
10 priate Canadian and Mexican authorities in the communities selected for the
11 demonstration project. The Assistant Director for Emergency Communica-
12 tions shall—

13 (1) identify solutions to facilitate interoperable communications
14 across national borders expeditiously;

15 (2) help ensure that emergency response providers can communicate
16 with each other in the event of natural disasters, acts of terrorism, and
17 other man-made disasters;

18 (3) provide technical assistance to enable emergency response pro-
19 viders to deal with threats and contingencies in a variety of environ-
20 ments;

21 (4) identify appropriate joint-use equipment to ensure communica-
22 tions access;

23 (5) identify solutions to facilitate communications between emer-
24 gency response providers in communities of differing population den-
25 sities; and

26 (6) take other actions or provide equipment as the Assistant Director
27 for Emergency Communications considers appropriate to foster inter-
28 operable emergency communications.

29 (d) DISTRIBUTION OF FUNDS.—

30 (1) TO EACH PARTICIPATING COMMUNITY.—The Secretary shall dis-
31 tribute funds under this section to each community participating in the
32 demonstration project through the State in which each community is
33 located.

34 (2) TO LOCAL AND TRIBAL GOVERNMENTS AND EMERGENCY PRO-
35 VIDERS SELECTED TO PARTICIPATE.—A State shall make the funds
36 available promptly to the local and tribal government and emergency
37 response providers selected by the Secretary to participate in the dem-
38 onstration project.

39 (3) REPORT.—Not later than 90 days after a State receives funds
40 under this subsection, the States shall report to the Assistant Director

1 for Emergency Communications on the status of the distribution of the
2 funds to local and tribal governments.

3 (e) MAXIMUM PERIOD OF GRANTS.—The Assistant Director for Emer-
4 gency Communications may not fund a participant under the demonstration
5 project for more than 3 years.

6 (f) TRANSFER OF INFORMATION AND KNOWLEDGE.—The Assistant Di-
7 rector for Emergency Communications shall establish mechanisms to ensure
8 that the information and knowledge gained by participants in the dem-
9 onstration project are transferred among the participants and to other inter-
10 ested parties, including other communities that submitted applications to
11 participate in the project.

12 **Chapter 125—Countering Weapons of Mass** 13 **Destruction Office**

Sec.

12501. Definitions.

12502. Mission.

12503. Relationship to other Department components and Federal agencies.

12504. Responsibilities.

12505. Technology research and development investment strategy for nuclear and radiological
detection.

12506. Testing authority.

12507. Personnel.

12508. Contracting and grant making authorities.

12509. Joint annual interagency review of global nuclear detection architecture.

12510. Securing the Cities program.

12511. Medical countermeasures.

12512. Annual report by Secretary.

14 **§ 12501. Definitions**

15 In this chapter:

16 (1) ASSISTANT SECRETARY.—The term “Assistant Secretary” means
17 the Assistant Secretary for the Countering Weapons of Mass Destruc-
18 tion Office.

19 (2) INTELLIGENCE COMMUNITY.—The term “intelligence commu-
20 nity” has the meaning given the term in section 3 of the National Se-
21 curity Act of 1947 (50 U.S.C. 3003).

22 (3) OFFICE.—The term “Office” means the Countering Weapons of
23 Mass Destruction Office.

24 (4) WEAPONS OF MASS DESTRUCTION.—The term “weapons of mass
25 destruction” has the meaning given the term in section 101 of the For-
26 eign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

27 **§ 12502. Mission**

28 The Office is responsible for coordinating with other Federal efforts and
29 developing a strategy and policy for the Department to plan for, detect, and
30 protect against the importation, possession, storage, transportation, develop-
31 ment, or use of unauthorized chemical, biological, radiological, or nuclear

1 materials, devices, or agents in the United States and to protect against an
2 attack using those materials, devices, or agents against the people, territory,
3 or interests of the United States.

4 **§ 12503. Relationship to other Department components and**
5 **Federal agencies**

6 (a) IN GENERAL.—The authority of the Assistant Secretary under this
7 chapter shall not affect the authorities or responsibilities of an officer of the
8 Department or of an officer of another department or agency of the United
9 States with respect to the command, control, or direction of the functions,
10 personnel, funds, assets, and liabilities of a component in the Department
11 or of a Federal department or agency.

12 (b) OFFICE FOR STRATEGY, POLICY, AND PLANS.—Not later than 1 year
13 after December 21, 2018, the Assistant Secretary, in coordination with the
14 Under Secretary for Strategy, Plans, and Policy, shall submit to the appro-
15 priate congressional committees a strategy and implementation plan to di-
16 rect programs in the Office and to integrate those programs with other pro-
17 grams and activities of the Department.

18 (c) FEDERAL EMERGENCY MANAGEMENT AGENCY.—Nothing in this
19 chapter or other provision of law may be construed to affect or reduce the
20 responsibilities of the Federal Emergency Management Agency or the Ad-
21 ministrator of the Federal Emergency Management Agency, including the
22 diversion of an asset, function, or mission of the Federal Emergency Man-
23 agement Agency or the Administrator of the Federal Emergency Manage-
24 ment Agency.

25 **§ 12504. Responsibilities**

26 (a) ASSISTANT SECRETARY.—The Assistant Secretary shall serve as the
27 Secretary’s principal advisor on—

28 (1) weapons of mass destruction matters and strategies; and

29 (2) the coordination of the efforts of the Department to counter
30 weapons of mass destruction.

31 (b) OFFICE.—

32 (1) DEFINITIONS.—In this subsection:

33 (A) ALASKA NATIVE-SERVING INSTITUTION.—The term “Alaska
34 Native-serving institution” has the meaning given the term in sec-
35 tion 317 of the Higher Education Act of 1965 (20 U.S.C. 1059d).

36 (B) ASIAN AMERICAN AND NATIVE AMERICAN PACIFIC IS-
37 LANDER-SERVING INSTITUTION.—The term “Asian American and
38 Native American Pacific Islander-serving institution” has the
39 meaning given the term in section 320 of the Higher Education
40 Act of 1965 (20 U.S.C. 1059g).

1 (C) HISPANIC-SERVING INSTITUTION.—The term “Hispanic-
2 serving institution” has the meaning given the term in section 502
3 of the Higher Education Act of 1965 (20 U.S.C. 1101a).

4 (D) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The
5 term “historically Black college or university” has the meaning
6 given the term “part B institution” in section 322 of the Higher
7 Education Act of 1965 (20 U.S.C. 1061).

8 (E) NATIVE HAWAIIAN-SERVING INSTITUTION.—The term “Na-
9 tive Hawaiian-serving institution” has the meaning given the term
10 in section 317 of the Higher Education Act of 1965 (20 U.S.C.
11 1059d).

12 (F) TRIBAL COLLEGE OR UNIVERSITY.—The term “Tribal Col-
13 lege or University” has the meaning given the term in section
14 316(b) of the Higher Education Act of 1965 (20 U.S.C.
15 1059c(b)).

16 (2) IN GENERAL.—The Office is responsible for coordinating Federal
17 efforts to detect and protect against the unauthorized importation, pos-
18 session, storage, transportation, development, or use of a nuclear explo-
19 sive device, fissile material, or radiological material in the United
20 States, and to protect against attack using those devices or materials
21 against the people, territory, or interests of the United States and, to
22 this end, shall—

23 (A) serve as the primary entity of the United States Govern-
24 ment to further develop, acquire, and support the deployment of
25 an enhanced domestic system to detect and report on attempts to
26 import, possess, store, transport, develop, or use an unauthorized
27 nuclear explosive device, fissile material, or radiological material in
28 the United States, and to improve that system over time;

29 (B) enhance and coordinate the nuclear detection efforts of Fed-
30 eral, State, local, and tribal governments and the private sector to
31 ensure a managed, coordinated response;

32 (C) establish, with the approval of the Secretary and in coordi-
33 nation with the Attorney General, the Secretary of Defense, and
34 the Secretary of Energy, additional protocols and procedures for
35 use within the United States to ensure that the detection of unau-
36 thorized nuclear explosive devices, fissile material, or radiological
37 material is promptly reported to the Attorney General, the Sec-
38 retary, the Secretary of Defense, the Secretary of Energy, and
39 other appropriate officials or their respective designees for appro-
40 priate action by law enforcement, military, emergency response, or
41 other authorities;

1 (D) develop, with the approval of the Secretary and in coordina-
2 tion with the Attorney General, the Secretary of State, the Sec-
3 retary of Defense, and the Secretary of Energy, an enhanced glob-
4 al nuclear detection architecture with implementation under
5 which—

6 (i) the Office will be responsible for the implementation of
7 the domestic portion of the global architecture;

8 (ii) the Secretary of Defense will retain responsibility for
9 implementation of Department of Defense requirements with-
10 in and outside the United States; and

11 (iii) the Secretary of State, the Secretary of Defense, and
12 the Secretary of Energy will maintain their respective respon-
13 sibilities for policy guidance and implementation of the por-
14 tion of the global architecture outside the United States,
15 which will be implemented consistent with applicable law and
16 relevant international arrangements;

17 (E) ensure that the expertise necessary to accurately interpret
18 detection data is made available in a timely manner for all tech-
19 nology deployed by the Domestic Nuclear Detection Office to im-
20 plement the global nuclear detection architecture;

21 (F) conduct, support, coordinate, and encourage an aggressive,
22 expedited, evolutionary, and transformational program of research
23 and development to generate and improve technologies to detect
24 and prevent the illicit entry, transport, assembly, or potential use
25 within the United States of a nuclear explosive device or fissile or
26 radiological material, and coordinate with the Under Secretary for
27 Science and Technology on basic and advanced or trans-
28 formational research and development efforts relevant to the mis-
29 sion of both organizations;

30 (G) carry out a program to test and evaluate technology for de-
31 tecting a nuclear explosive device and fissile or radiological mate-
32 rial, in coordination with the Secretary of Defense and the Sec-
33 retary of Energy, as appropriate, and establish performance
34 metrics for evaluating the effectiveness of individual detectors and
35 detection systems in detecting such devices or material—

36 (i) under realistic operational and environmental condi-
37 tions; and

38 (ii) against realistic adversary tactics and countermeasures;

39 (H) support and enhance the effective sharing and use of appro-
40 priate information generated by the intelligence community, law
41 enforcement agencies, counterterrorism community, other govern-

1 ment agencies, and foreign governments, as well as provide appro-
2 priate information to the entities;

3 (I) further enhance and maintain continuous awareness by ana-
4 lyzing information from all Domestic Nuclear Detection Office
5 mission-related detection systems;

6 (J) lead the development and implementation of the national
7 strategic five-year plan for improving the nuclear forensic and at-
8 tribution capabilities of the United States required under section
9 1036 of the National Defense Authorization Act for Fiscal Year
10 2010 (Public Law 111–84, 123 Stat. 2450);

11 (K) establish in the Office the National Technical Nuclear
12 Forensics Center to provide centralized stewardship, planning, as-
13 sessment, gap analysis, exercises, improvement, and integration
14 for all Federal nuclear forensics and attribution activities—

15 (i) to ensure an enduring national technical nuclear
16 forensics capability to strengthen the collective response of
17 the United States to nuclear terrorism or other nuclear at-
18 tacks; and

19 (ii) to coordinate and implement the national strategic five-
20 year plan referred to in subparagraph (J);

21 (L) establish a National Nuclear Forensics Expertise Develop-
22 ment Program, which—

23 (i) is devoted to developing and maintaining a vibrant and
24 enduring academic pathway from undergraduate to post-doc-
25 torate study in nuclear and geochemical science specialties di-
26 rectly relevant to technical nuclear forensics, including
27 radiochemistry, geochemistry, nuclear physics, nuclear engi-
28 neering, materials science, and analytical chemistry;

29 (ii) shall—

30 (I) make available for undergraduate study, student
31 scholarships with a duration of up to 4 years per stu-
32 dent, which shall include, if possible, at least one sum-
33 mer internship at a national laboratory or appropriate
34 Federal agency in the field of technical nuclear forensics
35 during the course of the student’s undergraduate career;

36 (II) make available for doctoral study, student fellow-
37 ships with a duration of up to 5 years per student, which
38 shall—

39 (aa) include, if possible, at least two summer in-
40 ternships at a national laboratory or appropriate
41 Federal agency in the field of technical nuclear

1 forensics during the course of the student's grad-
2 uate career; and

3 (bb) require each recipient to commit to serve for
4 2 years in a post-doctoral position in a technical nu-
5 clear forensics-related specialty at a national labora-
6 tory or appropriate Federal agency after gradua-
7 tion;

8 (III) make available to faculty, awards with a duration
9 of 3 to 5 years each, to ensure faculty and their grad-
10 uate students have a sustained funding stream; and

11 (IV) place a particular emphasis on reinvigorating
12 technical nuclear forensics programs while encouraging
13 the participation of undergraduate students, graduate
14 students, and university faculty from historically Black
15 colleges and universities, Hispanic-serving institutions,
16 Tribal Colleges and Universities, Asian American and
17 Native American Pacific Islander-serving institutions,
18 Alaska Native-serving institutions, and Native Hawaiian-
19 serving institutions; and

20 (iii) shall—

21 (I) provide for the selection of individuals to receive
22 scholarships or fellowships under this section through a
23 competitive process primarily on the basis of academic
24 merit and the nuclear forensics and attribution needs of
25 the United States Government;

26 (II) provide for the setting aside of up to 10 percent
27 of the scholarships or fellowships awarded under this
28 section for individuals who are Federal employees to en-
29 hance the education of the employees in areas of critical
30 nuclear forensics and attribution needs of the United
31 States Government, for doctoral education under the
32 scholarship or fellowship on a full-time or part-time
33 basis;

34 (III) provide that the Secretary may enter into a con-
35 tractual agreement with an institution of higher edu-
36 cation under which the amounts provided for a scholar-
37 ship under this section for tuition, fees, and other au-
38 thorized expenses are paid directly to the institution with
39 respect to which the scholarship is awarded;

40 (IV) require scholarship recipients to maintain satis-
41 factory academic progress; and

1 (V) require that—

2 (aa) a scholarship recipient who fails to maintain
3 a high level of academic standing, as defined by the
4 Secretary, who is dismissed for disciplinary reasons
5 from the educational institution the recipient is at-
6 tending, or who voluntarily terminates academic
7 training before graduation from the educational pro-
8 gram for which the scholarship was awarded is lia-
9 ble to the United States for repayment within 1
10 year after the date of default of all scholarship
11 funds paid to the recipient and to the institution of
12 higher education on the behalf of the recipient, pro-
13 vided that the repayment period may be extended by
14 the Secretary if the Secretary determines it nec-
15 essary, as established by regulation; and

16 (bb) a scholarship recipient who, for any reason
17 except death or disability, fails to begin or complete
18 the post-doctoral service requirements in a technical
19 nuclear forensics-related specialty at a national lab-
20 oratory or appropriate Federal agency after comple-
21 tion of academic training is liable to the United
22 States for an amount equal to—

23 (AA) the total amount of the scholarship re-
24 ceived by the recipient under this section; and

25 (BB) the interest on the amounts which
26 would be payable if at the time the scholarship
27 was received the scholarship was a loan bearing
28 interest at the maximum legally prevailing rate;

29 (M) provide an annual report to Congress on the activities car-
30 ried out under subparagraphs (J), (K), and (L); and

31 (N) perform other duties assigned by the Secretary.

32 (c) CHIEF MEDICAL OFFICER.—The Chief Medical Officer has the re-
33 sponsibility in the Department for medical issues related to natural disas-
34 ters, acts of terrorism, and other man-made disasters, including—

35 (1) serving as the principal advisor on medical and public health
36 issues to the Secretary, the Administrator of the Federal Emergency
37 Management Agency, the Assistant Secretary, and other Department
38 officials;

39 (2) providing operational medical support to all components of the
40 Department;

1 (3) as appropriate, providing medical liaisons to the components of
2 the Department, on a reimbursable basis, to provide subject matter ex-
3 pertise on operational medical issues;

4 (4) coordinating with Federal, State, local, and tribal governments,
5 the medical community, and others within and outside the Department,
6 including the Centers for Disease Control and Prevention and the Of-
7 fice of Assistant Secretary for Preparedness and Response of the De-
8 partment of Health and Human Services, with respect to medical and
9 public health matters; and

10 (5) performing other duties relating to these responsibilities that the
11 Secretary may require.

12 **§ 12505. Technology research and development investment**
13 **strategy for nuclear and radiological detection**

14 (a) IN GENERAL.—The Secretary, the Secretary of Energy, the Secretary
15 of Defense, and the Director of National Intelligence shall submit to Con-
16 gress a research and development investment strategy for nuclear and radio-
17 logical detection.

18 (b) CONTENTS.—The strategy under subsection (a) shall include—

19 (1) a long-term technology roadmap for nuclear and radiological de-
20 tection applicable to the mission needs of the Department, the Depart-
21 ment of Energy, the Department of Defense, and the Office of the Di-
22 rector of National Intelligence;

23 (2) budget requirements necessary to meet the roadmap; and

24 (3) documentation of how the Department, the Department of En-
25 ergy, the Department of Defense, and the Office of the Director of Na-
26 tional Intelligence will execute this strategy.

27 (c) ANNUAL REPORT.—The Assistant Secretary and the Under Secretary
28 for Science and Technology jointly and annually shall notify Congress that
29 the strategy and technology road map for nuclear and radiological detection
30 developed under subsections (a) and (b) is consistent with the national pol-
31 icy and strategic plan for identifying priorities, goals, objectives, and policies
32 for coordinating the Federal Government’s civilian efforts to identify and
33 develop countermeasures to terrorist threats from weapons of mass destruc-
34 tion that are required under section 10901(2) of this title.

35 **§ 12506. Testing authority**

36 (a) IN GENERAL.—The Assistant Secretary shall coordinate with the re-
37 sponsible Federal agency or other entity to facilitate the use by the Office,
38 by its contractors, or by other persons or entities, of existing Government
39 laboratories, centers, ranges, or other testing facilities for the testing of ma-
40 terials, equipment, models, computer software, and other items as may be
41 related to the responsibilities identified in section 12504(b) of this title. Use

1 of Government facilities shall be carried out in accordance with all applica-
2 ble laws, regulations, and contractual provisions, including those governing
3 security, safety, and environmental protection, including, when applicable,
4 section 10908 of this title. The Office may direct that private-sector entities
5 utilizing Government facilities under this section pay an appropriate fee to
6 the agency that owns or operates those facilities to defray additional costs
7 to the Government resulting from private-sector use.

8 (b) CONFIDENTIALITY OF TEST RESULTS.—The results of tests per-
9 formed with services made available shall be confidential and shall not be
10 disclosed outside the Federal Government without the consent of the per-
11 sons for whom the tests are performed.

12 (c) FEES.—Fees for services made available under this section shall not
13 exceed the amount necessary to recoup the direct and indirect costs in-
14 volved, such as direct costs of utilities, contractor support, and salaries of
15 personnel that are incurred by the United States to provide for the testing.

16 (d) USE OF FEES.—Fees received for services made available under this
17 section may be credited to the appropriation from which funds were ex-
18 pended to provide the services.

19 **§ 12507. Personnel**

20 (a) HIRING.—In hiring personnel for the Office, the Secretary has the
21 hiring and management authorities provided in section 1599h of title 10.
22 The term of appointments for employees under section 1599h(e)(1) of title
23 10 may not exceed 5 years before granting an extension under section
24 1599h(e)(2) of title 10.

25 (b) DETAIL.—The Secretary may request that the Secretary of Defense,
26 the Secretary of Energy, the Secretary of State, the Attorney General, the
27 Nuclear Regulatory Commission, and the directors of other Federal agen-
28 cies, including elements of the intelligence community, provide for the reim-
29 burable detail of personnel with relevant expertise to the Office.

30 **§ 12508. Contracting and grant making authorities**

31 The Secretary, acting through the Assistant Secretary, in carrying out
32 the responsibilities under section 12504(b) of this title shall—

33 (1) operate extramural and intramural programs and distribute
34 funds through grants, cooperative agreements, and other transactions
35 and contracts;

36 (2) ensure that activities under section 12504(b) of this title include
37 investigations of radiation detection equipment in configurations suit-
38 able for deployment at seaports, which may include underwater or
39 water surface detection equipment and detection equipment that can be
40 mounted on cranes and straddle cars used to move shipping containers;
41 and

1 (3) have the authority to establish or contract with one or more fed-
2 erally funded research and development centers to provide independent
3 analysis of homeland security issues and carry out other responsibilities
4 under this chapter.

5 **§ 12509. Joint annual interagency review of global nuclear**
6 **detection architecture**

7 (a) DEFINITION OF GLOBAL NUCLEAR DETECTION ARCHITECTURE.—In
8 this section, the term “global nuclear detection architecture” means the
9 global nuclear detection architecture developed under section 12504(b) of
10 this title.

11 (b) ANNUAL REVIEW.—

12 (1) IN GENERAL.—The Secretary, the Attorney General, the Sec-
13 retary of State, the Secretary of Defense, the Secretary of Energy, and
14 the Director of National Intelligence shall jointly ensure interagency co-
15 ordination on the development and implementation of the global nu-
16 clear detection architecture by ensuring that, not less frequently than
17 once each year—

18 (A) each relevant agency, office, or entity—

19 (i) assesses its involvement, support, and participation in
20 the development, revision, and implementation of the global
21 nuclear detection architecture; and

22 (ii) examines and evaluates components of the global nu-
23 clear detection architecture (including associated strategies
24 and acquisition plans) relating to the operations of that agen-
25 cy, office, or entity, to determine whether the components in-
26 corporate and address current threat assessments, scenarios,
27 or intelligence analyses developed by the Director of National
28 Intelligence or other agencies regarding threats relating to
29 nuclear or radiological weapons of mass destruction;

30 (B) each agency, office, or entity deploying or operating any nu-
31 clear or radiological detection technology under the global nuclear
32 detection architecture—

33 (i) evaluates the deployment and operation by that agency,
34 office, or entity of nuclear or radiological detection tech-
35 nologies under the global nuclear detection architecture;

36 (ii) identifies performance deficiencies and operational or
37 technical deficiencies in nuclear or radiological detection tech-
38 nologies deployed under the global nuclear detection architec-
39 ture; and

1 (iii) assesses the capacity of that agency, office, or entity
2 to implement the responsibilities of that agency, office, or en-
3 tity under the global nuclear detection architecture; and

4 (C) the Assistant Secretary and each of the relevant depart-
5 ments that are partners in the National Technical Forensics Cen-
6 ter—

7 (i) include, as part of the assessments, evaluations, and re-
8 views required under this paragraph, each office's or depart-
9 ment's activities and investments in support of nuclear
10 forensics and attribution activities and specific goals and ob-
11 jectives accomplished during the previous year pursuant to
12 the national strategic five-year plan for improving the nuclear
13 forensic and attribution capabilities of the United States re-
14 quired under section 1036 of the National Defense Authoriza-
15 tion Act for Fiscal Year 2010 (Public Law 111–84, 123 Stat.
16 2450);

17 (ii) attach, as an appendix to the Joint Interagency Annual
18 Review, the most current version of the strategy and plan;
19 and

20 (iii) include a description of new or amended bilateral and
21 multilateral agreements and efforts in support of nuclear
22 forensics and attribution activities accomplished during the
23 previous year.

24 (2) TECHNOLOGY.—Not less frequently than once each year, the
25 Secretary shall examine and evaluate the development, assessment, and
26 acquisition of radiation detection technologies deployed or implemented
27 in support of the domestic portion of the global nuclear detection archi-
28 tecture.

29 (c) ANNUAL REPORT ON JOINT INTERAGENCY REVIEW.—

30 (1) IN GENERAL.—Not later than March 31 of each year, the Sec-
31 retary, the Attorney General, the Secretary of State, the Secretary of
32 Defense, the Secretary of Energy, and the Director of National Intel-
33 ligence, shall jointly submit a report regarding the implementation of
34 this section and the results of the reviews required under subsection

35 (b) to—

36 (A) the President;

37 (B) the Committee on Appropriations, the Committee on Armed
38 Services, the Select Committee on Intelligence, and the Committee
39 on Homeland Security and Governmental Affairs of the Senate;
40 and

1 (C) the Committee on Appropriations, the Committee on Armed
2 Services, the Permanent Select Committee on Intelligence, the
3 Committee on Homeland Security, and the Committee on Science
4 and Technology of the House of Representatives.

5 (2) FORM.—The annual report submitted under paragraph (1) shall
6 be submitted in unclassified form to the maximum extent practicable,
7 but may include a classified annex.

8 **§ 12510. Securing the Cities program**

9 (a) ESTABLISHMENT.—The Secretary, through the Assistant Secretary,
10 shall establish the Securing the Cities (in this section referred to as “STC”)
11 program to enhance the ability of the United States to detect and prevent
12 terrorist attacks and other high-consequence events utilizing nuclear or
13 other radiological materials that pose a high risk to homeland security in
14 high-risk urban areas.

15 (b) ELEMENTS.—Through the STC program, the Secretary shall—

16 (1) assist State, local, tribal, and territorial governments in design-
17 ing and implementing, or enhancing existing, architectures for coordi-
18 nated and integrated detection and interdiction of nuclear or other ra-
19 diological materials that are out of regulatory control;

20 (2) support the development of an operating capability to detect and
21 report on nuclear and other radiological materials out of regulatory
22 control;

23 (3) provide resources to enhance detection, analysis, communication,
24 and coordination to better integrate State, local, tribal, and territorial
25 assets into Federal operations;

26 (4) facilitate alarm adjudication and provide subject matter expertise
27 and technical assistance on concepts of operation, training, exercises,
28 and alarm response protocols;

29 (5) communicate with, and promote sharing of information about the
30 presence or detection of nuclear or other radiological materials among,
31 appropriate Federal, State, local, tribal, and territorial government
32 agencies in a manner that ensures transparency with the jurisdictions
33 designated under subsection (c);

34 (6) provide augmenting resources, as appropriate, to enable State,
35 local, tribal, and territorial governments to sustain and refresh their
36 capabilities developed under the STC program;

37 (7) monitor expenditures under the STC program and track per-
38 formance in meeting the goals of the STC program; and

39 (8) provide any other assistance the Secretary determines appro-
40 priate.

41 (c) DESIGNATION OF JURISDICTIONS.—

1 (1) IN GENERAL.—In carrying out the STC program under sub-
2 section (a), the Secretary shall designate jurisdictions from among the
3 high-risk urban areas under section 12703 of this title.

4 (2) CONGRESSIONAL NOTIFICATION.—The Secretary shall notify the
5 Committee on Homeland Security and the Committee on Appropria-
6 tions of the House of Representatives and the Committee on Homeland
7 Security and Governmental Affairs and the Committee on Appropria-
8 tions of the Senate not later than 3 days before the designation of a
9 new jurisdiction under paragraph (1) or a change to a jurisdiction pre-
10 viously designated under paragraph (1).

11 (d) ACCOUNTABILITY.—

12 (1) IMPLEMENTATION.—

13 (A) IN GENERAL.—The Secretary shall develop, in consultation
14 with relevant stakeholders, an implementation plan for carrying
15 out the STC program that includes—

16 (i) a discussion of the goals of the STC program and a
17 strategy to achieve those goals;

18 (ii) performance metrics and milestones for the STC pro-
19 gram;

20 (iii) measures for achieving and sustaining capabilities
21 under the STC program; and

22 (iv) costs associated with achieving the goals of the STC
23 program.

24 (B) SUBMISSION TO CONGRESS.—Not later than 1 year after De-
25 cember 21, 2018, the Secretary shall submit to the appropriate
26 congressional committees and the Comptroller General the imple-
27 mentation plan required by subparagraph (A).

28 (2) REPORT REQUIRED.—Not later than 1 year after the submission
29 of the implementation plan under paragraph (1)(B), the Secretary shall
30 submit to the appropriate congressional committees and the Comp-
31 troller General a report that includes—

32 (A) an assessment of the effectiveness of the STC program,
33 based on the performance metrics and milestones required by
34 paragraph (1)(A); and

35 (B) proposals for changes to the STC program, including an ex-
36 planation of how those changes align with the strategy and goals
37 of the STC program and, as appropriate, address challenges faced
38 by the STC program.

39 (3) COMPTROLLER GENERAL REVIEW.—Not later than 18 months
40 after the submission of the report required by paragraph (2), the
41 Comptroller General shall submit to the appropriate congressional com-

1 mittees a report evaluating the implementation plan required by para-
2 graph (1) and the report required by paragraph (2), including an as-
3 sessment of progress made with respect to the performance metrics and
4 milestones required by paragraph (1)(A)(ii) and the sustainment of the
5 capabilities of the STC program.

6 (4) BRIEFING AND SUBMISSION REQUIREMENTS.—Before making
7 changes to the structure or requirements of the STC program, the As-
8 sistant Secretary shall—

9 (A) consult with appropriate congressional committees; and

10 (B) provide to those committees—

11 (i) a briefing on the proposed changes, including a jus-
12 tification for the changes;

13 (ii) documentation relating to the changes, including plans,
14 strategies, and resources to implement the changes; and

15 (iii) an assessment of the effect of the changes on the capa-
16 bilities of the STC program, taking into consideration pre-
17 vious resource allocations and stakeholder input.

18 **§ 12511. Medical countermeasures**

19 (a) DEFINITION OF MEDICAL COUNTERMEASURES.—In this section, the
20 term “medical countermeasures” means antibiotics, antivirals, antidotes,
21 therapeutics, radiological countermeasures, and other countermeasures that
22 may be deployed to protect the employees and working animals of the De-
23 partment in the event of a chemical, biological, radiological, nuclear, or ex-
24 plosives attack, naturally occurring disease outbreak, other event impacting
25 health, or pandemic.

26 (b) IN GENERAL.—Subject to the availability of appropriations, the Sec-
27 retary shall, as appropriate, establish a medical countermeasures program
28 within the components of the Department to—

29 (1) facilitate personnel readiness and protection for the employees
30 and working animals of the Department in the event of a chemical, bio-
31 logical, radiological, nuclear, or explosives attack, naturally occurring
32 disease outbreak, other event impacting health, or pandemic; and

33 (2) support the mission continuity of the Department.

34 (c) OVERSIGHT.—The Secretary, acting through the Chief Medical Offi-
35 cer, shall—

36 (1) provide programmatic oversight of the medical countermeasures
37 program established under subsection (b); and

38 (2) develop standards for—

39 (A) medical countermeasure storage, security, dispensing, and
40 documentation;

1 (B) maintaining a stockpile of medical countermeasures, includ-
2 ing antibiotics, antivirals, antidotes, therapeutics, and radiological
3 countermeasures, as appropriate;

4 (C) ensuring adequate partnerships with manufacturers and ex-
5 ecutive agencies that enable advance prepositioning by vendors of
6 inventories of appropriate medical countermeasures in strategic lo-
7 cations nationwide, based on risk and employee density, in accord-
8 ance with applicable Federal statutes and regulations;

9 (D) providing oversight and guidance regarding the dispensing
10 of stockpiled medical countermeasures;

11 (E) ensuring rapid deployment and dispensing of medical coun-
12 termeasures in a chemical, biological, radiological, nuclear, or ex-
13 plosives attack, naturally occurring disease outbreak, other event
14 impacting health, or pandemic;

15 (F) providing training to employees of the Department on med-
16 ical countermeasures; and

17 (G) supporting dispensing exercises.

18 (d) **MEDICAL COUNTERMEASURE WORKING GROUP.**—The Secretary, act-
19 ing through the Chief Medical Officer, shall establish a medical coun-
20 termeasures working group comprised of representatives from appropriate com-
21 ponents and offices of the Department to ensure that medical coun-
22 termeasures standards are maintained and guidance is consistent.

23 (e) **MEDICAL COUNTERMEASURES MANAGEMENT.**—NOT LATER THAN 120
24 DAYS AFTER THE DATE ON WHICH APPROPRIATIONS ARE MADE AVAILABLE
25 TO CARRY OUT SUBSECTION (B), THE CHIEF MEDICAL OFFICER SHALL DE-
26 VELOP AND SUBMIT TO THE SECRETARY AN INTEGRATED LOGISTICS SUP-
27 PORT PLAN FOR MEDICAL COUNTERMEASURES, INCLUDING—

28 (1) a methodology for determining the ideal types and quantities of
29 medical countermeasures to stockpile and how frequently the method-
30 ology shall be reevaluated;

31 (2) a replenishment plan; and

32 (3) inventory tracking, reporting, and reconciliation procedures for
33 existing stockpiles and new medical countermeasure purchases.

34 (f) **TRANSFER.**—Not later than 120 days after December 27, 2021, the
35 Secretary shall transfer all medical countermeasures-related programmatic
36 and personnel resources from the Under Secretary for Management to the
37 Chief Medical Officer.

38 (g) **STOCKPILE ELEMENTS.**—In determining the types and quantities of
39 medical countermeasures to stockpile under subsection (e), the Secretary,
40 acting through the Chief Medical Officer—

1 (1) shall use a risk-based methodology for evaluating types and
2 quantities of medical countermeasures required; and

3 (2) may use, if available—

4 (A) chemical, biological, radiological, and nuclear risk assess-
5 ments of the Department; and

6 (B) guidance on medical countermeasures of the Office of the
7 Assistant Secretary for Preparedness and Response and the Cen-
8 ters for Disease Control and Prevention.

9 (h) BRIEFING.—Not later than 180 days after December 27, 2021, the
10 Secretary shall provide a briefing to the Committee on Homeland Security
11 and Governmental Affairs of the Senate and the Committee on Homeland
12 Security of the House of Representatives regarding—

13 (1) the plan developed under subsection (e); and

14 (2) implementation of the requirements of this section.

15 **§ 12512. Annual report by Secretary**

16 Not later than 1 year after December 21, 2018, and annually thereafter,
17 the Secretary shall provide a briefing and report to the appropriate congres-
18 sional committees on—

19 (1) the organization and management of the chemical, biological, ra-
20 diological, and nuclear activities of the Department, including research
21 and development activities, and the location of each activity under the
22 organizational structure of the Office;

23 (2) a comprehensive inventory of chemical, biological, radiological,
24 and nuclear activities of the Department, including research and devel-
25 opment activities, highlighting areas of collaboration between compo-
26 nents, coordination with other agencies, and the effectiveness and ac-
27 complishments of consolidated chemical, biological, radiological, and
28 nuclear activities of the Department, including research and develop-
29 ment activities;

30 (3) information relating to how the organizational structure of the
31 Office will enhance the development of chemical, biological, radiological,
32 and nuclear priorities and capabilities of the Department;

33 (4) a discussion of any resulting cost savings and efficiencies gained
34 through activities described in paragraphs (1) and (2);

35 (5) information on how the Assistant Secretary is coordinating with
36 the Under Secretary of Science and Technology of the Department on
37 research and development activities; and

38 (6) recommendations for any necessary statutory changes, or, if no
39 statutory changes are necessary, an explanation of why no statutory or
40 organizational changes are necessary.

1 **Chapter 127—Homeland Security Grants**

Subchapter I—Grants to States, High-Risk Urban Areas, and Nonprofit Organizations

Part A—In General

Sec.

- 12701. Definitions.
- 12702. Homeland security grant programs.
- 12703. Urban Area Security Initiative.
- 12704. State Homeland Security Grant Program.
- 12705. Grants to directly eligible tribes.
- 12706. Terrorism prevention.
- 12707. Prioritization.
- 12708. Use of funds.
- 12709. Nonprofit Security Grant Program.

Part B—Administration

- 12721. Administration and coordination.
- 12722. Accountability.
- 12723. Identification of reporting redundancies and development of performance metrics.

Subchapter II—Grants To Address Cybersecurity Risks and Cybersecurity Threats to Information Systems

- 12731. Definitions.
- 12732. Program.
- 12733. Administration.
- 12734. Use of funds.
- 12735. Cybersecurity plans.
- 12736. Multi-entity grants.
- 12737. Planning committees.
- 12738. Special rule for Tribal governments.
- 12739. Review of plans.
- 12740. Limitation on use of funds.
- 12741. Opportunity to amend applications.
- 12742. Apportionment.
- 12743. Federal share.
- 12744. Responsibilities of grantees.
- 12745. Consultation with State, local, and Tribal representatives.
- 12746. Notification to Congress.
- 12747. Reports, study, and review.
- 12748. Authorization of appropriations.
- 12749. Termination.

2 **Subchapter I—Grants to States, High-Risk**

3 **Urban Areas, and Nonprofit Organizations**

4 **Part A—In General**

5 **§ 12701. Definitions**

6 In this subchapter:

7 (1) ADMINISTRATOR.—The term “Administrator” means the Admin-
8 strator of the Federal Emergency Management Agency.

9 (2) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appro-
10 priate committees of Congress” means—

11 (A) the Committee on Homeland Security and Governmental
12 Affairs of the Senate; and

13 (B) those committees of the House of Representatives that the
14 Speaker of the House of Representatives determines appropriate.

1 (3) CRITICAL INFRASTRUCTURE SECTORS.—The term “critical infra-
2 structure sectors” means the following sectors, in both urban and rural
3 areas:

4 (A) Agriculture and food.

5 (B) Banking and finance.

6 (C) Chemical industries.

7 (D) Commercial facilities.

8 (E) Commercial nuclear reactors, materials, and waste.

9 (F) Dams.

10 (G) The defense industrial base.

11 (H) Emergency services.

12 (I) Energy.

13 (J) Government facilities.

14 (K) Information technology.

15 (L) National monuments and icons.

16 (M) Postal and shipping.

17 (N) Public health and health care.

18 (O) Telecommunications.

19 (P) Transportation systems.

20 (Q) Water.

21 (4) DIRECTLY ELIGIBLE TRIBE.—The term “directly eligible tribe”
22 means—

23 (A) an Indian tribe—

24 (i) that is located in the continental United States;

25 (ii) that operates a law enforcement or emergency response
26 agency with the capacity to respond to calls for law enforce-
27 ment or emergency services;

28 (iii) that—

29 (I) is located on or near an international border or a
30 coastline bordering an ocean (including the Gulf of Mex-
31 ico) or international waters;

32 (II) is located within 10 miles of a system or asset in-
33 cluded on the prioritized critical infrastructure list estab-
34 lished under section 10712(a)(2) of this title or has such
35 a system or asset within its territory;

36 (III) is located within or contiguous to one of the 50
37 most populous metropolitan statistical areas in the
38 United States; or

39 (IV) has jurisdiction over not less than 1,000 square
40 miles of Indian country, as that term is defined in sec-
41 tion 1151 of title 18; and

1 (iv) that certifies to the Secretary that a State has not pro-
2 vided funds under section 12703 or 12704 of this title to the
3 Indian tribe or consortium of Indian tribes for the purpose
4 for which direct funding is sought; and

5 (B) a consortium of Indian tribes, if each tribe satisfies the re-
6 quirements of subparagraph (A).

7 (5) ELIGIBLE METROPOLITAN AREA.—The term “eligible metropoli-
8 tan area” means any of the 100 most populous metropolitan statistical
9 areas in the United States.

10 (6) HIGH-RISK URBAN AREA.—The term “high-risk urban area”
11 means a high-risk urban area designated under section 12703(b)(3)(A)
12 of this title.

13 (7) INDIAN TRIBE.—The term “Indian tribe” has the meaning given
14 the term in section 4(e) of the Indian Self-Determination and Edu-
15 cation Assistance Act (25 U.S.C. 450b(e)).

16 (8) METROPOLITAN STATISTICAL AREA.—The term “metropolitan
17 statistical area” means a metropolitan statistical area, as defined by
18 the Office of Management and Budget.

19 (9) NATIONAL SPECIAL SECURITY EVENT.—The term “National Spe-
20 cial Security Event” means a designated event that, by virtue of its po-
21 litical, economic, social, or religious significance, may be the target of
22 terrorism or other criminal activity.

23 (10) POPULATION.—The term “population” means population ac-
24 cording to the most recent United States census population estimates
25 available at the start of the relevant fiscal year.

26 (11) POPULATION DENSITY.—The term “population density” means
27 population divided by land area in square miles.

28 (12) QUALIFIED INTELLIGENCE ANALYST.—The term “qualified in-
29 telligence analyst” means an intelligence analyst (as that term is de-
30 fined in section 10512(a) of this title), including law enforcement per-
31 sonnel—

32 (A) who has successfully completed training to ensure baseline
33 proficiency in intelligence analysis and production, as determined
34 by the Secretary, which may include training using a curriculum
35 developed under section 10510 of this title; or

36 (B) whose experience ensures baseline proficiency in intelligence
37 analysis and production equivalent to the training required under
38 subparagraph (A), as determined by the Secretary.

39 (13) TARGET CAPABILITIES.—The term “target capabilities” means
40 the target capabilities for Federal, State, local, and tribal government

1 preparedness for which guidelines are required to be established under
2 section 20506 of this title.

3 (14) TRIBAL GOVERNMENT.—The term “tribal government” means
4 the government of an Indian tribe.

5 **§ 12702. Homeland security grant programs**

6 (a) GRANTS AUTHORIZED.—The Secretary, acting through the Adminis-
7 trator, may award grants under sections 12703, 12704, and 12709 of this
8 title to State, local, and tribal governments.

9 (b) PROGRAMS NOT AFFECTED.—This subchapter shall not be construed
10 to affect any of the following Federal programs:

11 (1) Firefighter and other assistance programs authorized under the
12 Federal Fire Prevention and Control Act of 1974 (15 U.S.C. 2201 et
13 seq.).

14 (2) Grants authorized under the Robert T. Stafford Disaster Relief
15 and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

16 (3) Emergency Management Performance Grants under the amend-
17 ments made by title II of the Implementing Recommendations of the
18 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 294).

19 (4) Grants to protect critical infrastructure, including port security
20 grants authorized under section 70107 of title 46, and grants author-
21 ized under titles XIV and XV of the Implementing Recommendations
22 of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat.
23 400, 422) and the amendments made by those titles.

24 (5) The Metropolitan Medical Response System authorized under
25 section 20304 of this title.

26 (6) The Interoperable Emergency Communications Grant Program
27 authorized under section 12309 of this title.

28 (7) Grant programs other than those administered by the Depart-
29 ment.

30 (c) RELATIONSHIP TO OTHER LAWS.—

31 (1) IN GENERAL.—The grant programs authorized under sections
32 12703 and 12704 of this title supersede all grant programs authorized
33 under section 1014 of the USA PATRIOT Act (42 U.S.C. 3714).

34 (2) ALLOCATION.—The allocation of grants authorized under sec-
35 tions 12703 and 12704 of this title is governed by the terms of this
36 subchapter and not by any other provision of law.

37 **§ 12703. Urban Area Security Initiative**

38 (a) ESTABLISHMENT.—There is in the Department the Urban Area Secu-
39 rity Initiative to provide grants to assist high-risk urban areas in pre-
40 venting, preparing for, protecting against, and responding to acts of ter-
41 rorism.

1 (b) ASSESSMENT AND DESIGNATION OF HIGH-RISK URBAN AREAS.—

2 (1) IN GENERAL.—The Secretary shall designate high-risk urban
3 areas to receive grants under this section based on procedures under
4 this subsection.

5 (2) INITIAL ASSESSMENT.—

6 (A) IN GENERAL.—For each fiscal year, the Secretary shall con-
7 duct an initial assessment of the relative threat, vulnerability, and
8 consequences from acts of terrorism faced by each eligible metro-
9 politan area, including consideration of—

10 (i) the factors set forth in subparagraphs (A) through (H)
11 and (K) of section 12707(a)(1) of this title; and

12 (ii) information and materials submitted under subpara-
13 graph (B).

14 (B) SUBMISSION OF INFORMATION BY ELIGIBLE METROPOLITAN
15 AREAS.—Prior to conducting each initial assessment under sub-
16 paragraph (A), the Secretary shall provide each eligible metropoli-
17 tan area with, and shall notify each eligible metropolitan area of,
18 the opportunity to—

19 (i) submit information that the eligible metropolitan area
20 believes to be relevant to the determination of the threat, vul-
21 nerability, and consequences it faces from acts of terrorism;
22 and

23 (ii) review the risk assessment conducted by the Depart-
24 ment of that eligible metropolitan area, including the bases
25 for the assessment by the Department of the threat, vulner-
26 ability, and consequences from acts of terrorism faced by that
27 eligible metropolitan area, and remedy erroneous or incom-
28 plete information.

29 (3) DESIGNATION OF HIGH-RISK URBAN AREAS.—

30 (A) IN GENERAL.—

31 (i) DESIGNATION.—For each fiscal year, after conducting
32 the initial assessment under paragraph (2), and based on that
33 assessment, the Secretary shall designate high-risk urban
34 areas that may submit applications for grants under this sec-
35 tion.

36 (ii) EXCEPTIONS.—Notwithstanding paragraph (2), the
37 Secretary may—

38 (I) in any case where an eligible metropolitan area
39 consists of more than one metropolitan division (as that
40 term is defined by the Office of Management and Budg-

1 et) designate more than one high-risk urban area within
2 a single eligible metropolitan area; and

3 (II) designate an area that is not an eligible metropoli-
4 tan area as a high-risk urban area based on the assess-
5 ment by the Secretary of the relative threat, vulner-
6 ability, and consequences from acts of terrorism faced by
7 the area.

8 (iii) SECRETARY NOT REQUIRED TO DESIGNATE ALL ELIGI-
9 BLE AREAS AS HIGH-RISK URBAN AREAS.—Nothing in this
10 subsection may be construed to require the Secretary to—

11 (I) designate all eligible metropolitan areas that sub-
12 mit information to the Secretary under paragraph
13 (2)(B)(i) as high-risk urban areas; or

14 (II) designate all areas within an eligible metropolitan
15 area as part of the high-risk urban area.

16 (B) JURISDICTIONS INCLUDED IN HIGH-RISK URBAN AREAS.—

17 (i) BY SECRETARY.—In designating high-risk urban areas
18 under subparagraph (A), the Secretary shall determine which
19 jurisdictions, at a minimum, shall be included in each high-
20 risk urban area.

21 (ii) BY HIGH-RISK URBAN AREA.—A high-risk urban area
22 designated by the Secretary may, in consultation with the
23 State or States in which the high-risk urban area is located,
24 add additional jurisdictions to the high-risk urban area.

25 (c) APPLICATION.—

26 (1) IN GENERAL.—An area designated as a high-risk urban area
27 under subsection (b) may apply for a grant under this section.

28 (2) MINIMUM CONTENTS OF APPLICATION.—In an application for a
29 grant under this section, a high-risk urban area shall submit—

30 (A) a plan describing the proposed division of responsibilities
31 and distribution of funding among the local and tribal govern-
32 ments in the high-risk urban area;

33 (B) the name of an individual to serve as a high-risk urban area
34 liaison with the Department and among the various jurisdictions
35 in the high-risk urban area; and

36 (C) information in support of the application the Secretary may
37 reasonably require.

38 (3) ANNUAL APPLICATIONS.—Applicants for grants under this sec-
39 tion shall apply or reapply on an annual basis.

40 (4) STATE REVIEW AND TRANSMISSION.—

1 (A) IN GENERAL.—To ensure consistency with State homeland
2 security plans, a high-risk urban area applying for a grant under
3 this section shall submit its application to each State within which
4 any part of that high-risk urban area is located for review before
5 submission of the application to the Department.

6 (B) DEADLINE.—Not later than 30 days after receiving an ap-
7 plication from a high-risk urban area under subparagraph (A), a
8 State shall transmit the application to the Department.

9 (C) OPPORTUNITY FOR STATE COMMENT.—If the Governor of
10 a State determines that an application of a high-risk urban area
11 is inconsistent with the State homeland security plan of that
12 State, or otherwise does not support the application, the Governor
13 shall—

- 14 (i) notify the Secretary, in writing, of that fact; and
15 (ii) provide an explanation of the reason for not supporting
16 the application at the time of transmission of the application.

17 (5) OPPORTUNITY TO AMEND.—In considering applications for
18 grants under this section, the Secretary shall provide applicants with
19 a reasonable opportunity to correct defects in the application, if any,
20 before making final awards.

21 (d) DISTRIBUTION OF AWARDS.—

22 (1) IN GENERAL.—If the Secretary approves the application of a
23 high-risk urban area for a grant under this section, the Secretary shall
24 distribute the grant funds to the State or States in which that high-
25 risk urban area is located.

26 (2) STATE DISTRIBUTION OF FUNDS.—

27 (A) IN GENERAL.—Not later than 45 days after the date on
28 which a State receives grant funds under paragraph (1), that
29 State shall provide the high-risk urban area awarded that grant
30 not less than 80 percent of the grant funds. Any funds retained
31 by a State shall be expended on items, services, or activities that
32 benefit the high-risk urban area.

33 (B) FUNDS RETAINED.—A State shall provide each relevant
34 high-risk urban area with an accounting of the items, services, or
35 activities on which any funds retained by the State under subpara-
36 graph (A) were expended.

37 (3) INTERSTATE URBAN AREAS.—If parts of a high-risk urban area
38 awarded a grant under this section are located in 2 or more States,
39 the Secretary shall distribute to each State—

40 (A) a portion of the grant funds in accordance with the pro-
41 posed distribution set forth in the application; or

1 (B) if no agreement on distribution has been reached, a portion
2 of the grant funds determined by the Secretary to be appropriate.

3 (4) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS
4 TO HIGH-RISK URBAN AREAS.—A State that receives grant funds under
5 paragraph (1) shall certify to the Secretary that the State has made
6 available to the applicable high-risk urban area the required funds
7 under paragraph (2).

8 **§ 12704. State Homeland Security Grant Program**

9 (a) ESTABLISHMENT.—There is in the Department a State Homeland Se-
10 curity Grant Program to assist State, local, and tribal governments in pre-
11 venting, preparing for, protecting against, and responding to acts of ter-
12 rorism.

13 (b) APPLICATION.—

14 (1) IN GENERAL.—Each State may apply for a grant under this sec-
15 tion and shall submit information in support of the application that the
16 Secretary may reasonably require.

17 (2) MINIMUM CONTENTS OF APPLICATION.—The Secretary shall re-
18 quire that each State include in its application, at a minimum—

19 (A) the purpose for which the State seeks grant funds and the
20 reasons why the State needs the grant to meet the target capabili-
21 ties of that State;

22 (B) a description of how the State plans to allocate the grant
23 funds to local governments and Indian tribes; and

24 (C) a budget showing how the State intends to expend the grant
25 funds.

26 (3) ANNUAL APPLICATIONS.—Applicants for grants under this sec-
27 tion shall apply or reapply on an annual basis.

28 (c) DISTRIBUTION TO LOCAL AND TRIBAL GOVERNMENTS.—

29 (1) IN GENERAL.—Not later than 45 days after receiving grant
30 funds, any State receiving a grant under this section shall make avail-
31 able to local and tribal governments, consistent with the applicable
32 State homeland security plan—

33 (A) not less than 80 percent of the grant funds;

34 (B) with the consent of local and tribal governments, items,
35 services, or activities having a value of not less than 80 percent
36 of the amount of the grant; or

37 (C) with the consent of local and tribal governments, grant
38 funds combined with other items, services, or activities having a
39 total value of not less than 80 percent of the amount of the grant.

40 (2) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS
41 TO LOCAL GOVERNMENTS.—A State shall certify to the Secretary that

1 the State has made the distribution to local and tribal governments re-
2 quired under paragraph (1).

3 (3) EXTENSION OF PERIOD.—The Governor of a State may request
4 in writing that the Secretary extend the period under paragraph (1)
5 for an additional period of time. The Secretary may approve a request
6 if the Secretary determines that the resulting delay in providing grant
7 funding to the local and tribal governments is necessary to promote ef-
8 fective investments to prevent, prepare for, protect against, or respond
9 to acts of terrorism.

10 (4) EXCEPTION.—Paragraph (1) does not apply to the District of
11 Columbia, Puerto Rico, American Samoa, the Northern Mariana Is-
12 lands, Guam, or the Virgin Islands.

13 (5) DIRECT FUNDING.—If a State fails to make the distribution to
14 local or tribal governments required under paragraph (1) in a timely
15 fashion, a local or tribal government entitled to receive the distribution
16 may petition the Secretary to request that grant funds be provided di-
17 rectly to the local or tribal government.

18 (d) MULTISTATE APPLICATIONS.—

19 (1) IN GENERAL.—Instead of, or in addition to, any application for
20 a grant under subsection (b), 2 or more States may submit an applica-
21 tion for a grant under this section in support of multistate efforts to
22 prevent, prepare for, protect against, and respond to acts of terrorism.

23 (2) ADMINISTRATION OF GRANT.—If a group of States applies for
24 a grant under this section, the States shall submit to the Secretary at
25 the time of application a plan describing—

26 (A) the division of responsibilities for administering the grant;
27 and

28 (B) the distribution of funding among the States that are par-
29 ties to the application.

30 (e) MINIMUM ALLOCATION.—

31 (1) IN GENERAL.—In allocating funds under this section, the Sec-
32 retary shall ensure that—

33 (A) except as provided in subparagraph (B), each State receives
34 for each fiscal year, from the funds appropriated for the State
35 Homeland Security Grant Program established under this section,
36 not less than 0.35 percent of the total funds appropriated for
37 grants under this section and section 12703 of this title; and

38 (B) for each fiscal year, American Samoa, the Northern Mar-
39 iana Islands, Guam, and the Virgin Islands each receive, from the
40 funds appropriated for the State Homeland Security Grant Pro-
41 gram established under this section, not less than an amount

1 equal to 0.08 percent of the total funds appropriated for grants
2 under this section and section 12703 of this title.

3 (2) EFFECT OF MULTISTATE AWARD ON STATE MINIMUM.—Any por-
4 tion of a multistate award provided to a State under subsection (d)
5 shall be considered in calculating the minimum State allocation under
6 this subsection.

7 **§ 12705. Grants to directly eligible tribes**

8 (a) IN GENERAL.—Notwithstanding section 12704(b) of this title, the
9 Secretary, acting through the Administrator, may award grants to directly
10 eligible tribes under section 12704 of this title.

11 (b) TRIBAL APPLICATIONS.—A directly eligible tribe may apply for a
12 grant under section 12704 of this title by submitting an application to the
13 Secretary that includes, as appropriate, the information required for an ap-
14 plication by a State under section 12704(b) of this title.

15 (c) CONSISTENCY WITH STATE PLANS.—

16 (1) IN GENERAL.—To ensure consistency with any applicable State
17 homeland security plan, a directly eligible tribe applying for a grant
18 under section 12704 of this title shall provide a copy of its application
19 to each State within which any part of the tribe is located for review
20 before the tribe submits the application to the Department.

21 (2) OPPORTUNITY FOR COMMENT.—If the Governor of a State deter-
22 mines that the application of a directly eligible tribe is inconsistent
23 with the State homeland security plan of that State, or otherwise does
24 not support the application, not later than 30 days after the date of
25 receipt of that application, the Governor shall—

26 (A) notify the Secretary, in writing, of that fact; and

27 (B) provide an explanation of the reason for not supporting the
28 application.

29 (d) FINAL AUTHORITY.—The Secretary shall have final authority to ap-
30 prove any application of a directly eligible tribe. The Secretary shall notify
31 each State within the boundaries of which any part of a directly eligible
32 tribe is located of the approval of an application by the tribe.

33 (e) PRIORITIZATION.—The Secretary shall allocate funds to directly eligi-
34 ble tribes in accordance with the factors applicable to allocating funds
35 among States under section 12707 of this title.

36 (f) DISTRIBUTION OF AWARDS TO DIRECTLY ELIGIBLE TRIBES.—If the
37 Secretary awards funds to a directly eligible tribe under this section, the
38 Secretary shall distribute the grant funds directly to the tribe and not
39 through any State.

40 (g) MINIMUM ALLOCATION.—

1 (1) IN GENERAL.—In allocating funds under this section, the Sec-
2 retary shall ensure that, for each fiscal year, directly eligible tribes col-
3 lectively receive, from the funds appropriated for the State Homeland
4 Security Grant Program established under section 12704 of this title,
5 not less than an amount equal to 0.1 percent of the total funds appro-
6 priated for grants under sections 12703 and 12704 of this title.

7 (2) EXCEPTION.—This subsection shall not apply in any fiscal year
8 in which the Secretary—

9 (A) receives fewer than 5 applications under this section; or

10 (B) does not approve at least 2 applications under this section.

11 (h) TRIBAL LIAISON.—A directly eligible tribe applying for a grant under
12 section 12704 of this title shall designate an individual to serve as a tribal
13 liaison with the Department and other Federal, State, local, and regional
14 government officials concerning preventing, preparing for, protecting
15 against, and responding to acts of terrorism.

16 (i) ELIGIBILITY FOR OTHER FUNDS.—A directly eligible tribe that re-
17 ceives a grant under section 12704 of this title may receive funds for other
18 purposes under a grant from the State or States within the boundaries of
19 which any part of the tribe is located and from any high-risk urban area
20 of which it is a part, consistent with the homeland security plan of the State
21 or high-risk urban area.

22 (j) STATE OBLIGATIONS.—

23 (1) IN GENERAL.—States are responsible for allocating grant funds
24 received under section 12704 of this title to tribal governments in order
25 to help those tribal communities achieve target capabilities not achieved
26 through grants to directly eligible tribes.

27 (2) DISTRIBUTION OF GRANT FUNDS.—With respect to a grant to
28 a State under section 12704 of this title, an Indian tribe shall be eligi-
29 ble for funding directly from that State, and shall not be required to
30 seek funding from any local government.

31 (3) IMPOSITION OF REQUIREMENTS.—A State may not impose un-
32 reasonable or unduly burdensome requirements on an Indian tribe as
33 a condition of providing the Indian tribe with grant funds or resources
34 under section 12704 of this title.

35 (k) RULE OF CONSTRUCTION.—Nothing in this section shall be construed
36 to affect the authority of an Indian tribe that receives funds under this sub-
37 chapter.

38 § 12706. Terrorism prevention

39 (a) LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM.—

40 (1) IN GENERAL.—The Secretary, acting through the Administrator,
41 shall ensure that not less than 25 percent of the total combined funds

1 appropriated for grants under sections 12703 and 12704 of this title
2 is used for law enforcement terrorism prevention activities.

3 (2) LAW ENFORCEMENT TERRORISM PREVENTION ACTIVITIES.—Law
4 enforcement terrorism prevention activities include—

5 (A) information sharing and analysis;

6 (B) target hardening;

7 (C) threat recognition;

8 (D) terrorist interdiction;

9 (E) training exercises to enhance preparedness for and response
10 to mass casualty and active shooter incidents and security events
11 at public locations, including airports and mass transit systems;

12 (F) overtime expenses consistent with a State homeland security
13 plan, including for the provision of enhanced law enforcement op-
14 erations in support of Federal agencies, including for increased
15 border security and border crossing enforcement;

16 (G) establishing, enhancing, and staffing with appropriately
17 qualified personnel, State, local, and regional fusion centers that
18 comply with the guidelines established under section 10512(j) of
19 this title;

20 (H) paying salaries and benefits for personnel, including individ-
21 uals employed by the grant recipient on the date of the relevant
22 grant application, to serve as qualified intelligence analysts;

23 (I) any other activity permitted under the Fiscal Year 2007
24 Program Guidance of the Department for the Law Enforcement
25 Terrorism Prevention Program; and

26 (J) any other terrorism prevention activity authorized by the
27 Secretary.

28 (3) PARTICIPATION OF UNDERREPRESENTED COMMUNITIES IN FU-
29 SION CENTERS.—The Secretary shall ensure that grant funds described
30 in paragraph (1) are used to support the participation in fusion cen-
31 ters, as appropriate, of law enforcement and other emergency response
32 providers from rural and other underrepresented communities at risk
33 from acts of terrorism.

34 (b) OFFICE FOR STATE AND LOCAL LAW ENFORCEMENT.—

35 (1) ESTABLISHMENT.—There is in the Policy Directorate of the De-
36 partment the Office for State and Local Law Enforcement.

37 (2) ASSISTANT SECRETARY FOR STATE AND LOCAL LAW ENFORCE-
38 MENT.—The Assistant Secretary for State and Local Law Enforce-
39 ment—

40 (A) is the head of the Office for State and Local Law Enforce-
41 ment; and

1 (B) shall have an appropriate background with experience in
2 law enforcement, intelligence, and other counterterrorism func-
3 tions.

4 (3) ASSIGNMENT OF PERSONNEL.—The Secretary shall assign to the
5 Office for State and Local Law Enforcement permanent staff and, as
6 appropriate and consistent with sections 10311(a), 10312(b)(2), and
7 11306(b)(2) of this title, other appropriate personnel detailed from
8 other components of the Department to carry out the responsibilities
9 under this subsection.

10 (4) RESPONSIBILITIES.—The Assistant Secretary for State and
11 Local Law Enforcement shall—

12 (A) lead the coordination of Department-wide policies relating
13 to the role of State and local law enforcement in preventing, pre-
14 paring for, protecting against, and responding to natural disasters,
15 acts of terrorism, and other man-made disasters within the United
16 States;

17 (B) serve as a liaison between State, local, and tribal law en-
18 forcement agencies and the Department;

19 (C) coordinate with the Office of Intelligence and Analysis to
20 ensure the intelligence and information sharing requirements of
21 State, local, and tribal law enforcement agencies are being ad-
22 dressed;

23 (D) work with the Secretary to ensure that law enforcement and
24 terrorism-focused grants to State, local, and tribal government
25 agencies, including grants under sections 12703 and 12704 of this
26 title, the Commercial Equipment Direct Assistance Program, and
27 other grants administered by the Department to support fusion
28 centers and law enforcement-oriented programs, are appropriately
29 focused on terrorism prevention activities;

30 (E) coordinate with the Directorate of Science and Technology,
31 the Federal Emergency Management Agency, the Department of
32 Justice, the National Institute of Justice, law enforcement organi-
33 zations, and other appropriate entities to support the development,
34 promulgation, and updating, as necessary, of national voluntary
35 consensus standards for training and personal protective equip-
36 ment to be used in a tactical environment by law enforcement offi-
37 cers; and

38 (F) conduct, jointly with the Secretary, a study to determine the
39 efficacy and feasibility of establishing specialized law enforcement
40 deployment teams to assist State, local, and tribal governments in
41 responding to natural disasters, acts of terrorism, or other man-

1 made disasters and report on the results of that study to the ap-
2 propriate committees of Congress.

3 (5) RULE OF CONSTRUCTION.—Nothing in this subsection shall be
4 construed to diminish, supersede, or replace the responsibilities, au-
5 thorities, or role of the Secretary.

6 **§ 12707. Prioritization**

7 (a) IN GENERAL.—In allocating funds among States and high-risk urban
8 areas applying for grants under section 12703 or 12704 of this title, the
9 Secretary, acting through the Administrator, shall consider, for each State
10 or high-risk urban area—

11 (1) its relative threat, vulnerability, and consequences from acts of
12 terrorism, including consideration of—

13 (A) its population, including appropriate consideration of mili-
14 tary, tourist, and commuter populations;

15 (B) its population density;

16 (C) its history of threats, including whether it has been the tar-
17 get of a prior act of terrorism;

18 (D) its degree of threat, vulnerability, and consequences related
19 to critical infrastructure (for all critical infrastructure sectors) or
20 key resources identified by the Secretary or the State homeland
21 security plan, including threats, vulnerabilities, and consequences
22 related to critical infrastructure or key resources in nearby juris-
23 dictions;

24 (E) the most current threat assessments available to the De-
25 partment;

26 (F) whether the State has, or the high-risk urban area is lo-
27 cated at or near, an international border;

28 (G) whether it has a coastline bordering an ocean (including the
29 Gulf of Mexico) or international waters;

30 (H) its likely need to respond to acts of terrorism occurring in
31 nearby jurisdictions;

32 (I) the extent to which it has unmet target capabilities;

33 (J) in the case of a high-risk urban area, the extent to which
34 that high-risk urban area includes—

35 (i) those incorporated municipalities, counties, parishes,
36 and Indian tribes within the relevant eligible metropolitan
37 area, the inclusion of which will enhance regional efforts to
38 prevent, prepare for, protect against, and respond to acts of
39 terrorism; and

1 (ii) other local and tribal governments in the surrounding
2 area that are likely to be called upon to respond to acts of
3 terrorism within the high-risk urban area; and

4 (K) such other factors as are specified in writing by the Sec-
5 retary; and

6 (2) the anticipated effectiveness of the proposed use of the grant by
7 the State or high-risk urban area in increasing the ability of that State
8 or high-risk urban area to prevent, prepare for, protect against, and
9 respond to acts of terrorism, to meet its target capabilities, and to oth-
10 erwise reduce the overall risk to the high-risk urban area, the State,
11 or the Nation.

12 (b) TYPES OF THREAT.—In assessing threat under this section, the Sec-
13 retary shall consider the following types of threat to critical infrastructure
14 sectors and to populations in all areas of the United States, urban and
15 rural:

16 (1) Biological.

17 (2) Chemical.

18 (3) Cyber.

19 (4) Explosives.

20 (5) Incendiary.

21 (6) Nuclear.

22 (7) Radiological.

23 (8) Suicide bombers.

24 (9) Other types of threat determined relevant by the Secretary.

25 **§ 12708. Use of funds**

26 (a) PERMITTED USES.—The Secretary, acting through the Administrator,
27 shall permit the recipient of a grant under section 12703 or 12704 of this
28 title to use grant funds to achieve target capabilities related to preventing,
29 preparing for, protecting against, and responding to acts of terrorism, con-
30 sistent with a State homeland security plan and relevant local, tribal, and
31 regional homeland security plans, including by working in conjunction with
32 a National Laboratory (as defined in section 2 of the Energy Policy Act
33 of 2005 (42 U.S.C. 15801)), through—

34 (1) developing and enhancing homeland security, emergency manage-
35 ment, or other relevant plans, assessments, or mutual aid agreements;

36 (2) designing, conducting, and evaluating training and exercises, in-
37 cluding training and exercises conducted under sections 11312 and
38 20508 of this title;

39 (3) protecting a system or asset included on the prioritized critical
40 infrastructure list established under section 10712(a)(2) of this title;

1 (4) purchasing, upgrading, storing, or maintaining equipment, in-
2 cluding computer hardware and software;

3 (5) ensuring operability and achieving interoperability of emergency
4 communications;

5 (6) responding to an increase in the threat level under the Homeland
6 Security Advisory System, or to the needs resulting from a National
7 Special Security Event;

8 (7) establishing, enhancing, and staffing with appropriately qualified
9 personnel, State, local, and regional fusion centers that comply with the
10 guidelines established under section 10512(j) of this title;

11 (8) enhancing school preparedness;

12 (9) enhancing the security and preparedness of secure and nonsecure
13 areas of eligible airports and surface transportation systems;

14 (10) supporting public safety answering points;

15 (11) paying salaries and benefits for personnel, including individuals
16 employed by the grant recipient on the date of the relevant grant appli-
17 cation, to serve as qualified intelligence analysts, regardless of whether
18 the analysts are current or new full-time employees or contract employ-
19 ees;

20 (12) paying expenses directly relating to administration of the grant,
21 except that expenses may not exceed 3 percent of the amount of the
22 grant;

23 (13) participating in any activity permitted under the Fiscal Year
24 2007 Program Guidance of the Department for the State Homeland
25 Security Grant Program, the Urban Area Security Initiative (including
26 activities permitted under the full-time counterterrorism staffing pilot),
27 or the Law Enforcement Terrorism Prevention Program;

28 (14) migrating an online service (as defined in section 10881(b) of
29 this title) to the .gov internet domain; and

30 (15) participating in any other appropriate activity, as determined by
31 the Secretary.

32 (b) LIMITATIONS ON USE OF FUNDS.—

33 (1) IN GENERAL.—Funds provided under section 12703 or 12704 of
34 this title may not be used—

35 (A) to supplant State or local funds, except that nothing in this
36 paragraph shall prohibit the use of grant funds provided to a
37 State or high-risk urban area for otherwise permissible uses under
38 subsection (a) on the basis that a State or high-risk urban area
39 has previously used State or local funds to support the same or
40 similar uses; or

41 (B) for any State or local government cost-sharing contribution.

1 (2) PERSONNEL.—

2 (A) IN GENERAL.—Not more than 50 percent of the amount
3 awarded to a grant recipient under section 12703 or 12704 of this
4 title in any fiscal year may be used to pay for personnel, including
5 overtime and backfill costs, in support of the permitted uses under
6 subsection (a).

7 (B) WAIVER.—At the request of the recipient of a grant under
8 section 12703 or 12704 of this title, the Secretary may grant a
9 waiver of the limitation under subparagraph (A).

10 (3) LIMITATIONS ON DISCRETION.—

11 (A) IN GENERAL.—With respect to the use of amounts awarded
12 to a grant recipient under section 12703 or 12704 of this title for
13 personnel costs under paragraph (2), the Secretary may not—

14 (i) impose a limit on the amount of the award that may
15 be used to pay for personnel, or personnel-related, costs that
16 is higher or lower than the percent limit imposed in para-
17 graph (2)(A); or

18 (ii) impose any additional limitation on the portion of the
19 funds of a recipient that may be used for a specific type, pur-
20 pose, or category of personnel, or personnel-related, costs.

21 (B) ANALYSTS.—If amounts awarded to a grant recipient under
22 section 12703 or 12704 of this title are used for paying salary or
23 benefits of a qualified intelligence analyst under subsection
24 (a)(11), the Secretary shall make the amounts available without
25 limitations placed on the period of time that the analyst can serve
26 under the grant.

27 (4) CONSTRUCTION.—

28 (A) IN GENERAL.—A grant awarded under section 12703 or
29 12704 of this title may not be used to acquire land or to construct
30 buildings or other physical facilities.

31 (B) EXCEPTIONS.—

32 (i) IN GENERAL.—Notwithstanding subparagraph (A),
33 nothing in this paragraph shall prohibit the use of a grant
34 awarded under section 12703 or 12704 of this title to achieve
35 target capabilities related to preventing, preparing for, pro-
36 tecting against, or responding to acts of terrorism, including
37 through the alteration or remodeling of existing buildings for
38 the purpose of making the buildings secure against acts of
39 terrorism.

1 (ii) REQUIREMENTS FOR EXCEPTION.—No grant awarded
2 under section 12703 or 12704 of this title may be used for
3 a purpose described in clause (i) unless—

4 (I) the grant is specifically approved by the Secretary;

5 (II) any construction work occurs under terms and
6 conditions consistent with the requirements under section
7 611(j)(9) of the Robert T. Stafford Disaster Relief and
8 Emergency Assistance Act (42 U.S.C. 5196(j)(9)); and

9 (III) the amount allocated for purposes under clause
10 (i) does not exceed the greater of \$1,000,000 or 15 per-
11 cent of the grant award.

12 (5) RECREATION.—Grants awarded under this subchapter may not
13 be used for recreational or social purposes.

14 (c) MULTIPLE-PURPOSE FUNDS.—Nothing in this subchapter shall be
15 construed to prohibit State, local, or tribal governments from using grant
16 funds under section 12703, 12704, and 12709 of this title in a manner that
17 enhances preparedness for disasters unrelated to acts of terrorism, if the
18 use assists the governments in achieving target capabilities related to pre-
19 venting, preparing for, protecting against, or responding to acts of ter-
20 rorism.

21 (d) REIMBURSEMENT OF COSTS.—

22 (1) PAID-ON-CALL OR VOLUNTEER REIMBURSEMENT.—In addition to
23 the activities described in subsection (a), a grant under section 12703
24 or 12704 of this title may be used to provide a reasonable stipend to
25 paid-on-call or volunteer emergency response providers who are not oth-
26 erwise compensated for travel to, or participation in, training or exer-
27 cises related to the purposes of this subchapter. Any reimbursement
28 shall not be considered compensation for purposes of rendering an
29 emergency response provider an employee under the Fair Labor Stand-
30 ards Act of 1938 (29 U.S.C. 201 et seq.).

31 (2) PERFORMANCE OF FEDERAL DUTY.—An applicant for a grant
32 under section 12703 or 12704 of this title may petition the Secretary
33 to use the funds from its grants under those sections for the reimburse-
34 ment of the cost of any activity relating to preventing, preparing for,
35 protecting against, or responding to acts of terrorism that is a Federal
36 duty and usually performed by a Federal agency, and that is being per-
37 formed by a State or local government under agreement with a Federal
38 agency.

39 (e) FLEXIBILITY IN UNSPENT HOMELAND SECURITY GRANT FUNDS.—
40 On request by the recipient of a grant under section 12703, 12704, or
41 12709 of this title, the Secretary may authorize the grant recipient to trans-

1 fer all or part of the grant funds from uses specified in the grant agreement
2 to other uses authorized under this section, if the Secretary determines that
3 the transfer is in the interests of homeland security.

4 (f) EQUIPMENT STANDARDS.—If an applicant for a grant under section
5 12703 or 12704 of this title proposes to upgrade or purchase, with assist-
6 ance provided under that grant, new equipment or systems that do not meet
7 or exceed any applicable national voluntary consensus standards developed
8 under section 20507 of this title, the applicant shall include in its applica-
9 tion an explanation of why the equipment or systems will serve the needs
10 of the applicant better than equipment or systems that meet or exceed the
11 standards.

12 **§ 12709. Nonprofit Security Grant Program**

13 (a) ESTABLISHMENT.—There is in the Department the Nonprofit Secu-
14 rity Grant Program (in this section referred to as the “Program”). Under
15 the Program, the Secretary, acting through the Administrator, shall make
16 grants to eligible nonprofit organizations described in subsection (b),
17 through the State in which the organizations are located, for target hard-
18 ening and other security enhancements to protect against terrorist attacks
19 or other threats.

20 (b) ELIGIBLE RECIPIENTS.—Eligible nonprofit organizations described in
21 this subsection are organizations that are—

22 (1) described in section 501(c)(3) of the Internal Revenue Code of
23 1986 (26 U.S.C. 501(c)(3)) and exempt from tax under section 501(a)
24 of the Internal Revenue Code of 1986 (26 U.S.C. 501(a)); and

25 (2) determined by the Secretary to be at risk of terrorist attacks or
26 other threats.

27 (c) PERMITTED USES.—

28 (1) IN GENERAL.—The recipient of a grant under this section may
29 use the grant for any of the following:

30 (A) Target hardening activities, including physical security en-
31 hancement equipment, inspection, and screening systems, and al-
32 teration or remodeling of existing buildings or physical facilities.

33 (B) Fees for security training relating to physical security and
34 cybersecurity, target hardening, terrorism awareness, and em-
35 ployee awareness.

36 (C) Facility security personnel costs.

37 (D) Expenses directly related to the administration of the grant,
38 except that those expenses may not exceed 5 percent of the
39 amount of the grant.

40 (E) Any other appropriate activity, including cybersecurity resil-
41 ience activities, as determined by the Administrator.

1 (2) RETENTION.—Each State through which a recipient receives a
2 grant under this section may retain not more than 5 percent of each
3 grant for expenses directly related to the administration of the grant.

4 (3) OUTREACH AND TECHNICAL ASSISTANCE.—

5 (A) IN GENERAL.—If the Administrator establishes target allo-
6 cations in determining award amounts under the Program, a State
7 may request a project to use a portion of the target allocation for
8 outreach and technical assistance if the State does not receive
9 enough eligible applications from nonprofit organizations located
10 outside high-risk urban areas.

11 (B) PRIORITY.—Any outreach or technical assistance described
12 in subparagraph (A) should prioritize underserved communities
13 and nonprofit organizations that are traditionally underrep-
14 resented in the Program.

15 (C) PARAMETERS.—In determining grant guidelines under sub-
16 section (g), the Administrator may determine the parameters for
17 outreach and technical assistance.

18 (d) AVAILABILITY.—The Administrator shall make funds provided under
19 this section available for use by a recipient of a grant for a period of not
20 less than 36 months.

21 (e) REPORT.—The Administrator shall annually for each of fiscal years
22 2023 through 2028 submit to the Committee on Homeland Security of the
23 House of Representatives and the Committee on Homeland Security and
24 Governmental Affairs of the Senate a report containing information on the
25 following:

26 (1) The expenditure by each grant recipient of grant funds made
27 available under this section.

28 (2) The number of applications submitted by eligible nonprofit orga-
29 nizations to each State.

30 (3) The number of applications submitted by each State to the Ad-
31 ministrator.

32 (4) The operations of the program office of the Program, including
33 staffing resources and efforts with respect to subparagraphs (A)
34 through (D) of subsection (c)(1).

35 (f) ADMINISTRATION .—Not later than 120 days after December 23,
36 2022, the Administrator shall ensure that in the Federal Emergency Man-
37 agement Agency a program office for the program (in this subsection re-
38 ferred to as the “program office”) shall—

39 (1) be headed by a senior official of the Federal Emergency Manage-
40 ment Agency; and

1 (2) administer the Program (including, where appropriate, in coordi-
2 nation with States) including relating to—

3 (A) outreach, engagement, education, and technical assistance
4 and support to eligible nonprofit organizations described in sub-
5 section (b), with particular attention to those organizations in un-
6 derserved communities before, during, and after the awarding of
7 grants, including web-based training videos for eligible nonprofit
8 organizations that prepare guidance on preparing an application
9 and the environmental planning and historic preservation process;

10 (B) the establishment of mechanisms to ensure program office
11 processes are conducted in accordance with constitutional, statu-
12 tory, and regulatory requirements that protect civil rights and civil
13 liberties and advance equal access for members of underserved
14 communities;

15 (C) the establishment of mechanisms for the Administrator to
16 provide feedback to eligible nonprofit organizations that do not re-
17 ceive grants;

18 (D) the establishment of mechanisms to identify and collect data
19 to measure the effectiveness of grants under the Program;

20 (E) the establishment and enforcement of standardized baseline
21 operational requirements for States, including requirements for
22 States to eliminate or prevent any administrative or operational
23 obstacles that may impact eligible nonprofit organizations de-
24 scribed in subsection (b) from receiving grants under the Program;

25 (F) carrying out efforts to prevent waste, fraud, and abuse, in-
26 cluding through audits of grantees; and

27 (G) promoting diversity in the types and locations of eligible
28 nonprofit organizations that are applying for grants under the
29 Program.

30 (g) GRANT GUIDELINES.—For each fiscal year, before awarding grants
31 under this section, the Administrator—

32 (1) shall publish guidelines, including a notice of funding opportunity
33 or similar announcement, as the Administrator determines appropriate;
34 and

35 (2) may prohibit States from closing application processes before the
36 publication of those guidelines.

37 (h) NONAPPLICATION OF CHAPTER 35 OF TITLE 44.—Chapter 35 of title
38 44 shall not apply to any changes to the application materials, Program
39 forms, or other core Program documentation intended to enhance participa-
40 tion by eligible nonprofit organizations in the Program.

41 (i) AUTHORIZATION OF APPROPRIATIONS.—

1 (1) IN GENERAL.—There is authorized to be appropriated
2 \$360,000,000 for each of fiscal years 2023 through 2028 under this
3 section, of which—

4 (A) \$180,000,000 each fiscal year shall be for recipients in
5 high-risk urban areas that receive funding under section 12703 of
6 this title; and

7 (B) \$180,000,000 each fiscal year shall be for recipients in ju-
8 risdictions that do not receive funding under section 12703 of this
9 title.

10 (2) OPERATION AND SUPPORT.—There is authorized to be appro-
11 priated \$18,000,000 for each of fiscal years 2023 through 2028 for
12 Operations and Support at the Federal Emergency Management Agen-
13 cy for costs incurred for the management and administration (including
14 evaluation) of this section.

15 **Part B—Administration**

16 **§ 12721. Administration and coordination**

17 (a) REGIONAL COORDINATION.—The Administrator shall ensure that—

18 (1) all recipients of grants administered by the Department to pre-
19 vent, prepare for, protect against, or respond to natural disasters, acts
20 of terrorism, or other man-made disasters (excluding assistance pro-
21 vided under section 203 or title IV or V of the Robert T. Stafford Dis-
22 aster Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et
23 seq., 5191 et seq.)) coordinate, as appropriate, their prevention, pre-
24 paredness, and protection efforts with neighboring State, local, and
25 tribal governments; and

26 (2) all high-risk urban areas and other recipients of grants adminis-
27 tered by the Department to prevent, prepare for, protect against, or
28 respond to natural disasters, acts of terrorism, or other man-made dis-
29 asters (excluding assistance provided under section 203 or title IV or
30 V of the Robert T. Stafford Disaster Relief and Emergency Assistance
31 Act (42 U.S.C. 5133, 5170 et seq., 5191 et seq.)) that include or sub-
32 stantially affect parts or all of more than one State coordinate, as ap-
33 propriate, across State boundaries, including, where appropriate,
34 through the use of regional working groups and requirements for re-
35 gional plans.

36 (b) PLANNING COMMITTEES.—

37 (1) IN GENERAL.—Any State or high-risk urban area receiving a
38 grant under section 12703 or 12704 of this title shall establish a State
39 planning committee or urban area working group to assist in prepara-
40 tion and revision of the State, regional, or local homeland security plan
41 or the threat and hazard identification and risk assessment and to as-

1 sist in determining effective funding priorities for grants under sections
2 12703 and 12704 of this title.

3 (2) COMPOSITION.—

4 (A) IN GENERAL.—The State planning committees and urban
5 area working groups shall include at least 1 representative from
6 each of the following significant stakeholders:

7 (i) Local or tribal government officials.

8 (ii) Emergency response providers, which shall include rep-
9 resentatives of fire service, law enforcement, emergency med-
10 ical services, and emergency managers.

11 (iii) Public health officials and other appropriate medical
12 practitioners.

13 (iv) Individuals representing educational institutions, in-
14 cluding elementary schools, community colleges, and other in-
15 stitutions of higher learning.

16 (v) State and regional interoperable communications coor-
17 dinators, as appropriate.

18 (vi) State and major urban area fusion centers, as appro-
19 priate.

20 (B) GEOGRAPHIC REPRESENTATION.—The members of the
21 State planning committee or urban area working group shall be
22 a representative group of individuals from the counties, cities,
23 towns, and Indian tribes in the State or high-risk urban area, in-
24 cluding, as appropriate, representatives of rural, high-population,
25 and high-threat jurisdictions.

26 (3) EXISTING PLANNING COMMITTEES.—Nothing in this subsection
27 may be construed to require that any State or high-risk urban area cre-
28 ate a State planning committee or urban area working group if that
29 State or high-risk urban area has established and uses a multijuris-
30 dictional planning committee or commission that meets the require-
31 ments of this subsection.

32 **§ 12722. Accountability**

33 (a) AUDITS OF GRANT PROGRAMS.—

34 (1) COMPLIANCE REQUIREMENTS.—

35 (A) AUDIT REQUIREMENT.—Each recipient of a grant adminis-
36 tered by the Department that expends not less than \$500,000 in
37 Federal funds during its fiscal year shall submit to the Secretary,
38 through the Administrator, a copy of the organization-wide finan-
39 cial and compliance audit report required under chapter 75 of title
40 31.

1 (B) ACCESS TO INFORMATION.—The Department and each re-
2 cipient of a grant administered by the Department shall provide
3 the Comptroller General and any officer or employee of the Gov-
4 ernment Accountability Office with full access to information re-
5 garding the activities carried out that are related to any grant ad-
6 ministered by the Department.

7 (C) IMPROPER PAYMENTS.—Consistent with subchapter IV of
8 chapter 33 of title 31, for each of the grant programs under sec-
9 tions 12703, 12704, and 20522 of this title, the Secretary shall
10 specify policies and procedures for—

11 (i) identifying activities funded under a grant program that
12 are susceptible to significant improper payments; and

13 (ii) reporting any improper payments to the Department.

14 (2) AGENCY PROGRAM REVIEW.—

15 (A) IN GENERAL.—The Secretary shall biennially conduct, for
16 each State and high-risk urban area receiving a grant adminis-
17 tered by the Department, a programmatic and financial review of
18 all grants awarded by the Department to prevent, prepare for,
19 protect against, or respond to natural disasters, acts of terrorism,
20 or other man-made disasters, excluding assistance provided under
21 section 203, title IV, or title V of the Robert T. Stafford Disaster
22 Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et
23 seq., 5191 et seq.).

24 (B) CONTENTS.—Each review under subparagraph (A) shall, at
25 a minimum, examine—

26 (i) whether the funds awarded were used in accordance
27 with the law, program guidance, and State homeland security
28 plans or other applicable plans; and

29 (ii) the extent to which funds awarded enhanced the ability
30 of a grantee to prevent, prepare for, protect against, and re-
31 spond to natural disasters, acts of terrorism, and other man-
32 made disasters.

33 (C) AUTHORIZATION OF APPROPRIATIONS.—In addition to any
34 other amounts authorized to be appropriated to the Secretary,
35 there are authorized to be appropriated to the Secretary for re-
36 views under this paragraph such sums as may be necessary.

37 (3) PERFORMANCE ASSESSMENT.—In order to ensure that States
38 and high-risk urban areas are using grants administered by the De-
39 partment appropriately to meet target capabilities and preparedness
40 priorities, the Secretary shall—

1 (A) ensure that each State or high-risk urban area conducts or
2 participates in exercises under section 20508(b) of this title;

3 (B) use performance metrics in accordance with the comprehen-
4 sive assessment system under section 20509 of this title and en-
5 sure that each State or high-risk urban area regularly tests its
6 progress against the metrics through the exercises required under
7 subparagraph (A);

8 (C) use the remedial action management program under section
9 20510 of this title; and

10 (D) ensure that each State receiving a grant administered by
11 the Department submits a report to the Administrator on its level
12 of preparedness, as required by section 20512(c) of this title.

13 (4) CONSIDERATION OF ASSESSMENTS.—In conducting program re-
14 views and performance audits under paragraph (2), the Secretary and
15 the Inspector General of the Department shall take into account the
16 performance assessment elements required under paragraph (3).

17 (5) RECOVERY AUDITS.—The Secretary shall conduct a recovery
18 audit under section 3352(i) of title 31 for a grant administered by the
19 Department with a total value of not less than \$1,000,000, if the Sec-
20 retary finds that—

21 (A) a financial audit has identified improper payments that can
22 be recouped; and

23 (B) it is cost-effective to conduct a recovery audit to recapture
24 the targeted funds.

25 (6) REMEDIES FOR NONCOMPLIANCE.—

26 (A) IN GENERAL.—If, as a result of a review or audit under this
27 subsection or otherwise, the Secretary finds that a recipient of a
28 grant under this subchapter has failed to substantially comply
29 with any provision of law or with any regulations or guidelines of
30 the Department regarding eligible expenditures, the Secretary
31 shall—

32 (i) reduce the amount of payment of grant funds to the re-
33 cipient by an amount equal to the amount of grants funds
34 that were not properly expended by the recipient;

35 (ii) limit the use of grant funds to programs, projects, or
36 activities not affected by the failure to comply;

37 (iii) refer the matter to the Inspector General of the De-
38 partment for further investigation;

39 (iv) terminate any payment of grant funds to be made to
40 the recipient; or

1 (v) take other actions the Secretary determines appro-
2 priate.

3 (B) DURATION OF PENALTY.—The Secretary shall apply an ap-
4 propriate penalty under subparagraph (A) until the Secretary de-
5 termines that the grant recipient is in full compliance with the law
6 and with applicable guidelines or regulations of the Department.

7 (b) REPORTS BY GRANT RECIPIENTS.—

8 (1) QUARTERLY REPORTS ON HOMELAND SECURITY SPENDING.—

9 (A) IN GENERAL.—As a condition of receiving a grant under
10 section 12703 or 12704 of this title, a State, high-risk urban area,
11 or directly eligible tribe shall, not later than 30 days after the end
12 of each Federal fiscal quarter, submit to the Secretary a report
13 on activities performed using grant funds during that fiscal quar-
14 ter.

15 (B) CONTENTS.—Each report submitted under subparagraph
16 (A) shall at a minimum include, for the applicable State, high-risk
17 urban area, or directly eligible tribe, and each subgrantee there-
18 of—

19 (i) the amount obligated to that recipient under section
20 12703 or 12704 of this title in that quarter;

21 (ii) the amount of funds received and expended under sec-
22 tion 12703 or 12704 of this title by that recipient in that
23 quarter; and

24 (iii) a summary description of expenditures made by that
25 recipient using the funds, and the purposes for which the ex-
26 penditures were made.

27 (C) END-OF-YEAR REPORT.—The report submitted under sub-
28 paragraph (A) by a State, high-risk urban area, or directly eligible
29 tribe relating to the last quarter of any fiscal year shall include—

30 (i) the amount and date of receipt of all funds received
31 under the grant during that fiscal year;

32 (ii) the identity of, and amount provided to, any subgrantee
33 for that grant during that fiscal year;

34 (iii) the amount and the dates of disbursements of funds
35 expended in compliance with section 12721(a)(1) of this title
36 or under mutual aid agreements or other sharing arrange-
37 ments that apply within the State, high-risk urban area, or
38 directly eligible tribe, as applicable, during that fiscal year;
39 and

40 (iv) an explanation of how the funds were used by each re-
41 cipient or subgrantee during that fiscal year.

1 (2) ANNUAL STATE PREPAREDNESS REPORT.—Any State applying
2 for a grant under section 12704 of this title shall submit to the Admin-
3 istrator annually a State preparedness report, as required by section
4 20512(c) of this title.

5 (3) ANNUAL REPORT ON EXPENDITURES.—

6 (A) DEFINITION OF HOMELAND SECURITY GRANT.—In this
7 paragraph, the term “homeland security grant” means any grant
8 made or administered by the Department, including—

- 9 (i) the State Homeland Security Grant Program;
10 (ii) the Urban Area Security Initiative Grant Program;
11 (iii) the Law Enforcement Terrorism Prevention Program;
12 (iv) the Citizen Corps; and
13 (v) the Metropolitan Medical Response System.

14 (B) LIST OF EXPENDITURES.—Not later than 12 months after
15 the date of receipt of the grant, and every 12 months thereafter
16 until all funds provided under the grant are expended, each State
17 or local government that receives a homeland security grant shall
18 submit a report to the Secretary that contains a list of all expendi-
19 tures made by the State or local government using funds from the
20 grant.

21 (c) REPORTS BY THE ADMINISTRATOR.—

22 (1) FEDERAL PREPAREDNESS REPORT.—The Administrator shall
23 submit to the appropriate committees of Congress annually the Federal
24 Preparedness Report required under section 20512(a) of this title.

25 (2) RISK ASSESSMENT.—

26 (A) IN GENERAL.—For each fiscal year, the Administrator shall
27 provide to the appropriate committees of Congress a detailed and
28 comprehensive explanation of the methodologies used to calculate
29 risk and compute the allocation of funds for grants administered
30 by the Department, including—

- 31 (i) all variables included in the risk assessment and the
32 weights assigned to each variable;
33 (ii) an explanation of how each variable, as weighted, cor-
34 relates to risk, and the basis for concluding there is a correla-
35 tion; and
36 (iii) any change in the methodologies from the previous fis-
37 cal year, including changes in variables considered, the
38 weighting of those variables, and computational methods.

39 (B) CLASSIFIED ANNEX.—The information required under sub-
40 paragraph (A) shall be provided in unclassified form to the extent
41 possible, and may include a classified annex if necessary.

1 (C) DEADLINE.—For each fiscal year, the information required
2 under subparagraph (A) shall be provided on the earlier of—

3 (i) October 31; or

4 (ii) 30 days before the issuance of any program guidance
5 for grants administered by the Department.

6 (3) TRIBAL FUNDING REPORT.—At the end of each fiscal year, the
7 Administrator shall submit to the appropriate committees of Congress
8 a report setting forth the amount of funding provided during that fiscal
9 year to Indian tribes under any grant program administered by the De-
10 partment, whether provided directly or through a subgrant from a
11 State or high-risk urban area.

12 **§ 12723. Identification of reporting redundancies and devel-**
13 **opment of performance metrics**

14 (a) DEFINITION OF COVERED GRANTS.—In this section, the term “cov-
15 ered grants” means grants awarded under section 12703 of this title, grants
16 awarded under section 12704 of this title, and any other grants specified
17 by the Administrator.

18 (b) PLAN TO ELIMINATE REDUNDANT AND UNNECESSARY REPORTING
19 REQUIREMENTS AND TO ASSESS EFFECTIVENESS OF PROGRAMS.—The Ad-
20 ministrator shall develop—

21 (1) a plan, including a specific timetable, for eliminating any redun-
22 dant and unnecessary reporting requirements imposed by the Adminis-
23 trator on State, local and tribal governments in connection with the
24 awarding of grants; and

25 (2) a plan, including a specific timetable, for promptly developing a
26 set of quantifiable performance measures and metrics to assess the ef-
27 fectiveness of the programs under which covered grants are awarded.

28 (c) BIENNIAL REPORTS.—Not later than January 10, 2018, and every
29 2 years thereafter, the Secretary shall submit to the appropriate committees
30 of Congress a grants management report that includes—

31 (1) the status of efforts to eliminate redundant and unnecessary re-
32 porting requirements imposed on grant recipients, including—

33 (A) progress made in implementing the plan required under
34 subsection (b)(1);

35 (B) a reassessment of the reporting requirements to identify
36 and eliminate redundant and unnecessary requirements;

37 (2) the status of efforts to develop quantifiable performance meas-
38 ures and metrics to assess the effectiveness of the programs under
39 which the covered grants are awarded, including—

40 (A) progress made in implementing the plan required under
41 subsection (b)(2); and

1 (B) progress made in developing and implementing additional
2 performance metrics and measures for grants, including as part of
3 the comprehensive assessment system required under section
4 20509 of this title; and

5 (3) a performance assessment of each program under which the cov-
6 ered grants are awarded, including—

7 (A) a description of the objectives and goals of the program;

8 (B) an assessment of the extent to which the objectives and
9 goals described in subparagraph (A) have been met, based on the
10 quantifiable performance measures and metrics required under
11 this section and sections 12722(a)(3) and 20509 of this title;

12 (C) recommendations for any program modifications to improve
13 the effectiveness of the program, to address changed or emerging
14 conditions; and

15 (D) an assessment of the experience of recipients of covered
16 grants, including the availability of clear and accurate information,
17 the timeliness of reviews and awards, and the provision of tech-
18 nical assistance, and recommendations for improving that experi-
19 ence.

20 (d) GRANTS PROGRAM MEASUREMENT STUDY.—The National Academy
21 of Public Administration shall assist the Administrator in implementing—

22 (1) quantifiable performance measures and metrics to assess the ef-
23 fectiveness of grants administered by the Department, as required
24 under this section and section 20509 of this title; and

25 (2) the plan required under subsection (b)(2).

26 **Subchapter II—Grants To Address Cyber-**
27 **security Risks and Cybersecurity**
28 **Threats to Information Systems**

29 **§ 12731. Definitions**

30 In this subchapter:

31 (1) CYBERSECURITY PLAN.—The term “Cybersecurity Plan” means
32 a plan submitted by an eligible entity under section 12735(a) of this
33 title.

34 (2) DIRECTOR.—The term “Director” means the Director of the Cy-
35 bersecurity and Infrastructure Security Agency.

36 (3) ELIGIBLE ENTITY.—The term “eligible entity” means a—

37 (A) State; or

38 (B) Tribal government.

39 (4) MULTI-ENTITY GROUP.—The term “multi-entity group” means a
40 group of 2 or more eligible entities desiring a grant under this sub-
41 chapter.

1 (5) ONLINE SERVICE.—The term “online service” means an internet-
2 facing service, including a website, email, virtual private network, or
3 custom application.

4 (6) RURAL AREA.—The term “rural area” has the meaning given the
5 term in section 5302 of title 49.

6 (7) STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.—The
7 term “State and Local Cybersecurity Grant Program” means the pro-
8 gram established under section 12732 of this title.

9 (8) TRIBAL GOVERNMENT.—The term “Tribal government” means
10 the recognized governing body of an Indian or Alaska Native Tribe,
11 band, nation, pueblo, village, community, component band, or compo-
12 nent reservation, that is individually identified (including parentheti-
13 cally) in the most recent list published pursuant to Section 104 of the
14 Federally Recognized Indian Tribe List Act of 1994 (25 U.S.C. 5131).

15 **§ 12732. Program**

16 (a) ESTABLISHMENT.—There is in the Department a program to award
17 grants to eligible entities to address cybersecurity risks and cybersecurity
18 threats to information systems owned or operated by, or on behalf of, State,
19 local, or Tribal governments.

20 (b) APPLICATION.—An eligible entity desiring a grant under the State
21 and Local Cybersecurity Grant Program shall submit to the Secretary an
22 application at such time, in such manner, and containing such information
23 as the Secretary may require.

24 **§ 12733. Administration**

25 The State and Local Cybersecurity Grant Program shall be administered
26 in the same office of the Department that administers grants made under
27 sections 12702 and 12703 of this title.

28 **§ 12734. Use of funds**

29 An eligible entity that receives a grant under this subchapter and a local
30 government that receives funds from a grant under this subchapter, as ap-
31 propriate, shall use the grant to—

32 (1) implement the Cybersecurity Plan of the eligible entity;

33 (2) develop or revise the Cybersecurity Plan of the eligible entity;

34 (3) pay expenses directly relating to the administration of the grant,
35 which shall not exceed 5 percent of the amount of the grant;

36 (4) assist with activities that address imminent cybersecurity threats,
37 as confirmed by the Secretary, acting through the Director, to the in-
38 formation systems owned or operated by, or on behalf of, the eligible
39 entity or a local government within the jurisdiction of the eligible enti-
40 ty; or

1 (5) fund any other appropriate activity determined by the Secretary,
2 acting through the Director.

3 **§ 12735. Cybersecurity plans**

4 (a) SUBMISSION OF PLAN TO SECRETARY.—An eligible entity applying
5 for a grant under this subchapter shall submit to the Secretary a Cyberse-
6 curity Plan for review in accordance with section 12739 of this title.

7 (b) REQUIRED ELEMENTS.—A Cybersecurity Plan of an eligible entity
8 shall—

9 (1) incorporate, to the extent practicable—

10 (A) any existing plans of the eligible entity to protect against
11 cybersecurity risks and cybersecurity threats to information sys-
12 tems owned or operated by, or on behalf of, State, local, or Tribal
13 governments; and

14 (B) if the eligible entity is a State, consultation and feedback
15 from local governments and associations of local governments
16 within the jurisdiction of the eligible entity;

17 (2) describe, to the extent practicable, how the eligible entity will—

18 (A) manage, monitor, and track information systems, applica-
19 tions, and user accounts owned or operated by, or on behalf of,
20 the eligible entity or, if the eligible entity is a State, local govern-
21 ments within the jurisdiction of the eligible entity, and the infor-
22 mation technology deployed on those information systems, includ-
23 ing legacy information systems and information technology that
24 are no longer supported by the manufacturer of the systems or
25 technology;

26 (B) monitor, audit, and, track network traffic and activity
27 transiting or traveling to or from information systems, applica-
28 tions, and user accounts owned or operated by, or on behalf of,
29 the eligible entity or, if the eligible entity is a State, local govern-
30 ments within the jurisdiction of the eligible entity;

31 (C) enhance the preparation, response, and resiliency of infor-
32 mation systems, applications, and user accounts owned or operated
33 by, or on behalf of, the eligible entity or, if the eligible entity is
34 a State, local governments within the jurisdiction of the eligible
35 entity, against cybersecurity risks and cybersecurity threats;

36 (D) implement a process of continuous cybersecurity vulner-
37 ability assessments and threat mitigation practices prioritized by
38 degree of risk to address cybersecurity risks and cybersecurity
39 threats on information systems, applications, and user accounts
40 owned or operated by, or on behalf of, the eligible entity or, if the

1 eligible entity is a State, local governments within the jurisdiction
2 of the eligible entity;

3 (E) ensure that the eligible entity and, if the eligible entity is
4 a State, local governments within the jurisdiction of the eligible
5 entity, adopt and use best practices and methodologies to enhance
6 cybersecurity, such as—

7 (i) the practices set forth in the cybersecurity framework
8 developed by the National Institute of Standards and Tech-
9 nology;

10 (ii) cybersecurity supply chain risk management best prac-
11 tices identified by the National Institute of Standards and
12 Technology; and

13 (iii) knowledge bases of adversary tools and tactics;

14 (F) promote the delivery of safe, recognizable, and trustworthy
15 online services by the eligible entity and, if the eligible entity is
16 a State, local governments within the jurisdiction of the eligible
17 entity, including through the use of the .gov internet domain;

18 (G) ensure continuity of operations of the eligible entity and, if
19 the eligible entity is a State, local governments within the jurisdic-
20 tion of the eligible entity, in the event of a cybersecurity incident,
21 including by conducting exercises to practice responding to a cy-
22 bersecurity incident;

23 (H) use the National Initiative for Cybersecurity Education
24 Workforce Framework for Cybersecurity developed by the National
25 Institute of Standards and Technology to identify and mitigate
26 any gaps in the cybersecurity workforces of the eligible entity and,
27 if the eligible entity is a State, local governments within the jurisdic-
28 tion of the eligible entity, enhance recruitment and retention ef-
29 forts for those workforces, and bolster the knowledge, skills, and
30 abilities of personnel of the eligible entity and, if the eligible entity
31 is a State, local governments within the jurisdiction of the eligible
32 entity, to address cybersecurity risks and cybersecurity threats,
33 such as through cybersecurity hygiene training;

34 (I) if the eligible entity is a State, ensure continuity of commu-
35 nications and data networks within the jurisdiction of the eligible
36 entity between the eligible entity and local governments within the
37 jurisdiction of the eligible entity in the event of an incident involv-
38 ing those communications or data networks;

39 (J) assess and mitigate, to the greatest degree possible, cyberse-
40 curity risks and cybersecurity threats relating to critical infra-
41 structure and key resources, the degradation of which may impact

1 the performance of information systems within the jurisdiction of
2 the eligible entity;

3 (K) enhance capabilities to share cyber threat indicators and re-
4 lated information between the eligible entity and—

5 (i) if the eligible entity is a State, local governments within
6 the jurisdiction of the eligible entity, including by expanding
7 information sharing agreements with the Department; and

8 (ii) the Department;

9 (L) leverage cybersecurity services offered by the Department;

10 (M) implement an information technology and operational tech-
11 nology modernization cybersecurity review process that ensures
12 alignment between information technology and operational tech-
13 nology cybersecurity objectives;

14 (N) develop and coordinate strategies to address cybersecurity
15 risks and cybersecurity threats in consultation with—

16 (i) if the eligible entity is a State, local governments and
17 associations of local governments within the jurisdiction of
18 the eligible entity; and

19 (ii) as applicable—

20 (I) eligible entities that neighbor the jurisdiction of the
21 eligible entity or, as appropriate, members of an Infor-
22 mation Sharing and Analysis Organization; and

23 (II) countries that neighbor the jurisdiction of the eli-
24 gible entity;

25 (O) ensure adequate access to, and participation in, the services
26 and programs described in this paragraph by rural areas within
27 the jurisdiction of the eligible entity; and

28 (P) distribute funds, items, services, capabilities, or activities to
29 local governments under 12744(b)(1) of this title, including the
30 fraction of that distribution the eligible entity plans to distribute
31 to rural areas under subsection 12744(b)(2) of this title;

32 (3) assess the capabilities of the eligible entity relating to the actions
33 described in paragraph (2);

34 (4) describe, as appropriate and to the extent practicable, the indi-
35 vidual responsibilities of the eligible entity and local governments with-
36 in the jurisdiction of the eligible entity in implementing the plan;

37 (5) outline, to the extent practicable, the necessary resources and a
38 timeline for implementing the plan; and

39 (6) describe the metrics the eligible entity will use to measure
40 progress towards—

41 (A) implementing the plan; and

1 (B) reducing cybersecurity risks to, and identifying, responding
2 to, and recovering from cybersecurity threats to, information sys-
3 tems owned or operated by, or on behalf of, the eligible entity or,
4 if the eligible entity is a State, local governments within the juris-
5 diction of the eligible entity.

6 (c) DISCRETIONARY ELEMENTS.—In drafting a Cybersecurity Plan, an
7 eligible entity may—

8 (1) consult with the Multi-State Information Sharing and Analysis
9 Center;

10 (2) include a description of cooperative programs developed by
11 groups of local governments within the jurisdiction of the eligible entity
12 to address cybersecurity risks and cybersecurity threats; and

13 (3) include a description of programs provided by the eligible entity
14 to support local governments and owners and operators of critical in-
15 frastructure to address cybersecurity risks and cybersecurity threats.

16 **§ 12736. Multi-entity grants**

17 (a) IN GENERAL.—The Secretary may award grants under this section
18 to a multi-entity group to support multi-entity efforts to address cybersecu-
19 rity risks and cybersecurity threats to information systems within the juris-
20 dictions of the eligible entities that comprise the multi-entity group.

21 (b) REQUIREMENTS.—To be eligible for a multi-entity grant under this
22 section, each eligible entity that comprises a multi-entity group shall have—

23 (1) a Cybersecurity Plan that has been reviewed by the Secretary in
24 accordance with section 12739 of this title; and

25 (2) a cybersecurity planning committee established in accordance
26 with section 12737 of this title.

27 (c) APPLICATION.—

28 (1) IN GENERAL.—A multi-entity group applying for a multi-entity
29 grant under subsection (a) shall submit to the Secretary an application
30 at such time, in such manner, and containing such information as the
31 Secretary may require.

32 (2) MULTI-ENTITY PROJECT PLAN.—An application for a grant
33 under this subchapter of a multi-entity group under paragraph (1)
34 shall include a plan describing—

35 (A) the division of responsibilities among the eligible entities
36 that comprise the multi-entity group;

37 (B) the distribution of funding from the grant among the eligi-
38 ble entities that comprise the multi-entity group; and

39 (C) how the eligible entities that comprise the multi-entity
40 group will work together to implement the Cybersecurity Plan of
41 each of those eligible entities.

1 **§ 12737. Planning committees**

2 (a) IN GENERAL.—An eligible entity that receives a grant under this sub-
3 chapter shall establish a cybersecurity planning committee to—

4 (1) assist with the development, implementation, and revision of the
5 Cybersecurity Plan of the eligible entity;

6 (2) approve the Cybersecurity Plan of the eligible entity; and

7 (3) assist with the determination of effective funding priorities for
8 a grant under this section in accordance with sections 12734 and
9 12740 of this title.

10 (b) COMPOSITION.—A committee of an eligible entity established under
11 subsection (a) shall—

12 (1) be comprised of representatives from—

13 (A) the eligible entity;

14 (B) if the eligible entity is a State, counties, cities, and towns
15 within the jurisdiction of the eligible entity; and

16 (C) institutions of public education and health within the juris-
17 diction of the eligible entity; and

18 (2) include, as appropriate, representatives of rural, suburban, and
19 high-population jurisdictions.

20 (c) CYBERSECURITY EXPERTISE.—Not less than 1/2 of the representa-
21 tives of a committee established under subsection (a) shall have professional
22 experience relating to cybersecurity or information technology.

23 (d) RULE OF CONSTRUCTION REGARDING EXISTING PLANNING COMMIT-
24 TEES.—Nothing in this section shall be construed to require an eligible enti-
25 ty to establish a cybersecurity planning committee if the eligible entity has
26 established and uses a multijurisdictional planning committee or commission
27 that—

28 (1) meets the requirements of this section; and

29 (2) may be expanded or leveraged to meet the requirements of this
30 section, including through the formation of a cybersecurity planning
31 subcommittee.

32 (e) RULE OF CONSTRUCTION REGARDING CONTROL OF INFORMATION
33 SYSTEMS IF ELIGIBLE ENTITIES.—Nothing in this section shall be con-
34 strued to permit a cybersecurity planning committee of an eligible entity
35 that meets the requirements of this section to make decisions relating to
36 information systems owned or operated by, or on behalf of, the eligible enti-
37 ty.

38 **§ 12738. Special rule for Tribal governments**

39 With respect to any requirement under section 12735 or 12737 of this
40 title, the Secretary, in consultation with the Secretary of the Interior and
41 Tribal governments, may prescribe an alternative substantively similar re-

1 requirement for Tribal governments if the Secretary finds that the alternative
2 requirement is necessary for the effective delivery and administration of
3 grants to Tribal governments under this subchapter.

4 **§ 12739. Review of plans**

5 (a) REVIEW AS CONDITION OF GRANT.—

6 (1) IN GENERAL.—Subject to subsection (c), before an eligible entity
7 may receive a grant under this subchapter, the Secretary, acting
8 through the Director, shall—

9 (A) review the Cybersecurity Plan of the eligible entity, includ-
10 ing any revised Cybersecurity Plans of the eligible entity; and

11 (B) determine that the Cybersecurity Plan reviewed under sub-
12 paragraph (A) satisfies the requirements under subsection (b).

13 (2) DURATION OF DETERMINATION.—In the case of a determination
14 under paragraph (1)(B) that a Cybersecurity Plan satisfies the require-
15 ments under subsection (b), the determination shall be effective for the
16 2-year period beginning on the date of the determination.

17 (3) ANNUAL RENEWAL.—Not later than 2 years after the date on
18 which the Secretary determines under paragraph (1)(B) that a Cyber-
19 security Plan satisfies the requirements under subsection (b), and an-
20 nually thereafter, the Secretary, acting through the Director, shall—

21 (A) determine whether the Cybersecurity Plan and any revisions
22 continue to meet the criteria described in subsection (b); and

23 (B) renew the determination if the Secretary, acting through
24 the Director, makes a positive determination under subparagraph
25 (A).

26 (b) PLAN REQUIREMENTS.—In reviewing a Cybersecurity Plan of an eli-
27 gible entity under this section, the Secretary, acting through the Director,
28 shall ensure that the Cybersecurity Plan—

29 (1) satisfies the requirements of section 12735(b) of this title; and

30 (2) has been approved by—

31 (A) the cybersecurity planning committee of the eligible entity
32 established under section 12737 of this title; and

33 (B) the Chief Information Officer, the Chief Information Secu-
34 rity Officer, or an equivalent official of the eligible entity.

35 (c) EXCEPTION.—Notwithstanding subsection (a) and section 12735 of
36 this title, the Secretary may award a grant under this section to an eligible
37 entity that does not submit a Cybersecurity Plan to the Secretary for review
38 before September 30, 2023, if the eligible entity certifies to the Secretary
39 that—

40 (1) the activities that will be supported by the grant are—

1 (A) integral to the development of the Cybersecurity Plan of the
2 eligible entity; or

3 (B) necessary to assist with activities described in section
4 12734(4) of this title, as confirmed by the Director; and

5 (2) the eligible entity will submit to the Secretary a Cybersecurity
6 Plan for review under this section by September 30, 2023.

7 (d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed
8 to provide authority to the Secretary to—

9 (1) regulate the manner by which an eligible entity or local govern-
10 ment improves the cybersecurity of the information systems owned or
11 operated by, or on behalf of, the eligible entity or local government; or

12 (2) condition the receipt of grants under this subchapter on—

13 (A) participation in a particular Federal program; or

14 (B) the use of a specific product or technology.

15 **§ 12740. Limitation of use of funds**

16 (a) IN GENERAL.—An entity that receives funds from a grant under this
17 subchapter may not use the grant—

18 (1) to supplant State or local funds;

19 (2) for a recipient cost-sharing contribution;

20 (3) to pay a ransom;

21 (4) for recreational or social purposes; or

22 (5) for a purpose that does not address cybersecurity risks or cyber-
23 security threats on information systems owned or operated by, or on
24 behalf of, the eligible entity that receives the grant or a local govern-
25 ment within the jurisdiction of the eligible entity.

26 (b) COMPLIANCE OVERSIGHT.—In addition to any other remedy available,
27 the Secretary may take such actions as are necessary to ensure that a re-
28 cipient of a grant under this subchapter uses the grant for the purposes
29 for which the grant is awarded.

30 (c) RULE OF CONSTRUCTION.—Nothing in subsection (a)(1) shall be con-
31 strued to prohibit the use of funds from a grant under this subchapter
32 awarded to a State, local, or Tribal government for otherwise permissible
33 uses under this subchapter on the basis that the State, local, or Tribal gov-
34 ernment has previously used State, local, or Tribal funds to support the
35 same or similar uses.

36 **§ 12741. Opportunity to amend applications**

37 In considering applications for grants under this subchapter, the Sec-
38 retary shall provide applicants with a reasonable opportunity to correct any
39 defects in those applications before making final awards, including by allow-
40 ing applicants to revise a submitted Cybersecurity Plan.

1 **§ 12742. Apportionment**

2 For each fiscal year, the Secretary shall apportion amounts appropriated
3 to carry out this subchapter among eligible entities as follows:

- 4 (1) **BASELINE AMOUNT.**—The Secretary shall first apportion—
5 (A) 0.25 percent of the amounts to each of Guam, American
6 Samoa, the Virgin Islands, and the Northern Mariana Islands;
7 (B) 1 percent of the amounts to each of the remaining States;
8 and
9 (C) 3 percent of the amounts to Tribal Governments.

10 (2) **REMAINDER.**—The Secretary shall apportion the remainder of
11 the amounts to States as follows:

- 12 (A) 50 percent of the remainder in the ratio that the population
13 of each State bears to the population of all States; and
14 (B) 50 percent of the remainder in the ratio that the population
15 of each State that resides in rural areas bears to the population
16 of all States that resides in rural areas.

17 (3) **AMONG TRIBAL GOVERNMENTS.**—In determining how to appor-
18 tion amounts to Tribal governments under paragraph (1)(C), the Sec-
19 retary shall consult with the Secretary of the Interior and Tribal govern-
20 ments.

21 (4) **MULTI-ENTITY GRANTS.**—An amount received from a multi-enti-
22 ty grant awarded under section 12736(a) of this title by a State or
23 Tribal government that is a member of a multi-entity group shall qual-
24 ify as an apportionment for the purposes of this section.

25 **§ 12743. Federal share**

26 (a) **IN GENERAL.**—The Federal share of the cost of an activity carried
27 out using funds made available with a grant under this subchapter may not
28 exceed—

- 29 (1) in the case of a grant to a Federal entity—
30 (A) for fiscal year 2023, 80 percent;
31 (B) for fiscal year 2024, 70 percent; and
32 (C) for fiscal year 2025, 60 percent; and
33 (2) in the case of a grant to a multi-entity group—
34 (A) for fiscal year 2023, 90 percent;
35 (B) for fiscal year 2024, 80 percent; and
36 (C) for fiscal year 2025, 70 percent.

37 (b) **WAIVER.**—

38 (1) **IN GENERAL.**—The Secretary may waive or modify the require-
39 ments of subsection (a) if an eligible entity or multi-entity group dem-
40 onstrates economic hardship.

1 (2) GUIDELINES.—The Secretary shall establish and publish guide-
2 lines for determining what constitutes economic hardship for the pur-
3 poses of this section.

4 (3) CONSIDERATIONS.—In developing guidelines under paragraph
5 (2), the Secretary shall consider, with respect to the jurisdiction of an
6 eligible entity—

7 (A) changes in rates of unemployment in the jurisdiction from
8 previous years;

9 (B) changes in the percentage of individuals who are eligible to
10 receive benefits under the supplemental nutrition assistance pro-
11 gram established under the Food and Nutrition Act of 2008 (7
12 U.S.C. 2011 et seq.) from previous years; and

13 (C) any other factors the Secretary considers appropriate.

14 (c) WAIVER FOR TRIBAL GOVERNMENTS.—Notwithstanding subsection
15 (b), the Secretary, in consultation with the Secretary of the Interior and
16 Tribal governments, may waive or modify the requirements of subsection (a)
17 for 1 or more Tribal governments if the Secretary determines that the waiv-
18 er is in the public interest.

19 **§ 12744. Responsibilities of grantees**

20 (a) CERTIFICATION.—Each eligible entity or multi-entity group that re-
21 ceives a grant under this subchapter shall certify to the Secretary that the
22 grant will be used—

23 (1) for the purpose for which the grant is awarded; and

24 (2) in compliance with sections 12734 and 12740 of this title.

25 (b) AVAILABILITY OF FUNDS TO LOCAL GOVERNMENTS AND RURAL
26 AREAS.—

27 (1) IN GENERAL.—Subject to paragraph (3), not later than 45 days
28 after the date on which an eligible entity or multi-entity group receives
29 a grant under this subchapter, the eligible entity or multi-entity group
30 shall, without imposing unreasonable or unduly burdensome require-
31 ments as a condition of receipt, obligate or otherwise make available
32 to local governments within the jurisdiction of the eligible entity or the
33 eligible entities that comprise the multi-entity group—

34 (A) not less than 80 percent of funds available under the grant;

35 (B) with the consent of the local governments, items, services,
36 capabilities, or activities having a value of not less than 80 percent
37 of the amount of the grant; or

38 (C) with the consent of the local governments, grant funds com-
39 bined with other items, services, capabilities, or activities having
40 a total value of not less than 80 percent of the amount of the
41 grant.

1 (2) AVAILABILITY TO RURAL AREAS.—In obligating funds, items,
2 services, capabilities, or activities to local governments under paragraph
3 (1), the eligible entity or eligible entities that comprise the multi-entity
4 group shall ensure that rural areas within the jurisdiction of the eligi-
5 ble entity or the eligible entities that comprise the multi-entity group
6 receive—

7 (A) not less than 25 percent of the amount of the grant award-
8 ed to the eligible entity;

9 (B) items, services, capabilities, or activities having a value of
10 not less than 25 percent of the amount of the grant awarded to
11 the eligible entity; or

12 (C) grant funds combined with other items, services, capabili-
13 ties, or activities having a total value of not less than 25 percent
14 of the grant awarded to the eligible entity.

15 (3) EXCEPTIONS.—This subsection shall not apply to—

16 (A) a grant awarded under this subchapter that solely supports
17 activities that are integral to the development or revision of the
18 Cybersecurity Plan of the eligible entity; or

19 (B) the District of Columbia, Puerto Rico, Guam, American
20 Samoa, the Virgin Islands, the Northern Mariana Islands, or a
21 Tribal government.

22 (e) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO
23 LOCAL GOVERNMENTS.—An eligible entity or multi-entity group shall cer-
24 tify to the Secretary that the eligible entity or multi-entity group has made
25 the distribution to local governments required under subsection (b).

26 (d) EXTENSION OF PERIOD.—

27 (1) IN GENERAL.—An eligible entity or multi-entity group may re-
28 quest in writing that the Secretary extend the period of time specified
29 in subsection (b) for an additional period of time.

30 (2) APPROVAL.—The Secretary may approve a request for an exten-
31 sion under paragraph (1) if the Secretary determines the extension is
32 necessary to ensure that the obligation and expenditure of grant funds
33 align with the purpose of the State and Local Cybersecurity Grant Pro-
34 gram.

35 (e) DIRECT FUNDING.—If an eligible entity does not make a distribution
36 to a local government required under subsection (b) in a timely fashion, the
37 local government may petition the Secretary to request the Secretary to pro-
38 vide funds directly to the local government.

39 (f) LIMITATION ON CONSTRUCTION.—A grant awarded under this sub-
40 chapter may not be used to acquire land or to construct, remodel, or per-
41 form alterations of buildings or other physical facilities.

1 (g) CONSULTATION IN ALLOCATING FUNDS.—An eligible entity applying
2 for a grant under this subchapter shall agree to consult the Chief Informa-
3 tion Officer, the Chief Information Security Officer, or an equivalent official
4 of the eligible entity in allocating funds from a grant awarded under this
5 subchapter.

6 (h) PENALTIES.—In addition to other remedies available to the Secretary,
7 if an eligible entity violates a requirement of this section, the Secretary
8 may—

9 (1) terminate or reduce the amount of a grant awarded under this
10 subchapter to the eligible entity; or

11 (2) distribute grant funds previously awarded to the eligible entity—

12 (A) in the case of an eligible entity that is a State, directly to
13 the appropriate local government as a replacement grant in an
14 amount determined by the Secretary; or

15 (B) in the case of an eligible entity that is a Tribal government,
16 to another Tribal government or Tribal governments as a replace-
17 ment grant in an amount determined by the Secretary.

18 **§ 12745. Consultation with State, local, and Tribal represent-**
19 **atives**

20 In carrying out this subchapter, the Secretary shall consult with State,
21 local, and Tribal representatives with professional experience relating to cy-
22 bersecurity, including representatives of associations representing State,
23 local, and Tribal governments, to inform—

24 (1) guidance for applicants for grants under this subchapter, includ-
25 ing guidance for Cybersecurity Plans;

26 (2) the study of risk-based formulas required under section 12747(d)
27 of this title;

28 (3) the development of guidelines required under section 12743(b)(2)
29 of this title; and

30 (4) any modifications described in section 12747(b)(4) of this title.

31 **§ 12746. Notification to Congress**

32 Not later than 3 business days before the date on which the Department
33 announces the award of a grant to an eligible entity under this subchapter,
34 including an announcement to the eligible entity, the Secretary shall provide
35 to the appropriate congressional committees notice of the announcement.

36 **§ 12747. Reports, study, and review**

37 (a) ANNUAL REPORTS BY GRANT RECIPIENTS.—

38 (1) IN GENERAL.—Not later than 1 year after the date on which an
39 eligible entity receives a grant under this subchapter for the purpose
40 of implementing the Cybersecurity Plan of the eligible entity, including
41 an eligible entity that comprises a multi-entity group that receives a

1 grant for that purpose, and annually thereafter until 1 year after the
2 date on which funds from the grant are expended or returned, the eligi-
3 ble entity shall submit to the Secretary a report that, using the metrics
4 described in the Cybersecurity Plan of the eligible entity, describes the
5 progress of the eligible entity in—

6 (A) implementing the Cybersecurity Plan of the eligible entity;

7 and

8 (B) reducing cybersecurity risks to, and identifying, responding
9 to, and recovering from cybersecurity threats to, information sys-
10 tems owned or operated by, or on behalf of, the eligible entity or,
11 if the eligible entity is a State, local governments within the juris-
12 diction of the eligible entity.

13 (2) ABSENCE OF PLAN.—Not later than 1 year after the date on
14 which an eligible entity that does not have a Cybersecurity Plan re-
15 ceives funds under this subchapter, and annually thereafter until 1 year
16 after the date on which funds from the grant are expended or returned,
17 the eligible entity shall submit to the Secretary a report describing how
18 the eligible entity obligated and expended grant funds to—

19 (A) develop or revise a Cybersecurity Plan; or

20 (B) assist with the activities described in section 12734(4).

21 (b) ANNUAL REPORTS TO CONGRESS.—Not less frequently than annually,
22 the Secretary, acting through the Director, shall submit to Congress a re-
23 port on—

24 (1) the use of grants awarded under this subchapter;

25 (2) the proportion of grants used to support cybersecurity in rural
26 areas;

27 (3) the effectiveness of the State and Local Cybersecurity Grant Pro-
28 gram;

29 (4) any necessary modifications to the State and Local Cybersecurity
30 Grant Program; and

31 (5) any progress made toward—

32 (A) developing, implementing, or revising Cybersecurity Plans;

33 and

34 (B) reducing cybersecurity risks to, and identifying, responding
35 to, and recovering from cybersecurity threats to, information sys-
36 tems owned or operated by, or on behalf of, State, local, or Tribal
37 governments as a result of the award of grants under this sub-
38 chapter.

39 (c) PUBLIC AVAILABILITY.—

40 (1) IN GENERAL.—The Secretary, acting through the Director, shall
41 make each report submitted under subsection (b) publicly available, in-

1 cluding by making each report available on the website of the Cyberse-
2 curity and Infrastructure Security Agency.

3 (2) REDACTIONS.—In making each report publicly available under
4 paragraph (1), the Director may make redactions that the Director, in
5 consultation with each eligible entity, determines necessary to protect
6 classified or other information exempt from disclosure under section
7 552 of title 5 (known as the Freedom of Information Act).

8 (d) STUDY OF RISK-BASED FORMULAS.—

9 (1) IN GENERAL.—Not later than September 30, 2024, the Sec-
10 retary, acting through the Director, shall submit to the appropriate
11 congressional committees a study and legislative recommendations on
12 the potential use of a risk-based formula for apportioning funds under
13 this subchapter, including—

14 (A) potential components that could be included in a risk-based
15 formula, including the potential impact of those components on
16 support for rural areas under this subchapter;

17 (B) potential sources of data and information necessary for the
18 implementation of a risk-based formula;

19 (C) any obstacles to implementing a risk-based formula, includ-
20 ing obstacles that require a legislative solution;

21 (D) if a risk-based formula were to be implemented for fiscal
22 year 2026, a recommended risk-based formula for the State and
23 Local Cybersecurity Grant Program; and

24 (E) any other information that the Secretary, acting through
25 the Director, determines necessary to help Congress understand
26 the progress towards, and obstacles to, implementing a risk-based
27 formula.

28 (2) INAPPLICABILITY OF PAPERWORK REDUCTION ACT.—The re-
29 quirements of chapter 35 of title 44 (known as the Paperwork Reduc-
30 tion Act) shall not apply to any action taken to carry out this sub-
31 section.

32 (e) TRIBAL CYBERSECURITY NEEDS REPORT.—Not later than 2 years
33 after November 15, 2021, the Secretary, acting through the Director, shall
34 submit to Congress a report that—

35 (1) describes the cybersecurity needs of Tribal governments, which
36 shall be determined in consultation with the Secretary of the Interior
37 and Tribal governments; and

38 (2) includes recommendations for addressing the cybersecurity needs
39 of Tribal governments, including necessary modifications to the State
40 and Local Cybersecurity Grant Program to better serve Tribal govern-
41 ments.

1 (f) COMPTROLLER GENERAL REVIEW.—Not later than 3 years after No-
 2 vember 15, 2021, the Comptroller General shall conduct a review of the
 3 State and Local Cybersecurity Grant program, including—

- 4 (1) the grant selection process of the Secretary; and
 5 (2) a sample of grants awarded under this subchapter.

6 **§ 12748. Authorization of appropriations**

7 (a) IN GENERAL.—There is authorized to be appropriated for activities
 8 under this subchapter—

- 9 (1) for fiscal year 2023, \$400,000,000;
 10 (2) for fiscal year 2024, \$300,000,000; and
 11 (3) for fiscal year 2025, \$100,000,000.

12 (b) TRANSFERS AUTHORIZED.—

13 (1) IN GENERAL.—During a fiscal year, the Secretary or the head
 14 of any component of the Department that administers the State and
 15 Local Cybersecurity Grant Program may transfer not more than 5 per-
 16 cent of the amounts appropriated pursuant to subsection (a) or other
 17 amounts appropriated to carry out the State and Local Cybersecurity
 18 Grant Program for that fiscal year to an account of the Department
 19 for salaries, expenses, and other administrative costs incurred for the
 20 management, administration, or evaluation of this subchapter.

21 (2) ADDITIONAL AMOUNTS.—Funds transferred under paragraph (1)
 22 shall be in addition to funds appropriated to the Department or the
 23 components described in paragraph (1) for salaries, expenses, and other
 24 administrative costs.

25 **§ 12749. Termination**

26 (a) IN GENERAL.—Subject to subsection (b), the requirements of this sec-
 27 tion shall terminate on September 30, 2025.

28 (b) EXCEPTION.—The reporting requirements under section 12747 of this
 29 title shall terminate on the date that is 1 year after the date on which the
 30 final funds from a grant under this subchapter are expended or returned.

31 **Chapter 129—Anti-Trafficking Training for**
 32 **Department Personnel**

Sec.

12901. Definition of human trafficking.
 12902. Training to identify human trafficking.
 12903. Reports.
 12904. Assistance to non-Federal entities.
 12905. Victim protection training.

33 **§ 12901. Definition of human trafficking**

34 In this chapter, the term “human trafficking” means an act or practice
 35 described in paragraph (11) or (12) of section 103 of the Trafficking Vic-
 36 tims Protection Act of 2000 (22 U.S.C. 7102(11), (12)).

1 **§ 12902. Training to identify human trafficking**

2 (a) IN GENERAL.—The Secretary shall implement a program to—

3 (1) train and periodically retrain relevant Transportation Security
4 Administration, U. S. Customs and Border Protection, and other De-
5 partment personnel that the Secretary considers appropriate, with re-
6 spect to how to effectively deter, detect, and disrupt human trafficking,
7 and, where appropriate, interdict a suspected perpetrator of human
8 trafficking, during the course of their primary roles and responsibil-
9 ities; and

10 (2) ensure that the personnel referred to in paragraph (1) regularly
11 receive current information on matters relating to the detection of
12 human trafficking, including information that becomes available outside
13 of the Department’s initial or periodic retraining schedule, to the ex-
14 tent relevant to their official duties and consistent with applicable in-
15 formation and privacy laws.

16 (b) TRAINING.—The training referred to in subsection (a) may be con-
17 ducted through in-class or virtual learning capabilities, and shall include—

18 (1) methods for identifying suspected victims of human trafficking
19 and, where appropriate, perpetrators of human trafficking;

20 (2) for appropriate personnel, methods to approach a suspected vic-
21 tim of human trafficking, where appropriate, in a manner that is sen-
22 sitive to the suspected victim and is not likely to alert a suspected per-
23 petrator of human trafficking;

24 (3) training that is most appropriate for the particular location or
25 environment in which the personnel receiving the training perform their
26 official duties;

27 (4) other topics determined by the Secretary to be appropriate; and

28 (5) a post-training evaluation for personnel receiving the training.

29 (c) TRAINING CURRICULUM REVIEW.—The Secretary shall annually reas-
30 sess the training program established under subsection (a) to ensure it is
31 consistent with current techniques, patterns, and trends associated with
32 human trafficking.

33 **§ 12903. Reports**

34 (a) EFFECTIVENESS OF PROGRAM.—Not later than 1 year after May 29,
35 2015, and annually thereafter, the Secretary shall report to Congress with
36 respect to the overall effectiveness of the program required by this chapter,
37 the number of cases reported by Department personnel in which human
38 trafficking was suspected, and, of those cases, the number of cases that
39 were confirmed cases of human trafficking.

40 (b) HUMAN TRAFFICKING INVESTIGATIONS.—Not later than 1 year after
41 December 21, 2018, and annually thereafter, the Executive Associate Direc-

1 tor of Homeland Security Investigations shall submit to the Committee on
2 Homeland Security and Governmental Affairs and the Committee on the
3 Judiciary of the Senate and the Committee on Homeland Security and the
4 Committee on the Judiciary of the House of Representatives a report on
5 human trafficking investigations undertaken by Homeland Security Inves-
6 tigation that includes—

7 (1) the number of confirmed human trafficking investigations by cat-
8 egory, including labor trafficking, sex trafficking, and transnational
9 and domestic human trafficking;

10 (2) the number of victims by category, including—

11 (A) whether the victim is a victim of sex trafficking or a victim
12 of labor trafficking; and

13 (B) whether the victim is a minor or an adult; and

14 (3) an analysis of the data described in paragraphs (1) and (2) and
15 other data available to Homeland Security Investigations that indicates
16 any general human trafficking or investigatory trends.

17 **§ 12904. Assistance to non-Federal entities**

18 The Secretary may provide training curricula to any State, local, or tribal
19 government, or private organization, to assist the government or organiza-
20 tion in establishing a program of training to identify human trafficking, on
21 request from the government or organization.

22 **§ 12905. Victim protection training**

23 (a) DIRECTIVE TO DEPARTMENT LAW ENFORCEMENT OFFICIALS AND
24 TASK FORCES.—

25 (1) IN GENERAL.—Not later than 180 days after December 21,
26 2018, the Secretary shall issue a directive to—

27 (A) all Federal law enforcement officers and relevant personnel
28 employed by the Department who may be involved in the investiga-
29 tion of human trafficking offenses; and

30 (B) members of all task forces led by the Department that par-
31 ticipate in the investigation of human trafficking offenses.

32 (2) REQUIRED INSTRUCTIONS.—The directive required to be issued
33 under paragraph (1) shall include instructions on—

34 (A) the investigation of individuals who patronize or solicit
35 human trafficking victims as being engaged in severe trafficking
36 in individuals and how individuals who patronize or solicit human
37 trafficking victims should be investigated for their role in severe
38 trafficking in individuals; and

39 (B) how victims of sex or labor trafficking often engage in
40 criminal acts as a direct result of severe trafficking in individuals
41 and how the individuals are victims of a crime, and affirmative

1 measures that should be taken to avoid arresting, charging, or
2 prosecuting those individuals who are victims of a crime for an of-
3 fense that is the direct result of their victimization.

4 (b) VICTIM SCREENING PROTOCOL.—

5 (1) IN GENERAL.—Not later than 180 days after December 21,
6 2018, the Secretary shall issue a screening protocol for use during all
7 anti-trafficking law enforcement operations in which the Department is
8 involved.

9 (2) REQUIREMENTS.—The directive required to be issued under
10 paragraph (1) shall—

11 (A) require the individual screening of all adults and children
12 who are suspected of engaging in commercial sex acts, child labor
13 that is a violation of law, or work in violation of labor standards
14 to determine whether each individual screened is a victim of
15 human trafficking;

16 (B) require affirmative measures to avoid arresting, charging,
17 or prosecuting human trafficking victims for an offense that is the
18 direct result of their victimization;

19 (C) be developed in consultation with relevant inter-agency part-
20 ners and nongovernmental organizations that specialize in the pre-
21 ventions of human trafficking or in the identification and support
22 of victims of human trafficking and survivors of human traf-
23 ficking; and

24 (D) include—

25 (i) procedures and practices to ensure that the screening
26 process minimizes trauma or revictimization of the individual
27 being screened; and

28 (ii) guidelines on assisting victims of human trafficking in
29 identifying and receiving restorative services.

30 (c) MANDATORY TRAINING.—The training described in sections 12902
31 and 12904 of this title shall include training necessary to implement—

32 (1) the directive required under subsection (a); and

33 (2) the protocol required under subsection (b).

34 **Subtitle II—National Emergency**
35 **Management**
36 **Chapter 201—General**

Sec.
20101. Definitions.

37 **§ 20101. Definitions**

38 In this subtitle:

1 (1) ADMINISTRATOR.—The term “Administrator” means the Admin-
2 istrator of the Agency.

3 (2) AGENCY.—The term “Agency” means the Federal Emergency
4 Management Agency.

5 (3) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appro-
6 priate committees of Congress” means—

7 (A) the Committee on Homeland Security and Governmental
8 Affairs of the Senate; and

9 (B) those committees of the House of Representatives that the
10 Speaker of the House of Representatives determines appropriate.

11 (4) CATASTROPHIC INCIDENT.—The term “catastrophic incident”
12 means any natural disaster, act of terrorism, or other man-made dis-
13 aster that results in extraordinary levels of casualties or damage or dis-
14 ruption severely affecting the population (including mass evacuations),
15 infrastructure, environment, economy, national morale, or government
16 functions in an area.

17 (5) DEPARTMENT.—The term “Department” means the Department
18 of Homeland Security.

19 (6) EMERGENCY; MAJOR DISASTER.—The terms “emergency” and
20 “major disaster” have the meanings given the terms in section 102 of
21 the Robert T. Stafford Disaster Relief and Emergency Assistance Act
22 (42 U.S.C. 5122).

23 (7) EMERGENCY MANAGEMENT.—The term “emergency manage-
24 ment” means the governmental function that coordinates and inte-
25 grates all activities necessary to build, sustain, and improve the capa-
26 bility to prepare for, protect against, respond to, recover from, or miti-
27 gate against threatened or actual natural disasters, acts of terrorism,
28 or other man-made disasters.

29 (8) EMERGENCY RESPONSE PROVIDERS.—The term “emergency re-
30 sponse providers” has the meaning given the term in section 10101 of
31 this title.

32 (9) FEDERAL COORDINATING OFFICER.—The term “Federal coordi-
33 nating officer” means a Federal coordinating officer as described in
34 section 302 of the Robert T. Stafford Disaster Relief and Emergency
35 Assistance Act (42 U.S.C. 5143).

36 (10) INDIVIDUAL WITH A DISABILITY.—The term “individual with a
37 disability” has the meaning given the term in section 3 of the Ameri-
38 cans with Disabilities Act of 1990 (42 U.S.C. 12102).

39 (11) LOCAL GOVERNMENT.—The term “local government” has the
40 meaning given the term in section 10101 of this title.

1 (12) NATIONAL INCIDENT MANAGEMENT SYSTEM.—The term “Na-
2 tional Incident Management System” means a system to enable effec-
3 tive, efficient, and collaborative incident management.

4 (13) NATIONAL RESPONSE PLAN.—The term “National Response
5 Plan” means the National Response Plan or any successor plan pre-
6 pared under section 11303(a)(6) of this title.

7 (14) SECRETARY.—The term “Secretary” means the Secretary of
8 Homeland Security.

9 (15) STATE.—The term “State” has the meaning given the term in
10 section 10101 of this title.

11 (16) SURGE CAPACITY.—The term “surge capacity” means the abil-
12 ity to rapidly and substantially increase the provision of search and res-
13 cue capabilities, food, water, medicine, shelter and housing, medical
14 care, evacuation capacity, staffing (including disaster assistance em-
15 ployees), and other resources necessary to save lives and protect prop-
16 erty during a catastrophic incident.

17 (17) TRIBAL GOVERNMENT.—The term “tribal government” means
18 the government of an Indian tribe or authorized tribal organization, or,
19 in Alaska, a Native village or Alaska Regional Native Corporation.

20 **Chapter 203—Emergency Management** 21 **Capabilities**

Sec.

20301. Surge Capacity Force.

20302. Evacuation preparedness technical assistance.

20303. Urban Search and Rescue Response System.

20304. Metropolitan Medical Response System Program.

20305. Logistics.

20306. Pre-positioned equipment program.

20307. Basic life supporting first aid and education.

20308. Improvements to information technology systems.

20309. Disclosure of certain information to law enforcement agencies.

22 **§ 20301. Surge Capacity Force**

23 (a) ESTABLISHMENT.—

24 (1) IN GENERAL.—The Administrator shall prepare and submit to
25 the appropriate committees of Congress a plan to establish and imple-
26 ment a Surge Capacity Force for deployment of individuals to respond
27 to natural disasters, acts of terrorism, and other man-made disasters,
28 including catastrophic incidents.

29 (2) AUTHORITY.—

30 (A) IN GENERAL.—Except as provided in subparagraph (B), the
31 plan shall provide for individuals in the Surge Capacity Force to
32 be trained and deployed under the authorities set forth in the Rob-
33 ert T. Stafford Disaster Relief and Emergency Assistance Act (42
34 U.S.C. 5121 et seq.).

1 (B) EXCEPTION.—If the Administrator determines that the ex-
2 isting authorities are inadequate for the training and deployment
3 of individuals in the Surge Capacity Force, the Administrator shall
4 report to Congress as to the additional statutory authorities that
5 the Administrator determines necessary.

6 (b) EMPLOYEES DESIGNATED TO SERVE.—The plan shall include proce-
7 dures under which the Secretary shall designate employees of the Depart-
8 ment who are not employees of the Agency and shall, in conjunction with
9 the heads of other Executive agencies, designate employees of those other
10 Executive agencies, as appropriate, to serve on the Surge Capacity Force.

11 (c) CAPABILITIES.—The plan shall ensure that the Surge Capacity
12 Force—

13 (1) includes a sufficient number of individuals credentialed under
14 section 11310 of this title that are capable of deploying rapidly and ef-
15 ficiently after activation to prepare for, respond to, and recover from
16 natural disasters, acts of terrorism, and other man-made disasters, in-
17 cluding catastrophic incidents; and

18 (2) includes a sufficient number of full-time, highly trained individ-
19 uals credentialed under section 11310 of this title to lead and manage
20 the Surge Capacity Force.

21 (d) TRAINING.—The plan shall ensure that the Administrator provides
22 appropriate and continuous training to members of the Surge Capacity
23 Force to ensure the personnel are adequately trained on the Agency's pro-
24 grams and policies for natural disasters, acts of terrorism, and other man-
25 made disasters.

26 (e) NO IMPACT ON AGENCY PERSONNEL CEILING.—Surge Capacity
27 Force members shall not be counted against any personnel ceiling applicable
28 to the Agency.

29 (f) EXPENSES.—The Administrator may provide members of the Surge
30 Capacity Force with travel expenses, including per diem in lieu of subsist-
31 ence, at rates authorized for employees of agencies under subchapter I of
32 chapter 57 of title 5, for the purpose of participating in any training that
33 relates to service as a member of the Surge Capacity Force.

34 (g) IMMEDIATE IMPLEMENTATION OF SURGE CAPACITY FORCE INVOLV-
35 ING FEDERAL EMPLOYEES.—The Administrator shall develop and imple-
36 ment—

37 (1) the procedures under subsection (b); and

38 (2) other elements of the plan needed to establish the portion of the
39 Surge Capacity Force consisting of individuals designated under those
40 procedures.

1 **§ 20302. Evacuation preparedness technical assistance**

2 (a) IN GENERAL.—The Administrator, in coordination with the heads of
3 other appropriate Federal agencies, shall provide evacuation preparedness
4 technical assistance to State, local, and tribal governments, including the
5 preparation of hurricane evacuation studies and technical assistance in de-
6 veloping evacuation plans, assessing storm surge estimates, evacuation
7 zones, evacuation clearance times, transportation capacity, and shelter ca-
8 pacity.

9 (b) GUIDANCE ON EVACUATION ROUTES.—

10 (1) DEFINITION OF STATE.—In this subsection, the term “State”
11 has the meaning given the term in section 102 of the Robert T. Staf-
12 ford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

13 (2) ADMINISTRATOR.—The Administrator, in coordination with the
14 Administrator of the Federal Highway Administration, shall develop
15 and issue guidance for State, local, and Indian tribal governments re-
16 garding the identification of evacuation routes. In developing the guid-
17 ance, the Administrator shall consider—

18 (A) whether evacuation routes have resisted impacts and recov-
19 ered quickly from disasters, regardless of cause;

20 (B) the need to evacuate special needs populations, including—

21 (i) individuals with a physical or mental disability;

22 (ii) individuals in schools, daycare centers, mobile home
23 parks, prisons, nursing homes and other long-term care facili-
24 ties, and detention centers;

25 (iii) individuals with limited English proficiency;

26 (iv) the elderly; and

27 (v) individuals who are tourists, seasonal workers, or home-
28 less;

29 (C) the sharing of information and other public communications
30 with evacuees during evacuations;

31 (D) the sheltering of evacuees, including the care, protection,
32 and sheltering of animals;

33 (E) the return of evacuees to their homes; and

34 (F) other items the Administrator considers appropriate.

35 (3) ADMINISTRATOR OF FEDERAL HIGHWAY ADMINISTRATION.—The
36 Administrator of the Federal Highway Administration, in coordination
37 with the Administrator, shall revise existing guidance or issue new
38 guidance as appropriate for State, local, and Indian tribal governments
39 regarding the design, construction, maintenance, and repair of evacu-
40 ation routes. In revising or issuing the guidance, the Administrator of
41 the Federal Highway Administration shall consider—

- 1 (A) methods that assist evacuation routes to—
- 2 (i) withstand likely risks to viability, including flammability
- 3 and hydrostatic forces;
- 4 (ii) improve durability, strength (including the ability to
- 5 withstand tensile stresses and compressive stresses), and sus-
- 6 tainability; and
- 7 (iii) provide for long-term cost savings;
- 8 (B) the ability of evacuation routes to effectively manage
- 9 contraflow operations;
- 10 (C) for evacuation routes on public lands, the viewpoints of the
- 11 applicable Federal land management agency regarding emergency
- 12 operations, sustainability, and resource protection; and
- 13 (D) other items the Administrator of the Federal Highway Ad-
- 14 ministration considers appropriate.

15 (4) STUDY.—The Administrator, in coordination with the Adminis-

16 trator of the Federal Highway Administration and State, local, and In-

17 dian tribal governments, may—

- 18 (A) conduct a study of the adequacy of available evacuation
- 19 routes to accommodate the flow of evacuees; and
- 20 (B) submit recommendations on how to help with anticipated
- 21 evacuation route flow, based on the study, to—
- 22 (i) the Federal Highway Administration;
- 23 (ii) the Agency;
- 24 (iii) State, local, and Indian tribal governments; and
- 25 (iv) Congress.

26 **§ 20303. Urban Search and Rescue Response System**

27 There is in the Agency the Urban Search and Rescue Response System.

28 **§ 20304. Metropolitan Medical Response System Program**

29 (a) IN GENERAL.—There is in the Agency the Metropolitan Medical Re-

30 sponse System Program.

31 (b) PURPOSES.—The Metropolitan Medical Response System Program

32 shall include each purpose of the Program as it existed on June 1, 2006.

33 **§ 20305. Logistics**

34 The Administrator shall develop an efficient, transparent, and flexible lo-

35 gistics system for procurement and delivery of goods and services necessary

36 for an effective and timely response to natural disasters, acts of terrorism,

37 and other man-made disasters and for real-time visibility of items at each

38 point throughout the logistics system.

39 **§ 20306. Pre-positioned equipment program**

40 (a) IN GENERAL.—The Administrator shall establish a pre-positioned

41 equipment program to pre-position standardized emergency equipment in at

1 least 11 locations to sustain and replenish critical assets used by State,
2 local, and tribal governments in response to (or rendered inoperable by the
3 effects of) natural disasters, acts of terrorism, and other man-made disas-
4 ters.

5 (b) NOTICE.—Not later than 60 days before the date of closure, the Ad-
6 ministrator shall notify State, local, and tribal officials in an area in which
7 a location for the pre-positioned equipment program will be closed.

8 **§ 20307. Basic life supporting first aid and education**

9 The Administrator shall enter into agreements with organizations to pro-
10 vide funds to emergency response providers to provide education and train-
11 ing in life supporting first aid to children.

12 **§ 20308. Improvements to information technology systems**

13 The Administrator, in coordination with the Chief Information Officer of
14 the Department, shall take appropriate measures to update and improve the
15 information technology systems of the Agency, including measures to—

16 (1) ensure that the multiple information technology systems of the
17 Agency (including the National Emergency Management Information
18 System, the Logistics Information Management System III, and the
19 Automated Deployment Database) are, to the extent practicable, fully
20 compatible and can share and access information, as appropriate, from
21 each other;

22 (2) ensure technology enhancements reach the headquarters and re-
23 gional offices of the Agency in a timely fashion, to allow seamless inte-
24 gration;

25 (3) develop and maintain a testing environment that ensures that all
26 system components are properly and thoroughly tested before their re-
27 lease;

28 (4) ensure that the information technology systems of the Agency
29 have the capacity to track disaster response personnel, mission assign-
30 ment task orders, commodities, and supplies used in response to a nat-
31 ural disaster, act of terrorism, or other man-made disaster;

32 (5) make appropriate improvements to the National Emergency
33 Management Information System to address shortcomings in the sys-
34 tem on October 4, 2006; and

35 (6) provide training, manuals, and guidance on information tech-
36 nology systems to personnel, including disaster response personnel, to
37 help ensure employees can properly use information technology sys-
38 tems.

1 **§ 20309. Disclosure of certain information to law enforce-**
 2 **ment agencies**

3 If circumstances require an evacuation, sheltering, or mass relocation, the
 4 Administrator may disclose information in any individual assistance data-
 5 base of the Agency under section 552a(b) of title 5 to any law enforcement
 6 agency of the Federal Government or a State, local, or tribal government
 7 in order to identify illegal conduct or address public safety or security
 8 issues, including compliance with sex offender notification laws.

9 **Chapter 205—Comprehensive**
 10 **Preparedness System**

Subchapter I—National Preparedness System

Sec.

- 20501. Definitions.
- 20502. Development of national preparedness goal and national preparedness system.
- 20503. National preparedness goal.
- 20504. National preparedness system.
- 20505. National planning scenarios.
- 20506. Target capabilities and preparedness priorities.
- 20507. Equipment and training standards.
- 20508. Training and exercises.
- 20509. Comprehensive assessment system.
- 20510. Remedial action management program.
- 20511. Federal response capability inventory.
- 20512. Reporting requirements.
- 20513. Federal preparedness.
- 20514. Use of existing resources.

Subchapter II—Additional Preparedness

- 20521. Emergency Management Assistance Compact grants.
- 20522. Emergency Management Performance Grants Program.
- 20523. Training for emergency response providers from Federal Government, foreign govern-
 ments, or private entities.
- 20524. National exercise simulation center.
- 20525. Real property transactions.

Subchapter III—Miscellaneous Authorities

- 20531. National Disaster Recovery Strategy.
- 20532. National Disaster Housing Strategy.
- 20533. Individuals with disabilities guidelines.
- 20534. Reunification.
- 20535. National Emergency Family Registry and Locator System.

11 **Subchapter I—National Preparedness**
 12 **System**

13 **§ 20501. Definitions**

14 In this chapter:

- 15 (1) CAPABILITY.—The term “capability” means the ability to provide
 16 the means to accomplish one or more tasks under specific conditions
 17 and to meet specific performance standards. A capability may be
 18 achieved with any combination of properly planned, organized,
 19 equipped, trained, and exercised personnel that achieves the intended
 20 outcome.

1 (2) CREDENTIALLED; CREDENTIALING.—The terms “credentialed”
2 and “credentialing” have the meanings given the terms in section
3 11301 of this title.

4 (3) HAZARD.—The term “hazard” has the meaning given the term
5 under section 602(a) of the Robert T. Stafford Disaster Relief and As-
6 sistance Act (42 U.S.C. 5195a(a)).

7 (4) MISSION ASSIGNMENT.—The term “mission assignment” means
8 a work order issued to a Federal agency by the Agency, directing com-
9 pletion by that agency of a specified task and setting forth funding,
10 other managerial controls, and guidance.

11 (5) NATIONAL PREPAREDNESS GOAL.—The term “national prepared-
12 ness goal” means the national preparedness goal established under sec-
13 tion 20503 of this title.

14 (6) NATIONAL PREPAREDNESS SYSTEM.—The term “national pre-
15 paredness system” means the national preparedness system established
16 under section 20504 of this title.

17 (7) NATIONAL TRAINING PROGRAM.—The term “national training
18 program” means the national training program established under sec-
19 tion 20508(a) of this title.

20 (8) OPERATIONAL READINESS.—The term “operational readiness”
21 means the capability of an organization, an asset, a system, or equip-
22 ment to perform the missions or functions for which it is organized or
23 designed.

24 (9) PERFORMANCE MEASURE.—The term “performance measure”
25 means a quantitative or qualitative characteristic used to gauge the re-
26 sults of an outcome compared to its intended purpose.

27 (10) PERFORMANCE METRIC.—The term “performance metric”
28 means a particular value or characteristic used to measure the outcome
29 that is generally expressed in terms of a baseline and a target.

30 (11) PREVENTION.—The term “prevention” means any activity un-
31 dertaken to avoid, prevent, or stop a threatened or actual act of ter-
32 rorism.

33 (12) RESOURCES.—The term “resources” has the meaning given the
34 term in section 11301 of this title.

35 (13) TYPE.—The term “type” means a classification of resources
36 that refers to the capability of a resource.

37 (14) TYPED; TYPING.—The terms “typed” and “typing” have the
38 meanings given the terms in section 11301 of this title.

1 **§ 20502. Development of national preparedness goal and na-**
2 **tional preparedness system**

3 To prepare the Nation for all hazards, including natural disasters, acts
4 of terrorism, and other man-made disasters, the President, consistent with
5 the declaration of policy under section 601 of the Robert T. Stafford Dis-
6 aster Relief and Emergency Assistance Act (42 U.S.C. 5195) and chapter
7 113 of this title, shall develop a national preparedness goal and a national
8 preparedness system.

9 **§ 20503. National preparedness goal**

10 (a) ESTABLISHMENT.—The President, acting through the Administrator,
11 shall complete, revise, and update, as necessary, a national preparedness
12 goal that defines the target level of preparedness to ensure the Nation’s
13 ability to prevent, respond to, recover from, and mitigate against natural
14 disasters, acts of terrorism, and other man-made disasters.

15 (b) CONSISTENT WITH NATIONAL INCIDENT MANAGEMENT SYSTEM AND
16 NATIONAL RESPONSE PLAN.—The national preparedness goal, to the great-
17 est extent practicable, shall be consistent with the National Incident Man-
18 agement System and the National Response Plan.

19 **§ 20504. National preparedness system**

20 (a) ESTABLISHMENT.—The President, acting through the Administrator,
21 shall develop a national preparedness system to enable the Nation to meet
22 the national preparedness goal.

23 (b) COMPONENTS.—The national preparedness system shall include the
24 following components:

- 25 (1) Target capabilities and preparedness priorities.
- 26 (2) Equipment and training standards.
- 27 (3) Training and exercises.
- 28 (4) A comprehensive assessment system.
- 29 (5) A remedial action management program.
- 30 (6) A Federal response capability inventory.
- 31 (7) Reporting requirements.
- 32 (8) Federal preparedness.

33 (c) NATIONAL PLANNING SCENARIOS.—The national preparedness system
34 may include national planning scenarios.

35 **§ 20505. National planning scenarios**

36 (a) IN GENERAL.—The Administrator, in coordination with the heads of
37 appropriate Federal agencies and the National Advisory Council, may de-
38 velop planning scenarios to reflect the relative risk requirements presented
39 by all hazards, including natural disasters, acts of terrorism, and other
40 man-made disasters, to provide the foundation for the flexible and adaptive

1 development of target capabilities and the identification of target capability
2 levels to meet the national preparedness goal.

3 (b) DEVELOPMENT.—In developing, revising, and replacing national plan-
4 ning scenarios, the Administrator shall ensure that the scenarios—

5 (1) reflect the relative risk of all hazards and illustrate the potential
6 scope, magnitude, and complexity of a broad range of representative
7 hazards; and

8 (2) provide the minimum number of representative scenarios nec-
9 essary to identify and define the tasks and target capabilities required
10 to respond to all hazards.

11 **§ 20506. Target capabilities and preparedness priorities**

12 (a) ESTABLISHMENT OF GUIDELINES ON TARGET CAPABILITIES.—The
13 Administrator, in coordination with the heads of appropriate Federal agen-
14 cies, the National Council on Disability, and the National Advisory Council,
15 shall complete, revise, and update, as necessary, guidelines to define risk-
16 based target capabilities for Federal, State, local, and tribal government
17 preparedness that will enable the Nation to prevent, respond to, recover
18 from, and mitigate against all hazards, including natural disasters, acts of
19 terrorism, and other man-made disasters.

20 (b) DISTRIBUTION OF GUIDELINES.—The Administrator shall ensure that
21 the guidelines are provided promptly to the appropriate committees of Con-
22 gress and the States.

23 (c) OBJECTIVES.—The Administrator shall ensure that the guidelines are
24 specific, flexible, and measurable.

25 (d) TERRORISM RISK ASSESSMENT.—With respect to analyzing and as-
26 sessing the risk of acts of terrorism, the Administrator shall consider—

27 (1) the variables of threat, vulnerability, and consequences related to
28 population (including transient commuting and tourist populations),
29 areas of high population density, critical infrastructure, coastline, and
30 international borders; and

31 (2) the most current risk assessment available from the Chief Intel-
32 ligence Officer of the Department of the threats of terrorism against
33 the United States.

34 (e) PREPAREDNESS PRIORITIES.—In establishing the guidelines under
35 subsection (a), the Administrator shall establish preparedness priorities that
36 appropriately balance the risk of all hazards, including natural disasters,
37 acts of terrorism, and other man-made disasters, with the resources re-
38 quired to prevent, respond to, recover from, and mitigate against the haz-
39 ards.

40 (f) MUTUAL AID AGREEMENTS.—The Administrator may provide support
41 for the development of mutual aid agreements in States.

1 **§ 20507. Equipment and training standards**

2 (a) **EQUIPMENT STANDARDS.**—

3 (1) **IN GENERAL.**—The Administrator, in coordination with the
4 heads of appropriate Federal agencies and the National Advisory Coun-
5 cil, shall support the development, promulgation, and updating, as nec-
6 essary, of national voluntary consensus standards for the performance,
7 use, and validation of equipment used by Federal, State, local, and
8 tribal governments and nongovernmental emergency response providers.

9 (2) **REQUIREMENTS.**—The national voluntary consensus standards
10 shall—

11 (A) be designed to achieve equipment and other capabilities con-
12 sistent with the national preparedness goal, including the safety
13 and health of emergency response providers;

14 (B) to the maximum extent practicable, be consistent with exist-
15 ing national voluntary consensus standards;

16 (C) take into account, as appropriate, threats that may not have
17 been contemplated when the existing standards were developed;
18 and

19 (D) focus on maximizing operability, interoperability, inter-
20 changeability, durability, flexibility, efficiency, efficacy, portability,
21 sustainability, and safety.

22 (b) **TRAINING STANDARDS.**—The Administrator shall—

23 (1) support the development, promulgation, and regular updating, as
24 necessary, of national voluntary consensus standards for training; and

25 (2) ensure that the training provided under the national training
26 program is consistent with the standards.

27 (c) **CONSULTATION WITH STANDARDS ORGANIZATIONS.**—In carrying out
28 this section, the Administrator shall consult with representatives of relevant
29 public- and private-sector national voluntary consensus standards develop-
30 ment organizations.

31 **§ 20508. Training and exercises**

32 (a) **NATIONAL TRAINING PROGRAM.**—

33 (1) **IN GENERAL.**—The Administrator, in coordination with the
34 heads of appropriate Federal agencies, the National Council on Dis-
35 ability, and the National Advisory Council, shall carry out a national
36 training program to implement the national preparedness goal, Na-
37 tional Incident Management System, National Response Plan, and
38 other related plans and strategies.

39 (2) **TRAINING PARTNERS.**—In developing and implementing the na-
40 tional training program, the Administrator shall—

1 (A) work with government training facilities, academic institu-
2 tions, private organizations, and other entities that provide special-
3 ized, state-of-the-art training for emergency managers or emer-
4 gency response providers; and

5 (B) utilize, as appropriate, training courses provided by commu-
6 nity colleges, State and local public safety academies, State and
7 private universities, and other facilities.

8 (b) NATIONAL EXERCISE PROGRAM.—

9 (1) IN GENERAL.—The Administrator, in coordination with the
10 heads of appropriate Federal agencies, the National Council on Dis-
11 ability, and the National Advisory Council, shall carry out a national
12 exercise program to test and evaluate the national preparedness goal,
13 National Incident Management System, National Response Plan, and
14 other related plans and strategies.

15 (2) REQUIREMENTS.—The national exercise program—

16 (A) shall be—

17 (i) as realistic as practicable, based on current risk assess-
18 ments, including credible and emerging threats,
19 vulnerabilities, and consequences, and designed to stress the
20 national preparedness system;

21 (ii) designed, as practicable, to simulate the partial or com-
22 plete incapacitation of a State, local, or tribal government;

23 (iii) carried out, as appropriate, with a minimum degree of
24 notice to involved parties regarding the timing and details of
25 the exercises, consistent with safety considerations;

26 (iv) designed to provide for the systematic evaluation of
27 readiness and enhance operational understanding of the inci-
28 dent command system and relevant mutual aid agreements;

29 (v) designed to address the unique requirements of popu-
30 lations with special needs, including the elderly; and

31 (vi) designed to promptly develop after-action reports and
32 plans for quickly incorporating lessons learned into future op-
33 erations; and

34 (B) shall include a selection of model exercises that State, local,
35 and tribal governments can readily adapt for use and provide as-
36 sistance to State, local, and tribal governments with the design,
37 implementation, and evaluation of exercises (whether a model exer-
38 cise program or an exercise designed locally) that—

39 (i) conform to the requirements under subparagraph (A);

40 (ii) are consistent with any applicable State, local, or tribal
41 strategy or plan; and

1 (iii) provide for systematic evaluation of readiness.

2 (3) NATIONAL LEVEL EXERCISES.—Periodically but not less than bi-
3 ennially, the Administrator shall perform national exercises to test and
4 evaluate the following:

5 (A) The capability of Federal, State, local, and tribal govern-
6 ments to detect, disrupt, and prevent threatened or actual cata-
7 strophic acts of terrorism, especially those involving weapons of
8 mass destruction.

9 (B) The readiness of Federal, State, local, and tribal govern-
10 ments to respond and recover in a coordinated and unified manner
11 to catastrophic incidents.

12 (c) ANNUAL GUIDANCE AND TRAINING.—The Administrator shall provide
13 guidance and training on an annual basis to State, local, and Indian tribal
14 governments, first responders, and utility companies on—

15 (1) the need to prioritize assistance to hospitals, nursing homes, and
16 other long-term care facilities to ensure that the health care facilities
17 remain functioning or return to functioning as soon as practicable dur-
18 ing power outages caused by natural hazards, including severe weather
19 events;

20 (2) how hospitals, nursing homes, and other long-term care facilities
21 should adequately prepare for power outages during a major disaster
22 or emergency, as those terms are defined in section 102 of the Robert
23 T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C.
24 5122); and

25 (3) how State, local, and Indian tribal governments, first responders,
26 utility companies, hospitals, nursing homes, and other long-term care
27 facilities should develop a strategy to coordinate emergency response
28 plans, including the activation of emergency response plans, in antici-
29 pation of a major disaster, including severe weather events.

30 **§ 20509. Comprehensive assessment system**

31 (a) ESTABLISHMENT.—The Administrator, in coordination with the Na-
32 tional Council on Disability and the National Advisory Council, shall estab-
33 lish a comprehensive system to assess, on an ongoing basis, the Nation's
34 prevention capabilities and overall preparedness, including operational readi-
35 ness.

36 (b) PERFORMANCE METRICS AND MEASURES.—The Administrator shall
37 ensure that each component of the national preparedness system, National
38 Incident Management System, National Response Plan, and other related
39 plans and strategies, and the reports required under section 20512 of this
40 title are developed, revised, and updated with clear and quantifiable per-
41 formance metrics, measures, and outcomes.

1 (c) CONTENTS.—The assessment system established under subsection (a)
2 shall assess—

3 (1) compliance with the national preparedness system, National Inci-
4 dent Management System, National Response Plan, and other related
5 plans and strategies;

6 (2) capability levels at the time of assessment against target capa-
7 bility levels defined pursuant to the guidelines established under section
8 20506(a) of this title;

9 (3) resources needed to meet the desired target capability levels de-
10 fined pursuant to the guidelines established under section 20506(a) of
11 this title; and

12 (4) performance of training, exercises, and operations.

13 **§ 20510. Remedial action management program**

14 The Administrator, in coordination with the National Council on Dis-
15 ability and the National Advisory Council, shall establish a remedial action
16 management program to—

17 (1) analyze training, exercises, and real-world events to identify and
18 disseminate lessons learned and best practices;

19 (2) generate and disseminate, as appropriate, after-action reports to
20 participants in exercises and real-world events; and

21 (3) conduct remedial action tracking and long-term trend analysis.

22 **§ 20511. Federal response capability inventory**

23 (a) IN GENERAL.—Under section 611(h)(1)(C) of the Robert T. Stafford
24 Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196(h)(1)(C)),
25 the Administrator shall accelerate the completion of the inventory of Federal
26 response capabilities.

27 (b) CONTENTS.—For each Federal agency with responsibilities under the
28 National Response Plan, the inventory shall include—

29 (1) for each capability—

30 (A) the performance parameters of the capability;

31 (B) the time frame within which the capability can be brought
32 to bear on an incident; and

33 (C) the readiness of the capability to respond to all hazards, in-
34 cluding natural disasters, acts of terrorism, and other man-made
35 disasters;

36 (2) a list of personnel credentialed under section 11310 of this title;

37 (3) a list of resources typed under section 11310 of this title; and

38 (4) emergency communications assets maintained by the Federal
39 Government and, if appropriate, State, local, and tribal governments
40 and the private sector.

1 (c) DEPARTMENT OF DEFENSE.—The Administrator, in coordination
2 with the Secretary of Defense, shall develop a list of organizations and func-
3 tions within the Department of Defense that may be used, pursuant to the
4 authority provided under the National Response Plan and sections 402,
5 403, and 502 of the Robert T. Stafford Disaster Relief and Emergency As-
6 sistance Act (42 U.S.C. 5170a, 5170b, 5192), to provide support to civil
7 authorities during natural disasters, acts of terrorism, and other man-made
8 disasters.

9 (d) DATABASE.—The Administrator shall establish an inventory database
10 to allow—

11 (1) real-time exchange of information regarding—

12 (A) capabilities;

13 (B) readiness;

14 (C) the compatibility of equipment;

15 (D) credentialed personnel; and

16 (E) typed resources;

17 (2) easy identification and rapid deployment of capabilities,
18 credentialed personnel, and typed resources during an incident; and

19 (3) the sharing of the inventory described in subsection (a) with
20 other Federal agencies, as appropriate.

21 **§ 20512. Reporting requirements**

22 (a) FEDERAL PREPAREDNESS REPORT.—

23 (1) IN GENERAL.—The Administrator, in coordination with the
24 heads of appropriate Federal agencies, shall submit annually to the ap-
25 propriate committees of Congress a report on the Nation's level of pre-
26 paredness for all hazards, including natural disasters, acts of terrorism,
27 and other man-made disasters.

28 (2) CONTENTS.—Each report shall include—

29 (A) an assessment of how Federal assistance supports the na-
30 tional preparedness system;

31 (B) the results of the comprehensive assessment carried out
32 under section 20509 of this title;

33 (C) a review of the inventory described in section 20511 of this
34 title, including the number and type of credentialed personnel in
35 each category of personnel trained and ready to respond to a nat-
36 ural disaster, act of terrorism, or other man-made disaster;

37 (D) an assessment of resources needed to meet preparedness
38 priorities established under section 20506(e) of this title, includ-
39 ing—

1 (i) an estimate of the amount of Federal, State, local, and
2 tribal expenditures required to attain the preparedness prior-
3 ities; and

4 (ii) the extent to which the use of Federal assistance dur-
5 ing the preceding fiscal year achieved the preparedness prior-
6 ities;

7 (E) an evaluation of the extent to which grants administered by
8 the Department, including grants under chapter 127 of this title—

9 (i) have contributed to the progress of State, local, and
10 tribal governments in achieving target capabilities; and

11 (ii) have led to the reduction of risk from natural disasters,
12 acts of terrorism, or other man-made disasters nationally and
13 in State, local, and tribal jurisdictions; and

14 (F) a discussion of whether the list of credentialed personnel of
15 the Agency described in section 20511(b)(2) of this title—

16 (i) complies with the strategic human capital plan devel-
17 oped under section 10102 of title 5; and

18 (ii) is sufficient to respond to a natural disaster, act of ter-
19 rorism, or other man-made disaster, including a catastrophic
20 incident.

21 (b) CATASTROPHIC RESOURCE ESTIMATE.—

22 (1) IN GENERAL.—The Administrator shall develop and submit an-
23 nually to the appropriate committees of Congress an estimate of the
24 resources of the Agency and other Federal agencies needed for, and de-
25 voted specifically to, developing the capabilities of Federal, State, local,
26 and tribal governments necessary to respond to a catastrophic incident.

27 (2) CONTENTS.—Each estimate shall include the resources necessary
28 for and devoted to—

29 (A) planning;

30 (B) training and exercises;

31 (C) Regional Office enhancements;

32 (D) staffing, including for surge capacity during a catastrophic
33 incident;

34 (E) additional logistics capabilities;

35 (F) other responsibilities under the catastrophic incident annex
36 and the catastrophic incident supplement of the National Response
37 Plan;

38 (G) State, local, and tribal government catastrophic incident
39 preparedness; and

40 (H) increases in the fixed costs or expenses of the Agency, in-
41 cluding rent or property acquisition costs or expenses, taxes, con-

1 tributions to the working capital fund of the Department, and se-
2 curity costs for the year after the year in which the estimate is
3 submitted.

4 (e) STATE PREPAREDNESS REPORT.—

5 (1) IN GENERAL.—A State receiving Federal preparedness assistance
6 administered by the Department annually shall submit a report to the
7 Administrator on the State’s level of preparedness.

8 (2) CONTENTS.—Each report shall include—

9 (A) an assessment of State compliance with the national pre-
10 paredness system, National Incident Management System, Na-
11 tional Response Plan, and other related plans and strategies;

12 (B) an assessment of current capability levels and a description
13 of target capability levels; and

14 (C) a discussion of the extent to which target capabilities identi-
15 fied in the applicable State homeland security plan and other ap-
16 plicable plans remain unmet and an assessment of resources need-
17 ed to meet the preparedness priorities established under section
18 20506(e) of this title, including—

19 (i) an estimate of the amount of expenditures required to
20 attain the preparedness priorities; and

21 (ii) the extent to which the use of Federal assistance dur-
22 ing the preceding fiscal year achieved the preparedness prior-
23 ities.

24 **§ 20513. Federal preparedness**

25 (a) AGENCY RESPONSIBILITY.—In support of the national preparedness
26 system, the President shall ensure that each Federal agency with respon-
27 sibilities under the National Response Plan—

28 (1) has the operational capability to meet the national preparedness
29 goal, including—

30 (A) the personnel to make and communicate decisions;

31 (B) organizational structures that are assigned, trained, and ex-
32 ercised for the missions of the agency;

33 (C) sufficient physical resources; and

34 (D) the command, control, and communication channels to
35 make, monitor, and communicate decisions;

36 (2) complies with the National Incident Management System, includ-
37 ing credentialing of personnel and typing of resources likely needed to
38 respond to a natural disaster, act of terrorism, or other man-made dis-
39 aster under section 11310 of this title;

1 (3) develops, trains, and exercises rosters of response personnel to
2 be deployed when the agency is called on to support a Federal re-
3 sponse;

4 (4) develops deliberate operational plans and the corresponding capa-
5 bilities, including crisis planning, to respond effectively to natural dis-
6 asters, acts of terrorism, and other man-made disasters in support of
7 the National Response Plan to ensure a coordinated Federal response;
8 and

9 (5) regularly updates, verifies the accuracy of, and provides to the
10 Administrator the information in the inventory required under section
11 20511 of this title.

12 (b) OPERATIONAL PLANS.—An operations plan developed under sub-
13 section (a)(4) shall meet the following requirements:

14 (1) The operations plan shall be coordinated under a unified system
15 with a common terminology, approach, and framework.

16 (2) The operations plan shall be developed, in coordination with
17 State, local, and tribal government officials, to address both regional
18 and national risks.

19 (3) The operations plan shall contain, as appropriate, the following
20 elements:

21 (A) Concepts of operations.

22 (B) Critical tasks and responsibilities.

23 (C) Detailed resource and personnel requirements, together with
24 sourcing requirements.

25 (D) Specific provisions for the rapid integration of the resources
26 and personnel of the agency into the overall response.

27 (4) The operations plan shall address, as appropriate, the following
28 matters:

29 (A) Support of State, local, and tribal governments in con-
30 ducting mass evacuations, including—

31 (i) transportation and relocation;

32 (ii) short- and long-term sheltering and accommodation;

33 (iii) provisions for populations with special needs, keeping
34 families together, and expeditious location of missing chil-
35 dren; and

36 (iv) policies and provisions for pets.

37 (B) The preparedness and deployment of public health and med-
38 ical resources, including resources to address the needs of evacuees
39 and populations with special needs.

1 (C) The coordination of interagency search and rescue oper-
2 ations, including land, water, and airborne search and rescue oper-
3 ations.

4 (D) The roles and responsibilities of the Senior Federal Law
5 Enforcement Official with respect to other law enforcement enti-
6 ties.

7 (E) The protection of critical infrastructure.

8 (F) The coordination of maritime salvage efforts among relevant
9 agencies.

10 (G) The coordination of Department of Defense and National
11 Guard support of civilian authorities.

12 (H) To the extent practicable, the utilization of Department of
13 Defense, National Air and Space Administration, National Oceanic
14 and Atmospheric Administration, and commercial aircraft and sat-
15 ellite remotely sensed imagery.

16 (I) The coordination and integration of support from the private
17 sector and nongovernmental organizations.

18 (J) The safe disposal of debris, including hazardous materials,
19 and, when practicable, the recycling of debris.

20 (K) The identification of the required surge capacity.

21 (L) Specific provisions for the recovery of affected geographic
22 areas.

23 (e) MISSION ASSIGNMENTS.—To expedite the provision of assistance
24 under the National Response Plan, the President shall ensure that the Ad-
25 ministrator, in coordination with Federal agencies with responsibilities
26 under the National Response Plan, develops pre-scripted mission assign-
27 ments, including logistics, communications, mass care, health services, and
28 public safety.

29 (d) CERTIFICATION.—The President shall certify to the Committee on
30 Homeland Security and Governmental Affairs of the Senate and the Com-
31 mittee on Homeland Security and the Committee on Transportation and In-
32 frastructure of the House of Representatives on an annual basis that each
33 Federal agency with responsibilities under the National Response Plan com-
34 plies with subsections (a) and (b).

35 (e) CONSTRUCTION.—Nothing in this section shall be construed to limit
36 the authority of the Secretary of Defense with regard to—

37 (1) the command, control, training, planning, equipment, exercises,
38 or employment of Department of Defense forces; or

39 (2) the allocation of Department of Defense resources.

1 **§ 20514. Use of existing resources**

2 In establishing the national preparedness goal and national preparedness
3 system, the Administrator shall use existing preparedness documents, plan-
4 ning tools, and guidelines to the extent practicable and consistent with this
5 subtitle.

6 **Subchapter II—Additional Preparedness**

7 **§ 20521. Emergency Management Assistance Compact grants**

8 (a) IN GENERAL.—The Administrator may make grants to administer the
9 Emergency Management Assistance Compact consented to by the Joint Res-
10 olution entitled “Joint Resolution granting the consent of Congress to the
11 Emergency Management Assistance Compact” (Public Law 104–321, 110
12 Stat. 3877).

13 (b) USES.—A grant under this section shall be used—

14 (1) to carry out recommendations identified in the Emergency Man-
15 agement Assistance Compact after-action reports for the 2004 and
16 2005 hurricane seasons;

17 (2) to administer compact operations on behalf of all member States
18 and territories;

19 (3) to continue coordination with the Agency and appropriate Fed-
20 eral agencies;

21 (4) to continue coordination with State, local, and tribal government
22 entities and their respective national organizations; and

23 (5) to assist State and local governments, emergency response pro-
24 viders, and organizations representing the providers with credentialing
25 emergency response providers and the typing of emergency response re-
26 sources.

27 (c) COORDINATION.—The Administrator shall consult with the Adminis-
28 trator of the Emergency Management Assistance Compact to ensure effec-
29 tive coordination of efforts in responding to requests for assistance.

30 (d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be ap-
31 propriated to carry out this section \$4,000,000 for fiscal year 2022, to re-
32 main available until expended.

33 **§ 20522. Emergency Management Performance Grants Pro-**
34 **gram**

35 (a) DEFINITIONS.—In this section:

36 (1) PROGRAM.—The term “program” means the emergency manage-
37 ment performance grants program described in subsection (b).

38 (2) STATE.—The term “State” has the meaning given that term in
39 section 102 of the Robert T. Stafford Disaster Relief and Emergency
40 Assistance Act (42 U.S.C. 5122).

1 (b) IN GENERAL.—The Administrator shall continue implementation of
2 an emergency management performance grants program to make grants to
3 States to assist State, local, and tribal governments in preparing for all haz-
4 ards, as authorized by the Robert T. Stafford Disaster Relief and Emer-
5 gency Assistance Act (42 U.S.C. 5121 et seq.).

6 (c) FEDERAL SHARE.—Except as otherwise specifically provided by title
7 VI of the Robert T. Stafford Disaster Relief and Emergency Assistance Act
8 (42 U.S.C. 5195 et seq.), the Federal share of the cost of an activity carried
9 out using funds made available under the program shall not exceed 50 per-
10 cent.

11 (d) APPORTIONMENT.—The Administrator shall apportion the amounts
12 appropriated each fiscal year to carry out the program among the States
13 as follows:

14 (1) The Administrator shall first apportion 0.25 percent of the
15 amounts to each of American Samoa, the Northern Mariana Islands,
16 Guam, and the Virgin Islands and 0.75 percent of the amounts to each
17 of the remaining States.

18 (2) The Administrator shall apportion the remainder of the amounts
19 in the ratio that the population of each State bears to the population
20 of all States.

21 (e) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be ap-
22 propriated to carry out the program \$950,000,000 for fiscal year 2022.

23 **§ 20523. Training for emergency response providers from**
24 **Federal Government, foreign governments, or pri-**
25 **vate entities**

26 (a) IN GENERAL.—The Center for Domestic Preparedness may provide
27 training to emergency response providers from the Federal Government, for-
28 eign governments, or private entities if the Center for Domestic Prepared-
29 ness is reimbursed for the cost of the training. Any reimbursement under
30 this subsection shall be credited to the account from which the expenditure
31 being reimbursed was made and is available, without fiscal year limitation,
32 for the purposes for which amounts in the account may be expended.

33 (b) TRAINING NOT TO INTERFERE WITH PRIMARY MISSION.—The head
34 of the Center for Domestic Preparedness shall ensure that any training pro-
35 vided under subsection (a) does not interfere with the primary mission of
36 the Center for Domestic Preparedness to train State and local emergency
37 response providers.

38 (c) TRAINING FEDERAL EMERGENCY MANAGEMENT AGENCY EMPLOY-
39 EES.—Subject to subsection (b), subsection (a) does not prohibit the Center
40 for Domestic Preparedness from providing training to employees of the
41 Agency in existing chemical, biological, radiological, nuclear, explosives,

1 mass casualty, and medical surge courses pursuant to 5 U.S.C. 4103 with-
2 out reimbursement for the cost of the training.

3 **§ 20524. National exercise simulation center**

4 The President shall establish a national exercise simulation center that—

5 (1) uses a mix of live, virtual, and constructive simulations to—

6 (A) prepare elected officials, emergency managers, emergency
7 response providers, and emergency support providers at all levels
8 of government to operate cohesively;

9 (B) provide a learning environment for the homeland security
10 personnel of all Federal agencies;

11 (C) assist in the development of operational procedures and ex-
12 ercises, particularly those based on catastrophic incidents; and

13 (D) allow incident commanders to exercise decision-making in a
14 simulated environment; and

15 (2) uses modeling and simulation for training, exercises, and com-
16 mand and control functions at the operational level.

17 **§ 20525. Real property transactions**

18 (a) APPLICATION.—This section applies only to real property in the
19 States, the District of Columbia, and Puerto Rico. It does not apply to real
20 property for river and harbor projects or flood control projects, or to leases
21 of Government-owned real property for agricultural or grazing purposes.

22 (b) REPORTS TO ARMED SERVICES COMMITTEES BEFORE TRANSACTION
23 MAY BE ENTERED INTO.—

24 (1) TRANSACTIONS THAT MAY NOT BE ENTERED INTO BEFORE EXPI-
25 RATION OF PERIOD AFTER REPORT IS SUBMITTED.—The Director of
26 the Office of Civil and Defense Mobilization, or the designee of the Di-
27 rector, may not enter into any of the following listed transactions by
28 or for the use of the Office until after the expiration of 30 days from
29 the date on which a report of the facts concerning the proposed trans-
30 action is submitted to the Committees on Armed Services of the Senate
31 and House of Representatives:

32 (A) An acquisition of fee title to any real property, if the esti-
33 mated price is more than \$50,000.

34 (B) A lease of real property to the United States, if the esti-
35 mated annual rental is more than \$50,000.

36 (C) A lease of real property owned by the United States, if the
37 estimated annual rental is more than \$50,000.

38 (D) A transfer of real property owned by the United States to
39 another Federal agency or to a State, if the estimated value is
40 more than \$50,000.

1 (E) A transfer of excess real property owned by the United
2 States to a disposal agency, if the estimated value is more than
3 \$50,000.

4 (2) SUMMARY OF GENERAL PLAN REQUIRED FOR CERTAIN TRANS-
5 ACTIONS.—If a transaction covered by clause (A) or (B) of paragraph
6 (1) is part of a project, the report must include a summarization of
7 the general plan for that project, including an estimate of the total cost
8 of the lands to be acquired or leases to be made.

9 (c) ANNUAL REPORTS TO ARMED SERVICES COMMITTEES.—The Director
10 of the Office of Civil and Defense Mobilization shall report annually to the
11 Committees on Armed Services of the Senate and the House of Representa-
12 tives on transactions described in subsection (a) that involve an estimated
13 value of more than \$5,000 but not more than \$50,000.

14 (d) STATEMENT OF COMPLIANCE IS CONCLUSIVE.—A statement in an in-
15 strument of conveyance, including a lease, that the requirements of this sec-
16 tion have been met, or that the conveyance is not subject to this section,
17 is conclusive.

18 **Subchapter III—Miscellaneous Authorities** 19 **§ 20531. National Disaster Recovery Strategy**

20 (a) IN GENERAL.—The Administrator, in coordination with the Secretary
21 of Housing and Urban Development, the Administrator of the Environ-
22 mental Protection Agency, the Secretary of Agriculture, the Secretary of
23 Commerce, the Secretary of the Treasury, the Secretary of Transportation,
24 the Administrator of the Small Business Administration, the Assistant Sec-
25 retary for Indian Affairs of the Department of the Interior, and the heads
26 of other appropriate Federal agencies, State, local, and tribal government
27 officials (including through the National Advisory Council), and representa-
28 tives of appropriate nongovernmental organizations, shall develop, coordi-
29 nate, and maintain a National Disaster Recovery Strategy to serve as a
30 guide to recovery efforts after major disasters and emergencies.

31 (b) CONTENTS.—The National Disaster Recovery Strategy shall—

32 (1) outline the most efficient and cost-effective Federal programs
33 that will meet the recovery needs of States, local and tribal govern-
34 ments, and individuals and households affected by a major disaster;

35 (2) clearly define the role, programs, authorities, and responsibilities
36 of each Federal agency that may be of assistance in providing assist-
37 ance in the recovery from a major disaster;

38 (3) promote the use of the most appropriate and cost-effective build-
39 ing materials (based on the hazards present in an area) in an area af-
40 fected by a major disaster, with the goal of encouraging the construc-
41 tion of disaster-resistant buildings; and

- 1 (4) describe in detail the programs that may be offered by the agen-
2 cies described in paragraph (2), including—
3 (A) discussing funding issues;
4 (B) detailing how responsibilities under the National Disaster
5 Recovery Strategy will be shared; and
6 (C) addressing other matters concerning the cooperative effort
7 to provide recovery assistance.

8 (c) REPORT.—

9 (1) IN GENERAL.—The Administrator shall submit to the appro-
10 priate committees of Congress a report describing in detail the Na-
11 tional Disaster Recovery Strategy and any additional authorities nec-
12 cessary to implement any portion of the National Disaster Recovery
13 Strategy.

14 (2) UPDATE.—The Administrator shall submit to the appropriate
15 committees of Congress a report updating the report submitted under
16 paragraph (1)—

17 (A) on the same date that any change is made to the National
18 Disaster Recovery Strategy; and

19 (B) on a periodic basis after the submission of the report under
20 paragraph (1), but not less than once every 5 years after the date
21 of the submission.

22 **§ 20532. National Disaster Housing Strategy**

23 (a) IN GENERAL.—The Administrator, in coordination with representa-
24 tives of the Federal agencies, governments, and organizations listed in sub-
25 section (b)(2), the National Advisory Council, the National Council on Dis-
26 ability, and other entities at the Administrator's discretion, shall develop,
27 coordinate, and maintain a National Disaster Housing Strategy.

28 (b) CONTENTS.—The National Disaster Housing Strategy shall—

29 (1) outline the most efficient and cost-effective Federal programs
30 that will best meet the short-term and long-term housing needs of indi-
31 viduals and households affected by a major disaster;

32 (2) clearly define the role, programs, authorities, and responsibilities
33 of each entity in providing housing assistance in the event of a major
34 disaster, including—

35 (A) the Agency;

36 (B) the Department of Housing and Urban Development;

37 (C) the Department of Agriculture;

38 (D) the Department of Veterans Affairs;

39 (E) the Department of Health and Human Services;

40 (F) the Bureau of Indian Affairs;

1 (G) any other Federal agency that may provide housing assist-
2 ance in the event of a major disaster;

3 (H) the American Red Cross; and

4 (I) State, local, and tribal governments;

5 (3) describe in detail the programs that may be offered by the enti-
6 ties described in paragraph (2), including—

7 (A) outlining any funding issues;

8 (B) detailing how responsibilities under the National Disaster
9 Housing Strategy will be shared; and

10 (C) addressing other matters concerning the cooperative effort
11 to provide housing assistance during a major disaster;

12 (4) consider methods through which housing assistance can be pro-
13 vided to individuals and households where employment and other re-
14 sources for living are available;

15 (5) describe programs directed to meet the needs of special-needs
16 and low-income populations and ensure that a sufficient number of
17 housing units are provided for individuals with disabilities;

18 (6) describe plans for the operation of clusters of housing provided
19 to individuals and households, including access to public services, site
20 management, security, and site density;

21 (7) describe plans for promoting the repair or rehabilitation of exist-
22 ing rental housing, including through lease agreements or other means,
23 in order to improve the provision of housing to individuals and house-
24 holds under section 408 of the Robert T. Stafford Disaster Relief and
25 Emergency Assistance Act (42 U.S.C. 5174); and

26 (8) describe any additional authorities necessary to carry out any
27 portion of the strategy.

28 (e) GUIDANCE.—The Administrator should develop and make publicly
29 available guidance on—

30 (1) types of housing assistance available under the Robert T. Staf-
31 ford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121
32 et seq.) to individuals and households affected by an emergency or
33 major disaster;

34 (2) eligibility for assistance (including, where appropriate, the con-
35 tinuation of assistance); and

36 (3) application procedures for assistance.

37 (d) REPORT.—

38 (1) IN GENERAL.—The Administrator shall submit to the appro-
39 priate committees of Congress a report describing in detail the Na-
40 tional Disaster Housing Strategy, including programs directed to meet-
41 ing the needs of populations with special needs.

1 (2) UPDATE.—The Administrator shall submit to the appropriate
2 committees of Congress a report updating the report submitted under
3 paragraph (1)—

4 (A) on the same date that any change is made to the National
5 Disaster Housing Strategy; and

6 (B) on a periodic basis after the submission of the report under
7 paragraph (1), but not less than once every 5 years after the date
8 of the submission.

9 **§ 20533. Individuals with disabilities guidelines**

10 The Administrator, in coordination with the National Advisory Council,
11 the National Council on Disability, the Interagency Coordinating Council on
12 Emergency Preparedness and Individuals With Disabilities established
13 under Executive Order No. 13347 (69 Fed. Reg. 44573), and the Disability
14 Coordinator (established under section 11313 of this title), shall develop
15 guidelines to accommodate individuals with disabilities, which shall include
16 guidelines for—

17 (1) the accessibility of, and communications and programs in, shel-
18 ters, recovery centers, and other facilities; and

19 (2) devices used in connection with disaster operations, including
20 first aid stations, mass feeding areas, portable payphone stations, port-
21 able toilets, and temporary housing.

22 **§ 20534. Reunification**

23 (a) DEFINITIONS.—In this section:

24 (1) CHILD LOCATOR CENTER.—The term “Child Locator Center”
25 means the National Emergency Child Locator Center established under
26 subsection (b).

27 (2) DECLARED EVENT.—The term “declared event” means a major
28 disaster or emergency.

29 (3) DISPLACED ADULT.—The term “displaced adult” means an indi-
30 vidual 21 years of age or older who is displaced from the habitual resi-
31 dence of that individual as a result of a declared event.

32 (4) DISPLACED CHILD.—The term “displaced child” means an indi-
33 vidual under 21 years of age who is displaced from the habitual resi-
34 dence of that individual as a result of a declared event.

35 (b) NATIONAL EMERGENCY CHILD LOCATOR CENTER.—

36 (1) IN GENERAL.—The Administrator, in coordination with the At-
37 torney General of the United States, shall establish in the National
38 Center for Missing and Exploited Children the National Emergency
39 Child Locator Center. In establishing the Child Locator Center, the
40 Administrator shall establish procedures to make all relevant informa-
41 tion available to the Child Locator Center in a timely manner to facili-

1 tate the expeditious identification and reunification of children with
2 their families.

3 (2) PURPOSES.—The purposes of the Child Locator Center are to—

4 (A) enable individuals to provide to the Child Locator Center
5 the name of, and other identifying information about, a displaced
6 child or a displaced adult who may have information about the lo-
7 cation of a displaced child;

8 (B) enable individuals to receive information about other
9 sources of information about displaced children and displaced
10 adults; and

11 (C) assist law enforcement in locating displaced children.

12 (3) RESPONSIBILITIES AND DUTIES.—The responsibilities and duties
13 of the Child Locator Center are to—

14 (A) establish a toll-free telephone number to receive reports of
15 displaced children and information about displaced adults that
16 may assist in locating displaced children;

17 (B) create a website to provide information about displaced chil-
18 dren;

19 (C) deploy its staff to the location of a declared event to gather
20 information about displaced children;

21 (D) assist in the reunification of displaced children with their
22 families;

23 (E) provide information to the public about additional resources
24 for disaster assistance;

25 (F) work in partnership with Federal, State, and local law en-
26 forcement agencies;

27 (G) provide technical assistance in locating displaced children;

28 (H) share information on displaced children and displaced
29 adults with governmental agencies and nongovernmental organiza-
30 tions providing disaster assistance;

31 (I) use its resources to gather information about displaced chil-
32 dren;

33 (J) refer reports of displaced adults to—

34 (i) an entity designated by the Attorney General to provide
35 technical assistance in locating displaced adults; and

36 (ii) the National Emergency Family Registry and Locator
37 System established under section 20535(b) of this title;

38 (K) enter into cooperative agreements with Federal and State agen-
39 cies and other organizations such as the American Red Cross as nec-
40 essary to implement the mission of the Child Locator Center; and

1 (L) develop an emergency response plan to prepare for the activation
2 of the Child Locator Center.

3 **§ 20535. National Emergency Family Registry and Locator**
4 **System**

5 (a) DEFINITION OF DISPLACED INDIVIDUAL.—In this section, the term
6 “displaced individual” means an individual displaced by an emergency or
7 major disaster.

8 (b) ESTABLISHMENT.—The Administrator shall establish a National
9 Emergency Family Registry and Locator System to help reunify families
10 separated after an emergency or major disaster.

11 (c) OPERATION.—The National Emergency Family Registry and Locator
12 System shall—

13 (1) allow a displaced adult (including a medical patient) to volun-
14 tarily register (and allow an adult who is the parent or guardian of a
15 displaced child to register the child), by submitting personal informa-
16 tion to be entered into a database (such as the name, current location
17 of residence, and any other relevant information that could be used by
18 others seeking to locate that individual);

19 (2) ensure that information submitted under paragraph (1) is acces-
20 sible to those individuals named by a displaced individual and to law
21 enforcement officials;

22 (3) be accessible through the Internet and through a toll-free num-
23 ber, to receive reports of displaced individuals; and

24 (4) include a means of referring displaced children to the National
25 Emergency Child Locator Center established under section 20534(b) of
26 this title.

27 (d) INFORMING THE PUBLIC.—The Administrator shall establish a mech-
28 anism to inform the public about the National Emergency Family Registry
29 and Locator System and its potential to assist in reunifying displaced indi-
30 viduals with their families.

31 (e) COORDINATION.—The Administrator shall enter into a memorandum
32 of understanding with the Department of Justice, the National Center for
33 Missing and Exploited Children, the Department of Health and Human
34 Services, and the American Red Cross and other relevant private organiza-
35 tions that will enhance the sharing of information to facilitate reunifying
36 displaced individuals (including medical patients) with their families.

37 **Chapter 207—Prevention of Fraud, Waste,**
38 **and Abuse**

Sec.

20701. Advance contracting.

20702. Oversight and accountability of Federal disaster expenditures.

20703. Limitation on length of certain noncompetitive contracts.

20704. Fraud, waste, and abuse controls.
20705. Registry of disaster response contractors.
20706. Fraud prevention training program.

1 **§ 20701. Advance contracting**

2 (a) ENTERING INTO CONTRACTS.—

3 (1) IN GENERAL.—The Administrator shall enter into 1 or more con-
4 tracts for recurring disaster response requirements, including specific
5 goods and services, for which the Agency is capable of contracting in
6 advance of a natural disaster or act of terrorism or other man-made
7 disaster in a cost-effective manner, using a contracting strategy that
8 maximizes the use of advance contracts to the extent practical and
9 cost-effective. A previously awarded contract for goods or services may
10 be maintained in fulfilling this requirement.

11 (2) CONSIDERED FACTORS.—Before entering into any contract under
12 this subsection, the Administrator shall consider section 307 of the
13 Robert T. Stafford Disaster Relief and Emergency Assistance Act (42
14 U.S.C. 5150).

15 (3) PRE-NEGOTIATED FEDERAL CONTRACTS FOR GOODS AND SERV-
16 ICES.—The Administrator, in coordination with State and local govern-
17 ments and other Federal agencies, shall establish a process to ensure
18 that Federal pre-negotiated contracts for goods and services are coordi-
19 nated with State and local governments, as appropriate.

20 (4) PRE-NEGOTIATED STATE AND LOCAL CONTRACTS FOR GOODS
21 AND SERVICES.—The Administrator shall encourage State and local
22 governments to establish pre-negotiated contracts with vendors for
23 goods and services in advance of natural disasters and acts of terrorism
24 or other man-made disasters.

25 (b) MAINTENANCE OF CONTRACTS.—The Administrator is responsible for
26 maintaining contracts for appropriate levels of goods and services in accord-
27 ance with a contracting strategy that maximizes the use of advance con-
28 tracts to the extent practical and cost-effective.

29 (c) REPORT ON CONTRACTS NOT USING COMPETITIVE PROCEDURES.—
30 At the end of each fiscal quarter, the Administrator shall submit a report
31 on each disaster assistance contract entered into by the Agency by other
32 than competitive procedures to the appropriate committees of Congress.

33 (d) UPDATED REPORT.—Not later than 180 days after December 31,
34 2020, the Administrator shall submit to the appropriate committees of Con-
35 gress an updated report that contains—

36 (1) the information required in the initial report under subpara-
37 graphs (A) and (B) of subsection (a)(1) of section 691 of the Post-

1 Katrina Emergency Reform Act of 2006 (Public Law 109–295, 120
2 Stat. 1457); and

3 (2) an updated strategy described in section 691(a)(1)(C) of the Act
4 that clearly defines—

5 (A) the objectives of advance contracts;

6 (B) how advance contracts contribute to disaster response oper-
7 ations of the Agency;

8 (C) how to maximize the award of advance contracts to small
9 business concerns, as defined in section 3 of the Small Business
10 Act (15 U.S.C. 632); and

11 (D) whether and how advance contracts should be prioritized in
12 relation to new post-disaster contract awards.

13 (e) ADDITIONAL DUTIES OF ADMINISTRATOR.—

14 (1) ENSURE THAT HEAD OF CONTRACTING ACTIVITY CARRIES OUT
15 CERTAIN DUTIES.—The Administrator shall ensure that the head of
16 contracting activity of the Agency—

17 (A) not later than 270 days after December 31, 2020, updates
18 the Disaster Contracting Desk Guide of the Agency to provide spe-
19 cific guidance—

20 (i) on whether and under what circumstances contracting
21 officers should consider using existing advance contracts en-
22 tered into in accordance with this section prior to making new
23 post-disaster contract awards, and include this guidance in
24 existing semi-annual training given to contracting officers;
25 and

26 (ii) for contracting officers to perform outreach to State
27 and local governments on the potential benefits of estab-
28 lishing their own pre-negotiated advance contracts;

29 (B) adheres to hard copy contract file management require-
30 ments in effect to ensure that the files relating to advance con-
31 tracts entered into in accordance with this section are complete
32 and up to date, whether the files will be transferred into the Elec-
33 tronic Contract Filing System of the Agency or remain in hard
34 copy format;

35 (C) notifies contracting officers of the 3-day time frame require-
36 ment for entering completed award documentation into the con-
37 tract writing system of the Agency when executing notice-to-pro-
38 ceed documentation;

39 (D) not later than 180 days after December 31, 2020, revises
40 the reporting methodology of the Agency to ensure that all dis-
41 aster contracts are included in each quarterly report submitted to

1 the appropriate congressional committees under this section on
2 disaster contract actions;

3 (E) identifies a single centralized resource listing advance con-
4 tracts entered into under this section and ensures that source is
5 current and up to date and includes all available advance con-
6 tracts; and

7 (F) communicates complete and up-to-date information on avail-
8 able advance contracts to State and local governments to inform
9 their advance contracting efforts.

10 (2) UPDATE AND IMPLEMENT GUIDANCE.—Not later than 180 days
11 after December 31, 2020, the Administrator shall update and imple-
12 ment guidance for program office and acquisition personnel of the
13 Agency to—

14 (A) identify acquisition planning time frames and considerations
15 across the entire acquisition planning process of the Agency; and

16 (B) clearly communicate the purpose and use of a master acqui-
17 sition planning schedule.

18 **§ 20702. Oversight and accountability of Federal disaster ex-**
19 **penditures**

20 (a) DEFINITION OF OVERSIGHT FUNDS.—In this section, the term “over-
21 sight funds” means funds referred to in subsection (b) that are designated
22 for use in performing oversight activities.

23 (b) AUTHORITY OF ADMINISTRATOR TO DESIGNATE FUNDS FOR OVER-
24 SIGHT ACTIVITIES.—The Administrator may designate up to 1 percent of
25 the total amount provided to a Federal agency for a mission assignment as
26 oversight funds to be used by the recipient agency for performing oversight
27 of activities carried out under the Agency reimbursable mission assignment
28 process. The funds are available until expended.

29 (c) USE OF FUNDS.—

30 (1) TYPES OF OVERSIGHT ACTIVITIES.—Oversight funds may be
31 used for the following types of oversight activities related to Agency
32 mission assignments:

33 (A) Monitoring, tracking, and auditing expenditures of funds.

34 (B) Ensuring that sufficient management and internal control
35 mechanisms are available so that Agency funds are spent appro-
36 priately and in accordance with all applicable laws and regulations.

37 (C) Reviewing selected contracts and other activities.

38 (D) Investigating allegations of fraud involving Agency funds.

39 (E) Conducting and participating in fraud prevention activities
40 with other Federal, State, and local government personnel and
41 contractors.

1 (2) PLANS AND REPORTS.—Oversight funds may be used to issue the
2 plans required under subsection (f) and the reports required under sub-
3 section (g).

4 (d) RESTRICTION ON USE OF FUNDS.—Oversight funds may not be used
5 to finance existing agency oversight responsibilities related to direct agency
6 appropriations used for disaster response, relief, and recovery activities.

7 (e) METHODS OF OVERSIGHT ACTIVITIES.—

8 (1) IN GENERAL.—Oversight activities may be carried out by an
9 agency under this section either directly or by contract. The activities
10 may include evaluations and financial and performance audits.

11 (2) COORDINATION OF OVERSIGHT ACTIVITIES.—To the extent prac-
12 ticable, evaluations and audits under this section shall be performed by
13 the inspector general of the agency.

14 (f) DEVELOPMENT OF OVERSIGHT PLANS.—

15 (1) IN GENERAL.—If an agency receives oversight funds for a fiscal
16 year, the head of the agency shall prepare a plan describing the over-
17 sight activities for disaster response, relief, and recovery anticipated to
18 be undertaken during the subsequent fiscal year.

19 (2) SELECTION OF OVERSIGHT ACTIVITIES.—In preparing the plan,
20 the head of the agency shall select oversight activities based upon a
21 risk assessment of those areas that present the greatest risk of fraud,
22 waste, and abuse.

23 (3) SCHEDULE.—The plan shall include a schedule for conducting
24 oversight activities, including anticipated dates of completion.

25 (g) FEDERAL DISASTER ASSISTANCE ACCOUNTABILITY REPORTS.—An
26 agency receiving oversight funds under this section shall submit annually to
27 the Administrator and the appropriate committees of Congress a consoli-
28 dated report regarding the use of the funds, including information summa-
29 rizing oversight activities and the results achieved.

30 **§ 20703. Limitation on length of certain noncompetitive con-**
31 **tracts**

32 (a) COVERED CONTRACTS.—This section applies to any contract in an
33 amount greater than the simplified acquisition threshold (as defined by sec-
34 tion 134 of title 41) entered into by the Department to facilitate response
35 to or recovery from a natural disaster, act of terrorism, or other man-made
36 disaster.

37 (b) REGULATIONS.—The Secretary shall promulgate regulations applica-
38 ble to contracts described in subsection (a) to restrict the contract period
39 of a contract entered into using procedures other than competitive proce-
40 dures pursuant to the exception provided in section 3304(a)(2) of title 41
41 to the minimum contract period necessary—

1 (1) to meet the urgent and compelling requirements of the work to
2 be performed under the contract; and

3 (2) to enter into another contract for the required goods or services
4 through the use of competitive procedures.

5 (c) SPECIFIC CONTRACT PERIOD.—The regulations promulgated under
6 subsection (b) shall require the contract period to not exceed 150 days, un-
7 less the Secretary determines that exceptional circumstances apply.

8 **§ 20704. Fraud, waste, and abuse controls**

9 (a) IN GENERAL.—The Administrator shall ensure that—

10 (1) all programs in the Agency administering Federal disaster relief
11 assistance develop and maintain proper internal management controls
12 to prevent and detect fraud, waste, and abuse;

13 (2) application databases used by the Agency to collect information
14 on eligible recipients must record disbursements;

15 (3) tracking to prevent and detect fraud, waste, and abuse is de-
16 signed to highlight and identify ineligible applications; and

17 (4) the databases used to collect information from applications for
18 assistance are integrated with disbursements and payment records.

19 (b) AUDITS AND REVIEWS REQUIRED.—The Administrator shall ensure
20 that any database or similar application processing system for Federal dis-
21 aster relief assistance programs administered by the Agency undergoes a re-
22 view by the Inspector General of the Department to determine the existence
23 and implementation of internal controls required under this section and sec-
24 tion 408(i) of the Robert T. Stafford Disaster Relief and Emergency Assist-
25 ance Act (42 U.S.C. 5174(i)).

26 **§ 20705. Registry of disaster response contractors**

27 (a) DEFINITIONS.—In this section, the terms “small business concern”,
28 “small business concern owned and controlled by service-disabled veterans”,
29 “small business concern owned and controlled by socially and economically
30 disadvantaged individuals”, and “small business concern owned and con-
31 trolled by women” have the meanings given the terms under the Small Busi-
32 ness Act (15 U.S.C. 631 et seq.).

33 (b) REGISTRY.—

34 (1) IN GENERAL.—The Administrator shall establish and maintain
35 a registry of contractors who are willing to perform debris removal, dis-
36 tribution of supplies, reconstruction, and other disaster or emergency
37 relief activities.

38 (2) CONTENTS.—The registry shall include, for each business con-
39 cern—

40 (A) the name of the business concern;

41 (B) the location of the business concern;

- 1 (C) the area served by the business concern;
- 2 (D) the type of good or service provided by the business con-
- 3 cern;
- 4 (E) the bonding level of the business concern; and
- 5 (F) whether the business concern is—
- 6 (i) a small business concern;
- 7 (ii) a small business concern owned and controlled by so-
- 8 cially and economically disadvantaged individuals;
- 9 (iii) a small business concern owned and controlled by
- 10 women; or
- 11 (iv) a small business concern owned and controlled by serv-
- 12 ice-disabled veterans.

13 (3) SOURCE OF INFORMATION.—

14 (A) SUBMISSION.—Information maintained in the registry shall
15 be submitted on a voluntary basis and be kept current by the sub-
16 mitting business concerns.

17 (B) ATTESTATION.—Each business concern submitting informa-
18 tion to the registry shall submit—

- 19 (i) an attestation that the information is true; and
- 20 (ii) documentation supporting the attestation.

21 (C) VERIFICATION.—The Administrator shall verify that the
22 documentation submitted by each business concern supports the
23 information submitted by that business concern.

24 (4) AVAILABILITY.—The registry shall be made generally available
25 on the website of the Agency.

26 (5) CONSULTATION OF REGISTRY AS PART OF ACQUISITION PLAN-
27 NING.—A Federal agency shall consult the registry as part of the ac-
28 quisition planning for contracting for debris removal, distribution of
29 supplies in a disaster, reconstruction, and other disaster or emergency
30 relief activities.

31 **§ 20706. Fraud prevention training program**

32 The Administrator shall develop and implement a program to provide
33 training on the prevention of waste, fraud, and abuse of Federal disaster
34 relief assistance relating to the response to or recovery from natural disas-
35 ters and acts of terrorism or other man-made disasters and ways to identify
36 potential waste, fraud, and abuse.

37 **Subtitle III—Port Security and**
 38 **Accountability**
 39 **Chapter 301—General**

Sec.
30101. Definitions.

1 **§ 30101. Definitions**

2 In this subtitle:

3 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—Except as other-
4 wise provided, the term “appropriate congressional committees”
5 means—

6 (A) the Committee on Appropriations of the Senate;

7 (B) the Committee on Commerce, Science, and Transportation
8 of the Senate;

9 (C) the Committee on Finance of the Senate;

10 (D) the Committee on Homeland Security and Governmental
11 Affairs of the Senate;

12 (E) the Committee on Appropriations of the House of Rep-
13 resentatives;

14 (F) the Committee on Homeland Security of the House of Rep-
15 resentatives;

16 (G) the Committee on Transportation and Infrastructure of the
17 House of Representatives;

18 (H) the Committee on Ways and Means of the House of Rep-
19 resentatives; and

20 (I) other congressional committees, as appropriate.

21 (2) COMMERCIAL CUSTOMS OPERATIONS ADVISORY COMMITTEE.—
22 The term “Commercial Customs Operations Advisory Committee”
23 means the Advisory Committee established under section 109 of the
24 Trade Facilitation and Trade Enforcement Act of 2015 (19 U.S.C.
25 4316) or any successor committee.

26 (3) COMMERCIAL SEAPORT PERSONNEL.—The term “commercial
27 seaport personnel” includes any person engaged in an activity relating
28 to the loading or unloading of cargo or passengers, the movement or
29 tracking of cargo, the maintenance and repair of intermodal equipment,
30 the operation of cargo-related equipment (whether or not integral to
31 the vessel), and the handling of mooring lines on the dock when a ves-
32 sel is made fast or let go in the United States.

33 (4) COMMISSIONER.—The term “Commissioner” means the Commis-
34 sioner responsible for U.S. Customs and Border Protection.

35 (5) CONTAINER.—The term “container” has the meaning given the
36 term in the International Convention for Safe Containers, with an-
37 nexes, done at Geneva, December 2, 1972 (29 UST 3707).

38 (6) CONTAINER SECURITY DEVICE.—The term “container security
39 device” means a device, or system—

40 (A) designed, at a minimum—

41 (i) to identify positively a container;

1 (ii) to detect and record unauthorized intrusion into a con-
2 tainer; and

3 (iii) to secure a container against tampering throughout
4 the supply chain; and

5 (B) that has a low false alarm rate, as determined by the Sec-
6 retary.

7 (7) DEPARTMENT.—The term “Department” means the Department
8 of Homeland Security.

9 (8) EXAMINATION.—The term “examination” means an inspection of
10 cargo to detect the presence of mis-declared, restricted, or prohibited
11 items that utilizes nonintrusive imaging and detection technology.

12 (9) INSPECTION.—The term “inspection” means the comprehensive
13 process used by U.S. Customs and Border Protection—

14 (A) to assess goods entering the United States to appraise them
15 for duty purposes, to detect the presence of restricted or prohib-
16 ited items, and to ensure compliance with all applicable laws; and

17 (B) that may include screening, conducting an examination, or
18 conducting a search.

19 (10) INTERNATIONAL SUPPLY CHAIN.—The term “international sup-
20 ply chain” means the end-to-end process for shipping goods to or from
21 the United States beginning at the point of origin (including manufac-
22 turer, supplier, or vendor) through a point of distribution to the des-
23 tination.

24 (11) RADIATION DETECTION EQUIPMENT.—The term “radiation de-
25 tection equipment” means any technology that is capable of detecting
26 or identifying nuclear and radiological material or nuclear and radio-
27 logical explosive devices.

28 (12) SCAN.—The term “scan” means utilizing nonintrusive imaging
29 equipment, radiation detection equipment, or both, to capture data, in-
30 cluding images of a container.

31 (13) SCREENING.—The term “screening” means a visual or auto-
32 mated review of information about goods, including manifest or entry
33 documentation accompanying a shipment being imported into the
34 United States, to determine the presence of mis-declared, restricted, or
35 prohibited items and assess the level of threat posed by the affected
36 cargo.

37 (14) SEARCH.—The term “search” means an intrusive examination
38 in which a container is opened and its contents are devanned and vis-
39 ually inspected for the presence of mis-declared, restricted, or prohib-
40 ited items.

1 (15) SECRETARY.—The term “Secretary” means the Secretary of
2 Homeland Security.

3 (16) TRANSPORTATION DISRUPTION.—The term “transportation dis-
4 ruption” means any significant delay, interruption, or stoppage in the
5 flow of trade caused by a natural disaster, heightened threat level, act
6 of terrorism, or transportation security incident.

7 (17) TRANSPORTATION SECURITY INCIDENT.—The term “transportation
8 security incident” has the meaning given the term in section
9 70101(6) of title 46.

10 **Chapter 303—Security of United States** 11 **Seaports**

Sec.

30301. Port Security Exercise Program.

30302. Facility exercise requirements.

30303. Domestic radiation detection and imaging.

30304. Integration of detection equipment and technologies.

30305. Random searches of containers.

30306. Threat assessment screening of port truck drivers.

30307. Center of Excellence for Maritime Domain Awareness.

12 **§ 30301. Port Security Exercise Program**

13 (a) IN GENERAL.—The Secretary, acting through the Administrator of
14 the Federal Emergency Management Agency and in coordination with the
15 Commandant of the Coast Guard, shall establish a Port Security Exercise
16 Program (in this section referred to as the “Exercise Program”) to test and
17 evaluate the capabilities of Federal, State, local, and foreign governments,
18 commercial seaport personnel and management, governmental and non-
19 governmental emergency response providers, the private sector, or any other
20 organization or entity, as the Secretary determines to be appropriate, to
21 prevent, prepare for, mitigate against, respond to, and recover from acts of
22 terrorism, natural disasters, and other emergencies at facilities required to
23 submit a plan under section 70103(e) of title 46.

24 (b) REQUIREMENTS.—The Secretary shall ensure that the Exercise Pro-
25 gram—

26 (1) conducts, on a periodic basis, port security exercises at the facili-
27 ties that are—

28 (A) sealed and tailored to the needs of each facility;

29 (B) live, in the case of the most at-risk facilities;

30 (C) as realistic as practicable and based on current risk assess-
31 ments, including credible threats, vulnerabilities, and con-
32 sequences;

33 (D) consistent with the National Incident Management System,
34 the National Response Plan, the National Infrastructure Protec-
35 tion Plan, the National Preparedness Guidance, the National Pre-

1 paredness Goal, the National Maritime Transportation Security
2 Plan, and other national initiatives;

3 (E) evaluated against clear and consistent performance meas-
4 ures;

5 (F) assessed to learn best practices, which shall be shared with
6 appropriate Federal, State, and local officials, commercial seaport
7 personnel and management, governmental and nongovernmental
8 emergency response providers, and the private sector; and

9 (G) followed by remedial action in response to lessons learned;
10 and

11 (2) assists State and local governments and facilities in designing,
12 implementing, and evaluating exercises that—

13 (A) conform to the requirements of paragraph (1); and

14 (B) are consistent with any applicable Area Maritime Transpor-
15 tation Security Plan and State or Urban Area Homeland Security
16 Plan.

17 (c) IMPROVEMENT PLAN.—The Secretary shall establish a port security
18 exercise improvement plan process to—

19 (1) identify and analyze each port security exercise for lessons
20 learned and best practices;

21 (2) disseminate lessons learned and best practices to participants in
22 the Exercise Program;

23 (3) monitor the implementation of lessons learned and best practices
24 by participants in the Exercise Program; and

25 (4) conduct remedial action tracking and long-term trend analysis.

26 **§ 30302. Facility exercise requirements**

27 The Secretary of the Department in which the Coast Guard is operating
28 shall require each high-risk facility to conduct live or full-scale exercises de-
29 scribed in section 105.220(c) of title 33, Code of Federal Regulations, not
30 less frequently than once every 2 years, in accordance with the facility secu-
31 rity plan required under section 70103(c) of title 46.

32 **§ 30303. Domestic radiation detection and imaging**

33 (a) SCANNING CONTAINERS.—Subject to section 318 of the Tariff Act of
34 1930 (19 U.S.C. 1318), all containers entering the United States through
35 the 22 ports through which the greatest volume of containers enter the
36 United States by vessel shall be scanned for radiation. To the extent prac-
37 ticable, the Secretary shall deploy next-generation radiation detection tech-
38 nology.

39 (b) STRATEGY.—The Secretary shall develop and implement a strategy
40 for the deployment of radiation detection capabilities that includes—

1 (1) a risk-based prioritization of ports of entry at which radiation
2 detection equipment will be deployed;

3 (2) a proposed timeline of when radiation detection equipment will
4 be deployed at each port of entry identified under paragraph (1);

5 (3) the type of equipment to be used at each port of entry identified
6 under paragraph (1), including the joint deployment and utilization of
7 radiation detection equipment and nonintrusive imaging equipment;

8 (4) standard operating procedures for examining containers with the
9 equipment, including sensor alarming, networking, and communications
10 and response protocols;

11 (5) operator training plans;

12 (6) an evaluation of the environmental health and safety impacts of
13 nonintrusive imaging technology and a radiation risk reduction plan, in
14 consultation with the Nuclear Regulatory Commission, the Occupa-
15 tional Safety and Health Administration, and the National Institute for
16 Occupational Safety and Health, that seeks to minimize radiation expo-
17 sure of workers and the public to levels as low as reasonably achievable;

18 (7) the policy of the Department for using nonintrusive imaging
19 equipment in tandem with radiation detection equipment; and

20 (8) a classified annex that—

21 (A) details plans for covert testing; and

22 (B) outlines the risk-based prioritization of ports of entry iden-
23 tified under paragraph (1).

24 (c) EXPANSION TO OTHER UNITED STATES PORTS OF ENTRY.—

25 (1) IN GENERAL.—The Secretary shall expand the strategy devel-
26 oped under subsection (b), in a manner consistent with the require-
27 ments of subsection (b), to provide for the deployment of radiation de-
28 tection capabilities at all other United States ports of entry not covered
29 by the strategy developed under subsection (b).

30 (2) RISK ASSESSMENT.—In expanding the strategy under paragraph
31 (1), the Secretary shall identify and assess the risks to those other
32 ports of entry in order to determine what equipment and practices will
33 best mitigate the risks.

34 (d) STANDARDS.—The Secretary, acting through the Assistant Secretary
35 for the Countering Weapons of Mass Destruction Office and in collaboration
36 with the National Institute of Standards and Technology, shall publish tech-
37 nical capability standards and recommended standard operating procedures
38 for the use of nonintrusive imaging and radiation detection equipment in
39 the United States. The standards and procedures—

1 (1) should take into account relevant standards and procedures uti-
2 lized by other Federal departments or agencies as well as those devel-
3 oped by international bodies; and

4 (2) shall not be designed so as to endorse specific companies or cre-
5 ate sovereignty conflicts with participating countries.

6 (e) INTERMODAL RAIL RADIATION DETECTION TEST CENTER.—

7 (1) ESTABLISHMENT.—In accordance with subsection (b), and to
8 comply with this section, the Secretary shall establish an Intermodal
9 Rail Radiation Detection Test Center (in this subsection referred to as
10 the “Test Center”).

11 (2) PROJECTS.—The Secretary shall conduct multiple, concurrent
12 projects at the Test Center to rapidly identify and test concepts specific
13 to the challenges posed by on-dock rail.

14 (3) LOCATION.—The Test Center shall be located in a public port
15 facility at which a majority of the containerized cargo is directly laden
16 from (or unladen to) on-dock, intermodal rail.

17 **§ 30304. Integration of detection equipment and tech-**
18 **nologies**

19 The Secretary is responsible for ensuring that domestic chemical, biologi-
20 cal, radiological, and nuclear detection equipment and technologies are inte-
21 grated, as appropriate, with other border security systems and detection
22 technologies.

23 **§ 30305. Random searches of containers**

24 The Secretary, acting through the Commissioner, shall develop and imple-
25 ment a plan, utilizing best practices for empirical scientific research design
26 and random sampling, to conduct random searches of containers in addition
27 to any targeted or pre-shipment inspection of the containers required by law
28 or regulation or conducted under any other program conducted by the Sec-
29 retary. Nothing in this section shall be construed to mean that implementa-
30 tion of the random sampling plan precludes additional searches of con-
31 tainers not inspected pursuant to the plan.

32 **§ 30306. Threat assessment screening of port truck drivers**

33 The Secretary shall implement a threat assessment screening, including
34 name-based checks against terrorist watch lists and immigration status
35 checks, for all port truck drivers with access to secure areas of a port who
36 have a commercial driver’s license but do not have a current and valid haz-
37 ardous materials endorsement issued under part 1572 of title 49, Code of
38 Federal Regulations, that is the same as the threat assessment screening
39 required for facility employees and longshoremen by the Commandant of the
40 Coast Guard under Coast Guard Notice USCG-2006-24189 (71 Fed. Reg.
41 25066).

1 **§ 30307. Center of Excellence for Maritime Domain Aware-**
 2 **ness**

3 (a) ESTABLISHMENT.—The Secretary shall establish a university-based
 4 Center for Excellence for Maritime Domain Awareness following the merit-
 5 review processes and procedures that have been established by the Secretary
 6 for selecting university program centers of excellence.

7 (b) DUTIES.—The Center established under subsection (a) shall—

8 (1) prioritize its activities based on the “National Plan To Improve
 9 Maritime Domain Awareness” published by the Department in October
 10 2005;

11 (2) recognize the extensive previous and ongoing work and existing
 12 competence in the field of maritime domain awareness at numerous
 13 academic and research institutions, such as the Naval Postgraduate
 14 School;

15 (3) leverage existing knowledge and continue development of a broad
 16 base of expertise in academia and industry in maritime domain aware-
 17 ness; and

18 (4) provide educational, technical, and analytical assistance to Fed-
 19 eral agencies with responsibilities for maritime domain awareness, in-
 20 cluding the Coast Guard, to focus on the need for interoperability, in-
 21 formation sharing, and common information technology standards and
 22 architecture.

23 **Chapter 305—Security of the International**
 24 **Supply Chain**

Subchapter I—General

Sec.

30501. Strategic plan to enhance the security of the international supply chain.

30502. Post-incident resumption of trade.

30503. Automated targeting system.

30504. Container security standards and procedures.

30505. Container Security Initiative.

30506. Avoiding duplication of effort and identifying security gaps.

Subchapter II—Customs—Trade Partnership Against Terrorism

30521. Establishment.

30522. Eligible entities.

30523. Minimum requirements.

30524. Tier 1 participants.

30525. Tier 2 participants.

30526. Tier 3 participants.

30527. Consequences for lack of compliance.

30528. Revalidation.

30529. Noncontainerized cargo.

30530. Program management.

Subchapter III—Miscellaneous Provisions

30541. Screening and scanning of cargo containers.

30542. Provision of assistance, equipment, and training.

30543. Information sharing relating to supply chain security cooperation.

Subchapter I—General

§ 30501. Strategic plan to enhance the security of the international supply chain

(a) STRATEGIC PLAN.—The Secretary, in consultation with appropriate Federal, State, local, and tribal government agencies and private-sector stakeholders responsible for security matters that affect or relate to the movement of containers through the international supply chain, shall develop, implement, and update, triennially, a strategic plan to enhance the security of the international supply chain.

(b) REQUIREMENTS.—The strategic plan required under subsection (a) shall—

(1) describe the roles, responsibilities, and authorities of Federal, State, local, and tribal government agencies and private-sector stakeholders that relate to the security of the movement of containers through the international supply chain;

(2) identify and address gaps and unnecessary overlaps in the roles, responsibilities, or authorities described in paragraph (1);

(3) identify and make recommendations regarding legislative, regulatory, and organizational changes necessary to improve coordination among the entities or to enhance the security of the international supply chain;

(4) provide measurable goals, including objectives, mechanisms, and a schedule, for furthering the security of commercial operations from point of origin to point of destination;

(5) build on available resources and consider costs and benefits;

(6) provide incentives for additional voluntary measures to enhance cargo security, as recommended by the Commissioner;

(7) consider the impact of supply chain security requirements on small- and medium-sized companies;

(8) include a process for sharing intelligence and information with private-sector stakeholders to assist in their security efforts;

(9) identify a framework for prudent and measured response in the event of a transportation security incident involving the international supply chain;

(10) provide protocols for the expeditious resumption of the flow of trade under section 30502 of this title;

(11) consider the linkages between supply chain security and security programs in other systems of movement, including travel security and terrorism finance programs; and

1 (12) expand on and relate to existing strategies and plans, including
2 the National Response Plan, the National Maritime Transportation Se-
3 curity Plan, the National Strategy for Maritime Security, and the 8
4 supporting plans of the Strategy, as required by Homeland Security
5 Presidential Directive–13.

6 (e) CONSULTATION.—In developing protocols under subsection (b)(10),
7 the Secretary shall consult with Federal, State, local, and private-sector
8 stakeholders, including the National Maritime Security Advisory Committee
9 and the Commercial Operations Advisory Committee.

10 (d) COMMUNICATION.—To the extent practicable, the strategic plan devel-
11 oped under subsection (a) shall provide for coordination with, and lines of
12 communication among, appropriate Federal, State, local, and private-sector
13 stakeholders on law enforcement actions, intermodal rerouting plans, and
14 other strategic infrastructure issues resulting from a transportation security
15 incident or transportation disruption.

16 (e) UTILIZATION OF ADVISORY COMMITTEES.—As part of the consulta-
17 tions described in subsection (a), the Secretary shall, to the extent prac-
18 ticable, utilize the Homeland Security Advisory Committee, the National
19 Maritime Security Advisory Committee, and the Commercial Operations Ad-
20 visory Committee to review, as necessary, the strategic plan and any subse-
21 quent updates to the strategic plan.

22 (f) INTERNATIONAL STANDARDS AND PRACTICES.—In furtherance of the
23 strategic plan required under subsection (a), the Secretary is encouraged to
24 consider proposed or established standards and practices of foreign govern-
25 ments and international organizations, including the International Maritime
26 Organization, the World Customs Organization, the International Labor Or-
27 ganization, and the International Organization for Standardization, as ap-
28 propriate, to establish standards and best practices for the security of con-
29 tainers moving through the international supply chain.

30 (g) UPDATE REPORTS.—Not later than 270 days after October 5, 2018,
31 and triennially thereafter, the Secretary shall submit to the appropriate con-
32 gressional committees a report that contains updates to the strategic plan
33 submitted under subsection (a) since the prior report.

34 **§ 30502. Post-incident resumption of trade**

35 (a) IN GENERAL.—The Secretary shall develop and update, as necessary,
36 protocols for the resumption of trade under section 30501(b)(10) of this
37 title in the event of a transportation disruption or a transportation security
38 incident. The protocols shall include—

39 (1) the identification of the appropriate initial incident commander,
40 if the Commandant of the Coast Guard is not the appropriate indi-

1 vidual, and lead departments, agencies, or offices to execute the proto-
2 cols;

3 (2) a plan to redeploy resources and personnel, as necessary, to rees-
4 tablish the flow of trade;

5 (3) a plan to provide training for the periodic instruction of per-
6 sonnel of U.S. Customs and Border Protection, the Coast Guard, and
7 the Transportation Security Administration in trade resumption func-
8 tions and responsibilities; and

9 (4) appropriate factors for establishing prioritization of vessels and
10 cargo determined by the President to be critical for response and recov-
11 ery, including factors relating to public health, national security, and
12 economic need.

13 (b) VESSELS.—In determining the prioritization of vessels accessing fa-
14 cilities (as defined under section 70101 of title 46), the Commandant of the
15 Coast Guard may, to the extent practicable and consistent with the proto-
16 cols and plans required under this section to ensure the safe and secure
17 transit of vessels to ports in the United States after a transportation secu-
18 rity incident, give priority to a vessel—

19 (1) that has an approved security plan under section 70103(c) of
20 title 46, or a valid international ship security certificate, as provided
21 under part 104 of title 33, Code of Federal Regulations;

22 (2) that is manned by individuals who are described in section
23 70105(b)(2)(B) of title 46; and

24 (3) that is operated by validated participants in the Customs–Trade
25 Partnership Against Terrorism (in this chapter referred to as “C–
26 TPAT”) program.

27 (c) CARGO.—In determining the prioritization of the resumption of the
28 flow of cargo and consistent with the protocols established under this sec-
29 tion, the Commissioner may give preference to cargo—

30 (1) entering a port of entry directly from a foreign seaport des-
31 ignated under the Container Security Initiative;

32 (2) from the supply chain of a validated C–TPAT participant and
33 other private-sector entities, as appropriate; or

34 (3) that has undergone—

35 (A) a nuclear or radiological detection scan;

36 (B) an x-ray, density, or other imaging scan; and

37 (C) a system to positively identify the container at the last port
38 of departure prior to arrival in the United States, which data has
39 been evaluated and analyzed by personnel of U.S. Customs and
40 Border Protection.

1 (d) COORDINATION.—The Secretary shall ensure that there is appropriate
2 coordination among the Commandant of the Coast Guard, the Commis-
3 sioner, and other Federal officials following a maritime disruption or mari-
4 time transportation security incident in order to provide for the resumption
5 of trade.

6 (e) COMMUNICATION.—Consistent with section 30501 of this title, the
7 Commandant of the Coast Guard, the Commissioner, and other appropriate
8 Federal officials shall promptly communicate any revised procedures or in-
9 structions intended for the private sector following a maritime disruption or
10 maritime transportation security incident.

11 **§ 30503. Automated targeting system**

12 (a) IN GENERAL.—The Secretary, acting through the Commissioner,
13 shall—

14 (1) identify and seek the submission of data related to the movement
15 of a shipment of cargo through the international supply chain; and

16 (2) analyze the data described in paragraph (1) to identify high-risk
17 cargo for inspection.

18 (b) REQUIREMENT.—The Secretary, acting through the Commissioner,
19 shall require the electronic transmission to the Department of additional
20 data elements for improved high-risk targeting, including appropriate secu-
21 rity elements of entry data, as determined by the Secretary, to be provided
22 as advanced information with respect to cargo destined for importation into
23 the United States prior to loading of the cargo on vessels at foreign sea-
24 ports.

25 (c) CONSIDERATION.—The Secretary, acting through the Commissioner,
26 shall—

27 (1) consider the cost, benefit, and feasibility of—

28 (A) requiring additional non-manifest documentation;

29 (B) reducing the time period allowed by law for revisions to a
30 container cargo manifest;

31 (C) reducing the time period allowed by law for submission of
32 certain elements of entry data, for vessel or cargo; and

33 (D) taking other actions the Secretary considers beneficial for
34 improving the information relied on for the Automated Targeting
35 System and any successor targeting system in furthering the secu-
36 rity and integrity of the international supply chain; and

37 (2) consult with stakeholders, including the Commercial Operations
38 Advisory Committee, and identify to them the need for the information
39 referred to in paragraph (1)(D), and the appropriate timing of its sub-
40 mission.

1 (d) REGULATIONS.—The Secretary shall promulgate regulations to carry
2 out this section. In promulgating regulations, the Secretary shall adhere to
3 the parameters applicable to the development of regulations under section
4 343(a) of the Customs Border Security Act of 2002 (19 U.S.C. 1415(a)),
5 including provisions relating to consultation, technology, analysis, use of in-
6 formation, confidentiality, and timing requirements.

7 (e) SYSTEM IMPROVEMENTS.—The Secretary, acting through the Com-
8 missioner, shall—

9 (1) conduct, through an independent panel, a review of the effective-
10 ness and capabilities of the Automated Targeting System;

11 (2) consider future iterations of the Automated Targeting System,
12 which would incorporate smart features, such as more complex algo-
13 rithms and real-time intelligence, instead of relying solely on rule sets
14 that are periodically updated;

15 (3) ensure that the Automated Targeting System has the capability
16 to electronically compare manifest and other available data for cargo
17 entered into or bound for the United States to detect any significant
18 anomalies between the data and facilitate the resolution of the anoma-
19 lies;

20 (4) ensure that the Automated Targeting System has the capability
21 to electronically identify, compile, and compare select data elements for
22 cargo entered into or bound for the United States following a maritime
23 transportation security incident, in order to efficiently identify cargo
24 for increased inspection or expeditious release; and

25 (5) develop a schedule to address the recommendations of the Comp-
26 troller General, the Inspector General of the Department of the Treas-
27 ury, and the Inspector General of the Department with respect to the
28 operation of the Automated Targeting System.

29 (f) SECURE TRANSMISSION OF CERTAIN INFORMATION.—All information
30 required by the Department from supply chain partners shall be transmitted
31 in a secure fashion, as determined by the Secretary, so as to protect the
32 information from unauthorized access.

33 **§ 30504. Container security standards and procedures**

34 (a) ESTABLISHMENT.—

35 (1) IN GENERAL.—The Secretary shall initiate a rulemaking pro-
36 ceeding to establish minimum standards and procedures for securing
37 containers in transit to the United States.

38 (2) DEADLINE FOR ENFORCEMENT.—

39 (A) ENFORCEMENT OF RULE.—Not later than 2 years after the
40 date on which the standards and procedures are established under

1 paragraph (1), all containers bound for ports of entry in the
2 United States shall meet the standards and procedures.

3 (B) INTERIM REQUIREMENT.—If an interim final rule issued
4 pursuant to the proceeding described in paragraph (1) was not
5 issued by April 1, 2008—

6 (i) all containers in transit to the United States are re-
7 quired to meet the requirements of the International Organi-
8 zation for Standardization Publicly Available Specification
9 17712 standard for sealing containers; and

10 (ii) the requirements of this subparagraph cease to be ef-
11 fective on the effective date of the interim final rule issued
12 under this subsection.

13 (b) REVIEW AND ENHANCEMENT.—The Secretary shall regularly review
14 and enhance the standards and procedures established under subsection (a),
15 as appropriate, based on tests of technologies as they become commercially
16 available to detect container intrusion and the highest consequence threats,
17 particularly weapons of mass destruction.

18 (c) INTERNATIONAL CARGO SECURITY STANDARDS.—The Secretary, in
19 consultation with the Secretary of State, the Secretary of Energy, and other
20 Federal Government officials, as appropriate, and with the Commercial Op-
21 erations Advisory Committee, the Homeland Security Advisory Committee,
22 and the National Maritime Security Advisory Committee, is encouraged to
23 promote and establish international standards for the security of containers
24 moving through the international supply chain with foreign governments
25 and international organizations, including the International Maritime Orga-
26 nization, the International Organization for Standardization, the Inter-
27 national Labor Organization, and the World Customs Organization.

28 (d) INTERNATIONAL TRADE AND OTHER OBLIGATIONS.—In carrying out
29 this section, the Secretary shall consult with appropriate Federal depart-
30 ments and agencies and private-sector stakeholders and ensure that actions
31 under this section do not violate international trade obligations or other
32 international obligations of the United States.

33 **§ 30505. Container Security Initiative**

34 (a) ESTABLISHMENT.—The Secretary, acting through the Commissioner,
35 shall establish and implement a program (in this section referred to as the
36 “Container Security Initiative”) to identify and examine or search maritime
37 containers that pose a security risk before loading the containers in a for-
38 eign port for shipment to the United States, either directly or through a
39 foreign port.

40 (b) ASSESSMENT.—The Secretary, acting through the Commissioner, may
41 designate foreign seaports to participate in the Container Security Initiative

1 after the Secretary has assessed the costs, benefits, and other factors associ-
2 ated with the designation, including—

3 (1) the level of risk for the potential compromise of containers by
4 terrorists, or other threats as determined by the Secretary;

5 (2) the volume of cargo being imported to the United States directly
6 from, or being trans-shipped through, the foreign seaport;

7 (3) the results of the Coast Guard assessments conducted under sec-
8 tion 70108 of title 46;

9 (4) the commitment of the government of the country in which the
10 foreign seaport is located to cooperate with the Department in sharing
11 critical data and risk management information and to maintain pro-
12 grams to ensure employee integrity; and

13 (5) the potential for validation of security practices at the foreign
14 seaport by the Department.

15 (e) NOTIFICATION.—The Secretary shall notify the appropriate congres-
16 sional committees of the designation of a foreign port under the Container
17 Security Initiative or the revocation of a designation before notifying the
18 public of the designation or revocation.

19 (d) NEGOTIATIONS.—The Secretary, in cooperation with the Secretary of
20 State and in consultation with the United States Trade Representative, may
21 enter into negotiations with the government of each foreign nation in which
22 a seaport is designated under the Container Security Initiative to ensure full
23 compliance with the requirements under the Container Security Initiative.

24 (e) OVERSEAS INSPECTIONS.—

25 (1) REQUIREMENTS AND PROCEDURES.—The Secretary shall—

26 (A) establish minimum technical capability criteria and standard
27 operating procedures for the use of nonintrusive inspection and
28 nuclear and radiological detection systems in conjunction with the
29 Container Security Initiative;

30 (B) require each port designated under the Container Security
31 Initiative to operate nonintrusive inspection and nuclear and radio-
32 logical detection systems in accordance with the technical capa-
33 bility criteria and standard operating procedures established under
34 subparagraph (A);

35 (C) continually monitor the technologies, processes, and tech-
36 niques used to inspect cargo at ports designated under the Con-
37 tainer Security Initiative to ensure adherence to the criteria and
38 the use of the procedures; and

39 (D) consult with the Secretary of Energy in establishing the
40 minimum technical capability criteria and standard operating pro-
41 cedures established under subparagraph (A) pertaining to radi-

1 ation detection technologies to promote consistency in detection
2 systems at foreign ports designated under the Container Security
3 Initiative.

4 (2) CONSTRAINTS.—The criteria and procedures established under
5 paragraph (1)(A)—

6 (A) shall be consistent, as practicable, with relevant standards
7 and procedures utilized by other Federal departments or agencies,
8 or developed by international bodies if the United States consents
9 to the standards and procedures;

10 (B) shall not apply to activities conducted under the Megaports
11 Initiative of the Department of Energy; and

12 (C) shall not be designed to endorse the product or technology
13 of any specific company or to conflict with the sovereignty of a
14 country in which a foreign seaport designated under the Container
15 Security Initiative is located.

16 (f) SAVINGS PROVISION.—The authority of the Secretary under this sec-
17 tion shall not affect any authority or duplicate any efforts or responsibilities
18 of the Federal Government with respect to the deployment of radiation de-
19 tection equipment outside of the United States.

20 (g) COORDINATION.—The Secretary shall—

21 (1) coordinate with the Secretary of Energy, as necessary, to provide
22 radiation detection equipment required to support the Container Secu-
23 rity Initiative through the Department of Energy’s Second Line of De-
24 fense Program and Megaports Initiative; or

25 (2) work with the private sector or host governments, when possible,
26 to obtain radiation detection equipment that meets the Department’s
27 and the Department of Energy’s technical specifications for the equip-
28 ment.

29 (h) STAFFING.—The Secretary shall develop a human capital manage-
30 ment plan to determine adequate staffing levels in the United States and
31 in foreign seaports including, as appropriate, the remote location of per-
32 sonnel in countries in which foreign seaports are designated under the Con-
33 tainer Security Initiative.

34 (i) ANNUAL DISCUSSIONS.—The Secretary, in coordination with the ap-
35 propriate Federal officials, shall hold annual discussions with foreign gov-
36 ernments of countries in which foreign seaports designated under the Con-
37 tainer Security Initiative are located regarding best practices, technical as-
38 sistance, training needs, and technological developments that will assist in
39 ensuring the efficient and secure movement of international cargo.

40 (j) LESSER RISK PORT.—The Secretary, acting through the Commis-
41 sioner, may treat cargo loaded in a foreign seaport designated under the

1 Container Security Initiative as presenting a lesser risk than similar cargo
2 loaded in a foreign seaport that is not designated under the Container Secu-
3 rity Initiative, for the purpose of clearing the cargo into the United States.

4 (k) PROHIBITION.—

5 (1) IN GENERAL.—The Secretary shall issue a “do not load” order,
6 using existing authorities, to prevent the onload of any cargo loaded
7 at a port designated under the Container Security Initiative that has
8 been identified as high risk, including by the Automated Targeting Sys-
9 tem, unless the cargo is determined to no longer be high risk
10 through—

11 (A) a scan of the cargo with nonintrusive imaging equipment
12 and radiation detection equipment;

13 (B) a search of the cargo; or

14 (C) additional information received by the Department.

15 (2) RULE OF CONSTRUCTION.—Nothing in this subsection shall be
16 construed to interfere with the ability of the Secretary to deny entry
17 of any cargo into the United States.

18 (l) REPORT.—Not later than 270 days after October 5, 2018, the Sec-
19 retary, acting through the Commissioner, shall, in consultation with other
20 appropriate government officials and the Commercial Operations Advisory
21 Committee, submit a report to the appropriate congressional committees on
22 the effectiveness of, and the need for any improvements to, the Container
23 Security Initiative. The report shall include—

24 (1) a description of the technical assistance delivered to, as well as
25 needed at, each designated seaport;

26 (2) a description of the human capital management plan at each des-
27 ignated seaport;

28 (3) a summary of the requests made by the United States to foreign
29 governments to conduct physical or nonintrusive inspections of cargo
30 at designated seaports, and whether each request was granted or de-
31 nied by the foreign government;

32 (4) an assessment of the effectiveness of screening, scanning, and in-
33 spection protocols and technologies utilized at designated seaports and
34 the effect on the flow of commerce at the seaports, as well as any rec-
35 ommendations for improving the effectiveness of screening, scanning,
36 and inspection protocols and technologies utilized at designated sea-
37 ports;

38 (5) a description and assessment of the outcome of any security inci-
39 dent involving a foreign seaport designated under the Container Secu-
40 rity Initiative;

1 (6) the rationale for the continuance of each port designated under
2 the Consumer Security Initiative;

3 (7) a description of the potential for remote targeting to decrease the
4 number of personnel who are deployed at foreign ports under the Con-
5 sumer Security Initiative; and

6 (8) a summary and assessment of the aggregate number and extent
7 of trade compliance lapses at each seaport designated under the Con-
8 tainer Security Initiative.

9 (m) COORDINATION OF ASSESSMENTS.—

10 (1) IN GENERAL.—The Secretary shall, to the extent practicable,
11 conduct the assessments required by the following provisions of law
12 concurrently, or develop a process by which the assessments are coordi-
13 nated between the Coast Guard and U.S. Customs and Border Protec-
14 tion:

15 (A) This section.

16 (B) Section 30523 of this title.

17 (C) Section 70108 of title 46.

18 (2) LIMITATION.—Nothing in paragraph (1) shall be construed to af-
19 fect or diminish the Secretary's authority or discretion—

20 (A) to conduct an assessment of a foreign port at any time;

21 (B) to compel the Secretary to conduct an assessment of a for-
22 eign port so as to ensure that 2 or more assessments are con-
23 ducted concurrently; or

24 (C) to cancel an assessment of a foreign port if the Secretary
25 is unable to conduct 2 or more assessments concurrently.

26 (3) MULTIPLE ASSESSMENT REPORT.—The Secretary shall provide
27 written notice to the Committee on Commerce, Science, and Transpor-
28 tation of the Senate and the Committee on Transportation and Infra-
29 structure and the Committee on Homeland Security of the House of
30 Representatives when the Secretary conducts 2 or more assessments of
31 the same port within a 3-year period.

32 **§ 30506. Avoiding duplication of effort and identifying secu-**
33 **rity gaps**

34 The Secretary shall—

35 (1) provide the Administrator with updates to vulnerability assess-
36 ments required under section 70102(b)(3) of title 46 to avoid duplica-
37 tion of effort between the Coast Guard and the Transportation Security
38 Administration; and

39 (2) identify security gaps between authorities of operating entities in
40 the Department that a threat could exploit to cause a transportation
41 security incident (as defined in section 70101 of title 46).

1 **Subchapter II—Customs–Trade**
2 **Partnership Against Terrorism**

3 **§ 30521. Establishment**

4 (a) IN GENERAL.—The Secretary, acting through the Commissioner, may
5 establish a voluntary government-private-sector program (to be known as
6 the “Customs-Trade Partnership Against Terrorism” or “C-TPAT”) to
7 strengthen and improve the overall security of the international supply chain
8 and United States border security, and to facilitate the movement of secure
9 cargo through the international supply chain, by providing benefits to par-
10 ticipants meeting or exceeding the program requirements. Participants in
11 C-TPAT shall include Tier 1 participants, Tier 2 participants, and Tier 3
12 participants.

13 (b) REVIEW OF MINIMUM SECURITY REQUIREMENTS.—The Secretary,
14 acting through the Commissioner, shall review the minimum security re-
15 quirements of C-TPAT at least once every year and update requirements
16 as necessary.

17 **§ 30522. Eligible entities**

18 Importers, customs brokers, forwarders, air, sea, and land carriers, con-
19 tract logistics providers, and other entities in the international supply chain
20 and intermodal transportation system are eligible to apply to voluntarily
21 enter into partnerships with the Department under C-TPAT.

22 **§ 30523. Minimum requirements**

23 An applicant seeking to participate in C-TPAT shall—

24 (1) demonstrate a history of moving cargo in the international sup-
25 ply chain;

26 (2) conduct an assessment of its supply chain based upon security
27 criteria established by the Secretary, acting through the Commissioner,
28 including—

29 (A) business partner requirements;

30 (B) container security;

31 (C) physical security and access controls;

32 (D) personnel security;

33 (E) procedural security;

34 (F) security training and threat awareness; and

35 (G) information technology security;

36 (3) implement and maintain security measures and supply chain se-
37 curity practices meeting security criteria established by the Commis-
38 sioner; and

39 (4) meet all other requirements established by the Commissioner, in
40 consultation with the Commercial Operations Advisory Committee.

1 **§ 30524. Tier 1 participants**

2 (a) BENEFITS.—The Secretary, acting through the Commissioner, shall
3 offer limited benefits to a Tier 1 participant who has been certified in ac-
4 cordance with the guidelines referred to in subsection (b). Benefits may in-
5 clude a reduction in the score assigned pursuant to the Automated Tar-
6 geting System of not greater than 20 percent of the high-risk threshold es-
7 tablished by the Secretary.

8 (b) GUIDELINES.—The Secretary, acting through the Commissioner, shall
9 update the guidelines for certifying a C-TPAT participant's security meas-
10 ures and supply chain security practices under this section. The guidelines
11 shall include a background investigation and extensive documentation re-
12 view.

13 (c) TIME FRAME.—To the extent practicable, the Secretary, acting
14 through the Commissioner, shall complete the Tier 1 certification process
15 within 90 days of receipt of an application for participation in C-TPAT.

16 **§ 30525. Tier 2 participants**

17 (a) VALIDATION.—The Secretary, acting through the Commissioner, shall
18 validate the security measures and supply chain security practices of a Tier
19 1 participant in accordance with the guidelines referred to in subsection (c).
20 The validation shall include on-site assessments at appropriate foreign loca-
21 tions utilized by the Tier 1 participant in its supply chain and shall, to the
22 extent practicable, be completed not later than 1 year after certification as
23 a Tier 1 participant.

24 (b) BENEFITS.—The Secretary, acting through the Commissioner, shall
25 extend benefits to each C-TPAT participant that has been validated as a
26 Tier 2 participant under this section, which may include—

- 27 (1) reduced scores in the Automated Targeting System;
28 (2) reduced examinations of cargo; and
29 (3) priority searches of cargo.

30 (c) GUIDELINES.—The Secretary, acting through the Commissioner, shall
31 develop a schedule and update the guidelines for validating a participant's
32 security measures and supply chain security practices under this section.

33 **§ 30526. Tier 3 participants**

34 (a) IN GENERAL.—The Secretary, acting through the Commissioner, shall
35 establish a third tier of C-TPAT participation that offers additional bene-
36 fits to participants who demonstrate a sustained commitment to maintain-
37 ing security measures and supply chain security practices that exceed the
38 guidelines established for validation as a Tier 2 participant in C-TPAT
39 under section 30525 of this title.

1 (b) CRITERIA.—The Secretary, acting through the Commissioner, shall
2 designate criteria for validating a C-TPAT participant as a Tier 3 partici-
3 pant under this section. Criteria may include—

4 (1) compliance with any additional guidelines established by the Sec-
5 retary that exceed the guidelines established under section 30525 of
6 this title for validating a C-TPAT participant as a Tier 2 participant,
7 particularly with respect to controls over access to cargo throughout
8 the supply chain;

9 (2) submission of additional information regarding cargo prior to
10 loading, as determined by the Secretary;

11 (3) utilization of container security devices, technologies, policies, or
12 practices that meet standards and criteria established by the Secretary;
13 and

14 (4) compliance with any other cargo requirements established by the
15 Secretary.

16 (c) BENEFITS.—The Secretary, acting through the Commissioner, in con-
17 sultation with the Commercial Operations Advisory Committee and the Na-
18 tional Maritime Security Advisory Committee, shall extend benefits to each
19 C-TPAT participant that has been validated as a Tier 3 participant under
20 this section, which may include—

21 (1) the expedited release of a Tier 3 participant's cargo in destina-
22 tion ports within the United States during all threat levels designated
23 by the Secretary;

24 (2) further reduction in examinations of cargo;

25 (3) priority for examinations of cargo; and

26 (4) further reduction in the risk score assigned pursuant to the
27 Automated Targeting System; and

28 (5) inclusion in joint incident management exercises, as appropriate.

29 **§ 30527. Consequences for lack of compliance**

30 (a) IN GENERAL.—If at any time a C-TPAT participant's security meas-
31 ures and supply chain security practices fail to meet any of the require-
32 ments under this subchapter, the Commissioner may deny the participant
33 benefits otherwise available under this subchapter in whole or in part. The
34 Commissioner shall develop procedures that provide appropriate protections
35 to C-TPAT participants before benefits are revoked. The procedures may
36 not limit the ability of the Commissioner to take actions to protect the na-
37 tional security of the United States.

38 (b) FALSE OR MISLEADING INFORMATION.—If a C-TPAT participant
39 knowingly provides false or misleading information to the Commissioner
40 during the validation process provided for under this subchapter, the Com-
41 missioner shall suspend or expel the participant from C-TPAT for an ap-

1 appropriate period of time. The Commissioner, after the completion of the
2 process under subsection (c), may publish in the Federal Register a list of
3 participants who have been suspended or expelled from C-TPAT under this
4 subsection, and may make the list available to C-TPAT participants.

5 (c) RIGHT OF APPEAL.—

6 (1) APPEAL OF DENIAL OF BENEFITS.—A C-TPAT participant may
7 appeal a decision of the Commissioner under subsection (a). The appeal
8 shall be filed with the Secretary not later than 90 days after the date
9 of the decision, and the Secretary shall issue a determination not later
10 than 180 days after the appeal is filed.

11 (2) APPEAL OF SUSPENSION OR EXPULSION.—A C-TPAT partici-
12 pant may appeal a decision of the Commissioner under subsection (b).
13 The appeal shall be filed with the Secretary not later than 30 days
14 after the date of the decision, and the Secretary shall issue a deter-
15 mination not later than 180 days after the appeal is filed.

16 **§ 30528. Revalidation**

17 The Secretary, acting through the Commissioner, shall develop and imple-
18 ment—

19 (1) a revalidation process for Tier 2 and Tier 3 participants;

20 (2) a framework based upon objective criteria for identifying partici-
21 pants for periodic revalidation not less frequently than once during
22 each 4-year period following the initial validation; and

23 (3) an annual plan for revalidation that includes—

24 (A) performance measures;

25 (B) an assessment of the personnel needed to perform the re-
26 validations; and

27 (C) the number of participants that will be revalidated during
28 the following year.

29 **§ 30529. Noncontainerized cargo**

30 The Secretary, acting through the Commissioner, shall consider the po-
31 tential for participation in C-TPAT by importers of noncontainerized car-
32 goes that otherwise meet the requirements under this subchapter.

33 **§ 30530. Program management**

34 (a) IN GENERAL.—The Secretary, acting through the Commissioner, shall
35 establish sufficient internal quality controls and record management to sup-
36 port the management systems of C-TPAT. In managing the program, the
37 Secretary shall ensure that the program includes the following:

38 (1) A 5-year plan to identify outcome-based goals and performance
39 measures of the program.

40 (2) An annual plan for each fiscal year designed to match available
41 resources to the projected workload.

1 (3) A standardized work program to be used by agency personnel to
2 carry out the certifications, validations, and revalidations of partici-
3 pants. The Secretary shall keep records and monitor staff hours associ-
4 ated with the completion of each review.

5 (b) DOCUMENTATION OF REVIEWS.—The Secretary, acting through the
6 Commissioner, shall maintain a record management system to document de-
7 terminations on the reviews of each C-TPAT participant, including certifi-
8 cations, validations, and revalidations.

9 (c) CONFIDENTIAL INFORMATION SAFEGUARDS.—In consultation with
10 the Commercial Operations Advisory Committee, the Secretary, acting
11 through the Commissioner, shall develop and implement procedures to en-
12 sure the protection of confidential data collected, stored, or shared with gov-
13 ernment agencies or as part of the application, certification, validation, and
14 revalidation processes.

15 (d) RESOURCE MANAGEMENT STAFFING PLAN.—The Secretary, acting
16 through the Commissioner, shall—

17 (1) develop a staffing plan to recruit and train staff (including a for-
18 malized training program) to meet the objectives identified in the stra-
19 tegic plan of the C-TPAT program; and

20 (2) provide cross-training in post-incident trade resumption for per-
21 sonnel who administer the C-TPAT program.

22 (e) REPORT TO CONGRESS.—In connection with the President's annual
23 budget submission for the Department, the Secretary shall report to the ap-
24 propriate congressional committees on the progress made by the Commis-
25 sioner to certify, validate, and revalidate C-TPAT participants. The report
26 shall be due on the same date that the President's budget is submitted to
27 the Congress.

28 **Subchapter III—Miscellaneous Provisions**

29 **§ 30541. Screening and scanning of cargo containers**

30 (a) ONE HUNDRED PERCENT SCREENING OF CARGO CONTAINERS AND
31 100 PERCENT SCANNING OF HIGH-RISK CONTAINERS.—

32 (1) SCREENING OF CARGO CONTAINERS.—The Secretary shall ensure
33 that 100 percent of the cargo containers originating outside the United
34 States and unloaded at a United States seaport undergo a screening
35 to identify high-risk containers

36 (2) SCANNING OF HIGH-RISK CONTAINERS.—The Secretary shall en-
37 sure that 100 percent of the containers that have been identified as
38 high-risk under paragraph (1), or through other means, are scanned
39 or searched before the containers leave a United States seaport facility.

40 (b) FULL-SCALE IMPLEMENTATION.—

1 (1) IN GENERAL.—A container that was loaded on a vessel in a for-
2 eign port shall not enter the United States (either directly or via a for-
3 eign port) unless the container was scanned by nonintrusive imaging
4 equipment and radiation detection equipment at a foreign port before
5 it was loaded on a vessel.

6 (2) APPLICATION.—Paragraph (1) shall apply with respect to con-
7 tainers loaded on a vessel in a foreign country on or after the earlier
8 of—

9 (A) July 1, 2012; or

10 (B) another date established by the Secretary under paragraph

11 (3).

12 (3) ESTABLISHMENT OF EARLIER DEADLINE.—The Secretary shall
13 establish a date under paragraph (2)(B) pursuant to the lessons
14 learned through the pilot integrated scanning systems established
15 under section 231 of the Security and Accountability For Every Port
16 Act of 2006 (or SAFE Port Act) (Public Law 109–347, 120 Stat.
17 1915).

18 (4) EXTENSIONS.—The Secretary may extend the date specified in
19 subparagraph (A) or (B) of paragraph (2) for 2 years, and may renew
20 the extension in additional 2-year increments, for containers loaded in
21 a port or ports, if the Secretary certifies to Congress that at least 2
22 of the following conditions exist:

23 (A) Systems to scan containers under paragraph (1) are not
24 available for purchase and installation.

25 (B) Systems to scan containers under paragraph (1) do not
26 have a sufficiently low false alarm rate for use in the supply chain.

27 (C) Systems to scan containers under paragraph (1) cannot be
28 purchased, deployed, or operated at ports overseas, including, if
29 applicable, because a port does not have the physical characteris-
30 tics to install a system.

31 (D) Systems to scan containers under paragraph (1) cannot be
32 integrated, as necessary, with existing systems.

33 (E) Use of systems that are available to scan containers under
34 paragraph (1) will significantly impact trade capacity and the flow
35 of cargo.

36 (F) Systems to scan containers under paragraph (1) do not ade-
37 quately provide an automated notification of questionable or high-
38 risk cargo as a trigger for further inspection by appropriately
39 trained personnel.

40 (5) EXEMPTION FOR MILITARY CARGO.—Notwithstanding this sec-
41 tion, supplies bought by the Secretary of Defense and transported in

1 compliance with section 2631 of title 10 and military cargo of foreign
2 countries are exempt from the requirements of this section.

3 (6) REPORT ON EXTENSIONS.—An extension under paragraph (4)
4 for a port takes effect on the expiration of the 60-day period beginning
5 on the date the Secretary provides a report to Congress that—

6 (A) states what container traffic will be affected by the exten-
7 sion;

8 (B) provides supporting evidence to support the Secretary’s cer-
9 tification of the basis for the extension; and

10 (C) explains what measures the Secretary is taking to ensure
11 that scanning can be implemented as early as possible at the port
12 or ports that are the subject of the report.

13 (7) REPORT ON RENEWAL OF EXTENSION.—If an extension under
14 paragraph (4) takes effect, the Secretary shall, after 1 year, submit a
15 report to Congress on whether the Secretary expects to seek to renew
16 the extension.

17 (8) SCANNING TECHNOLOGY STANDARDS.—In implementing para-
18 graph (1), the Secretary shall—

19 (A) establish technological and operational standards for sys-
20 tems to scan containers;

21 (B) ensure that the standards are consistent with the global nu-
22 clear detection architecture developed under the Homeland Secu-
23 rity Act of 2002 (Public Law 107–296, 116 Stat. 2135); and

24 (C) coordinate with other Federal agencies that administer
25 scanning or detection programs at foreign ports.

26 (9) INTERNATIONAL TRADE AND OTHER OBLIGATIONS.—In carrying
27 out this subsection, the Secretary shall consult with appropriate Fed-
28 eral departments and agencies and private-sector stakeholders, and en-
29 sure that actions under this section do not violate international trade
30 obligations, and are consistent with the World Customs Organization
31 framework or other international obligations of the United States.

32 (c) REPORT.—Not later than 6 months after the submission of a report
33 under section 231(d) of the Security and Accountability For Every Port Act
34 of 2006 (or SAFE Port Act) (Public Law 109–347, 120 Stat. 1916), and
35 every 6 months thereafter, the Secretary shall submit a report to the appro-
36 priate congressional committees describing the status of full-scale deploy-
37 ment under subsection (b) and the cost of deploying the system at each for-
38 eign port at which the integrated scanning systems are deployed.

39 (d) SCANNING TECHNOLOGY REVIEW.—

40 (1) SOLICITATION OF PROPOSALS.—Not later than 1 year after Oc-
41 tober 5, 2018, and not less frequently than once every 5 years there-

1 after until the date of full-scale implementation of 100 percent screen-
2 ing of cargo containers and 100 percent scanning of high-risk con-
3 tainers required under this section, the Secretary shall solicit proposals
4 for scanning technologies, consistent with the standards under sub-
5 section (b)(8), to improve scanning of cargo at domestic ports. In solici-
6 ting the proposals, the Secretary shall establish measures to assess the
7 performance of the proposed scanning technologies, including—

8 (A) the rate of false positives;

9 (B) the delays in processing time; and

10 (C) the impact on the supply chain.

11 (2) PILOT PROGRAM.—

12 (A) ESTABLISHMENT.—The Secretary may establish a pilot pro-
13 gram to determine the efficacy of a scanning technology referred
14 to in paragraph (1).

15 (B) APPLICATION PROCESS.—In carrying out the pilot program,
16 the Secretary shall—

17 (i) solicit applications from domestic ports;

18 (ii) select up to 4 domestic ports to participate in the pilot
19 program; and

20 (iii) select ports with unique features and differing levels
21 of trade volume.

22 (3) REPORT.—Not later than 1 year after initiating a pilot program
23 under paragraph (2)(A), the Secretary shall submit to the Committees
24 on Commerce, Science, and Transportation and Homeland Security and
25 Governmental Affairs of the Senate and Committee on Homeland Secu-
26 rity of the House of Representatives a report on the pilot program, in-
27 cluding—

28 (A) an evaluation of the scanning technologies proposed to im-
29 prove security at domestic ports and to meet the full-scale imple-
30 mentation requirement;

31 (B) the costs to implement a pilot program;

32 (C) the benefits of the proposed scanning technologies;

33 (D) the impact of the pilot program on the supply chain; and

34 (E) recommendations for implementation of advanced cargo
35 scanning technologies at domestic ports.

36 (4) SHARING PILOT PROGRAM TESTING RESULTS.—The results of
37 the pilot testing of advanced cargo scanning technologies shall be
38 shared, as appropriate, with government agencies and private stake-
39 holders whose responsibilities encompass the secure transport of cargo.

1 **§ 30542. Provision of assistance, equipment, and training**

2 (a) INSPECTION TECHNOLOGY AND TRAINING.—The Secretary, in coordi-
3 nation with the Secretary of State, the Secretary of Energy, and appro-
4 priate representatives of other Federal agencies, may provide technical as-
5 sistance, equipment, and training to facilitate the implementation of supply
6 chain security measures at ports designated under the Container Security
7 Initiative.

8 (b) ACQUISITION AND TRAINING.—Unless otherwise prohibited by law,
9 the Secretary may—

10 (1) lease, lend, provide, or otherwise assist in the deployment of non-
11 intrusive inspection and radiation detection equipment at foreign land
12 and sea ports under terms and conditions the Secretary prescribes, in-
13 cluding nonreimbursable loans or the transfer of ownership of equip-
14 ment; and

15 (2) provide training and technical assistance for domestic or foreign
16 personnel responsible for operating or maintaining the equipment.

17 **§ 30543. Information sharing relating to supply chain secu-**
18 **urity cooperation**

19 (a) PURPOSES.—The purposes of this section are—

20 (1) to establish continuing liaison and to provide for supply chain se-
21 curity cooperation between the Department and the private sector; and

22 (2) to provide for regular and timely interchange of information be-
23 tween the private sector and the Department concerning developments
24 and security risks in the supply chain environment.

25 (b) DEVELOPMENT OF SYSTEM.—The Secretary shall develop a system
26 to collect appropriate risk information relating to the supply chain from,
27 and to share that information with, the private-sector entities determined
28 appropriate by the Secretary.

29 (c) CONSULTATION.—In developing the system under subsection (b), the
30 Secretary shall consult with the Commercial Operations Advisory Committee
31 and a broad range of public- and private-sector entities likely to utilize the
32 system, including importers, exporters, carriers, customs brokers, and
33 freight forwarders, among other parties.

34 (d) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section
35 shall be construed to limit or otherwise affect the ability of a Federal, State,
36 or local government entity, under applicable law, to obtain supply chain se-
37 curity information, including information lawfully and properly disclosed
38 generally or broadly to the public, and to use the information in any manner
39 permitted by law.

40 (e) AUTHORITY TO ISSUE WARNINGS.—The Secretary may provide
41 advisories, alerts, and warnings to relevant companies, targeted sectors,

1 other governmental entities, or the general public regarding potential risks
 2 to the supply chain as appropriate. In issuing a warning, the Secretary shall
 3 take appropriate actions to protect from disclosure—

4 (1) the source of any voluntarily submitted supply chain security in-
 5 formation that forms the basis for the warning; and

6 (2) information that is proprietary, business sensitive, relates specifi-
 7 cally to the submitting person or entity, or is otherwise not appro-
 8 priately in the public domain.

9 **Chapter 307—Administration**

Sec.

30701. Designation of liaison office of Department of State.

30702. Homeland Security Science and Technology Advisory Committee.

30703. Research, development, test, and evaluation efforts in furtherance of maritime and
 cargo security.

30704. Maritime cybersecurity risk assessment model and information sharing.

30705. Updates of maritime operations coordination plan.

30706. Maritime security capabilities assessments.

30707. Operational data sharing capability.

10 **§ 30701. Designation of liaison office of Department of State**

11 (a) IN GENERAL.—The Secretary of State shall designate a liaison office
 12 in the Department of State to assist the Secretary, as appropriate, in nego-
 13 tiating cargo security-related international agreements.

14 (b) RELATIONSHIP WITH COAST GUARD.—Nothing in this section shall
 15 be construed to affect—

16 (1) the authorities, functions, or capabilities of the Coast Guard to
 17 perform its missions; or

18 (2) the requirement under section 10312 of this title that those au-
 19 thorities, functions, and capabilities be maintained intact.

20 **§ 30702. Homeland Security Science and Technology Advi- 21 sory Committee**

22 The Under Secretary for Science and Technology shall utilize the Home-
 23 land Security Science and Technology Advisory Committee, as appropriate,
 24 to provide outside expertise in advancing cargo security technology.

25 **§ 30703. Research, development, test, and evaluation efforts 26 in furtherance of maritime and cargo security**

27 (a) IN GENERAL.—The Secretary shall—

28 (1) direct research, development, testing, and evaluation efforts in
 29 furtherance of maritime and cargo security;

30 (2) coordinate with public- and private-sector entities to develop and
 31 test technologies, and process innovations in furtherance of these objec-
 32 tives; and

33 (3) evaluate the technologies.

34 (b) COORDINATION.—The Secretary, in coordination with the Under Sec-
 35 retary for Science and Technology, the Assistant Secretary for Policy, the

1 Commandant of the Coast Guard, the Assistant Secretary for the Counter-
2 tering Weapons of Mass Destruction Office, the Chief Financial Officer, and
3 the heads of other appropriate offices or entities of the Department, shall
4 ensure that—

5 (1) research, development, testing, and evaluation efforts funded by
6 the Department in furtherance of maritime and cargo security are co-
7 ordinated within the Department and with other appropriate Federal
8 agencies to avoid duplication of efforts; and

9 (2) the results of the efforts are shared throughout the Department
10 and with other Federal, State, and local agencies, as appropriate.

11 **§ 30704. Maritime cybersecurity risk assessment model and**
12 **information sharing**

13 (a) RISK ASSESSMENT MODEL.—The Secretary, through the Com-
14 mandant of the Coast Guard and the Under Secretary responsible for over-
15 seeing the critical infrastructure protection, cybersecurity, and other related
16 programs of the Department, shall—

17 (1) not later than 1 year after October 5, 2018, coordinate with the
18 National Maritime Security Advisory Committee, the Area Maritime
19 Security Advisory Committee, and other maritime stakeholders, as nec-
20 essary, to develop and implement a maritime cybersecurity risk assess-
21 ment model, consistent with the activities described in section 2(e) of
22 the National Institute of Standards and Technology Act (15 U.S.C.
23 272(e)), to evaluate current and future cybersecurity risks that have
24 the potential to affect the maritime transportation system or that
25 would cause a transportation security incident (as defined in 46 U.S.C.
26 70101) in ports; and

27 (2) not less than biennially thereafter, evaluate the effectiveness of
28 the cybersecurity risk assessment model established under paragraph
29 (1).

30 (b) INFORMATION SHARING.—The Commandant of the Coast Guard and
31 the Under Secretary responsible for overseeing the critical infrastructure
32 protection, cybersecurity, and other related programs of the Department
33 shall—

34 (1) ensure there is a process for each Area Maritime Security Advi-
35 sory Committee established under section 70112 of title 46—

36 (A) to facilitate the sharing of information related to cybersecu-
37 rity risks that may cause transportation security incidents;

38 (B) to timely report transportation security incidents to the na-
39 tional level; and

1 (C) to disseminate the reports across the entire maritime trans-
2 portation system via the National Cybersecurity and Communica-
3 tions Integration Center; and

4 (2) issue voluntary guidance for the management of those cybersecu-
5 rity risks in each Area Maritime Transportation Security Plan and fa-
6 cility security plan required under section 70103 of title 46 approved
7 after the date that the cybersecurity risk assessment model is developed
8 under subsection (a).

9 **§ 30705. Updates of maritime operations coordination plan**

10 (a) IN GENERAL.—Not later than 180 days after October 5, 2018, and
11 biennially thereafter, the Secretary shall—

12 (1) update the Maritime Operations Security Plan, published by the
13 Department on July 7, 2011, to strengthen coordination, planning, in-
14 formation sharing, and intelligence integration for maritime operations
15 of components and offices of the Department with responsibility for
16 maritime security missions; and

17 (2) submit each update to the Committee on Commerce, Science, and
18 Transportation and the Committee on Homeland Security and Govern-
19 mental Affairs of the Senate and the Committee on Transportation and
20 Infrastructure and the Committee on Homeland Security of the House
21 of Representatives.

22 (b) CONTENTS.—Each update shall address the following:

23 (1) Coordinating the planning, integration of maritime operations,
24 and development of joint maritime domain awareness efforts of any
25 component or office of the Department with responsibility for maritime
26 security missions;

27 (2) Maintaining effective information sharing and, as appropriate,
28 intelligence integration with Federal, State, and local officials and the
29 private sector regarding threats to maritime security;

30 (3) Cooperating and coordinating with Federal departments and
31 agencies, and State and local agencies, in the maritime environment in
32 support of maritime security missions.

33 (4) Highlighting the work completed in the context of other national
34 and Department maritime security strategic guidance and how the
35 work fits with the Maritime Operations Coordination Plan.

36 **§ 30706. Maritime security capabilities assessments**

37 Not later than 180 days after October 5, 2018, and annually thereafter,
38 the Secretary shall submit to the Committee on Commerce, Science, and
39 Transportation and the Committee on Homeland Security and Govern-
40 mental Affairs of the Senate and the Committee on Transportation and In-
41 frastructure and the Committee on Homeland Security of the House of Rep-

1 representatives an assessment of the number and type of maritime assets and
2 the number of personnel required to increase the Department's maritime re-
3 sponse rate pursuant to section 11115 of this title.

4 **§ 30707. Operational data sharing capability**

5 (a) IN GENERAL.—Not later than June 23, 2024, the Secretary shall,
6 consistent with the ongoing Integrated Multi-Domain Enterprise joint effort
7 by the Department and the Department of Defense, establish a secure cen-
8 tralized capability to allow real-time or near real-time data and information
9 sharing between Customs and Border Protection and the Coast Guard for
10 purposes of maritime boundary domain awareness and enforcement activi-
11 ties along the maritime boundaries of the United States including the mari-
12 time boundaries in the northern and southern continental United States and
13 Alaska.

14 (b) PRIORITY.—In establishing the capability under subsection (a), the
15 Secretary shall prioritize enforcement areas experiencing the highest levels
16 of enforcement activity.

17 (c) REQUIREMENTS.—The capability established under subsection (a)
18 shall be sufficient for the secure sharing of data, information, and surveil-
19 lance necessary for operational missions, including data from governmental
20 assets, irrespective of whether an asset located in or around mission oper-
21 ations areas belongs to the Coast Guard, Customs and Border Protection,
22 or any other partner agency.

23 (d) ELEMENTS.—The Commissioner and the Commandant of the Coast
24 Guard shall jointly—

25 (1) assess and delineate the types of data and quality of data sharing
26 needed to meet the respective operational missions of Customs and
27 Border Protection and the Coast Guard, including video surveillance,
28 seismic sensors, infrared detection, space-based remote sensing, and
29 any other necessary data or information;

30 (2) develop appropriate requirements and processes for the
31 credentialing of personnel of Customs and Border Protection and per-
32 sonnel of the Coast Guard to access and use the capability established
33 under subsection(a); and

34 (3) establish a cost-sharing agreement for the long-term operation
35 and maintenance of the capability and the assets that provide data to
36 the capability.

37 (e) REPORTS.—Not later than December 23, 2024, the Secretary shall
38 submit to the Committee on Commerce, Science, and Transportation and
39 the Committee on Homeland Security and Governmental Affairs of the Sen-
40 ate and the Committee on Transportation and Infrastructure and the Com-

1 mittee on Homeland Security of the House of Representatives a report on
2 the establishment of the capability under this section.

3 (f) RULE OF CONSTRUCTION.—Nothing in this section may be construed
4 to authorize the Coast Guard, Customs and Border Protection, or any other
5 partner agency to acquire, share, or transfer personal information relating
6 to an individual in violation of any Federal or State law or regulation.

7 **Subtitle IV—Transportation Security**
8 **Chapter 401—General**

Sec.

40101. Definitions.

9 **§ 40101. Definitions**

10 (a) DEPARTMENT.—In chapters 403 through 407 of this title, the term
11 “Department” means the Department of Homeland Security.

12 (b) SECRETARY.—In this subtitle, the term “Secretary” means the Sec-
13 retary of Homeland Security.

14 **Chapter 403—Transportation Security**
15 **Planning, Information Sharing, and En-**
16 **hancements**

Subchapter I—Security Planning and Information Sharing

Sec.

40301. National Domestic Preparedness Consortium.

40302. National Transportation Security Center of Excellence.

40303. Immunity for reports of suspected terrorist activity or suspicious behavior and re-
sponse.

Subchapter II—Security Enhancements

40311. Definitions.

40312. Authorization of Visible Intermodal Prevention and Response teams.

40313. Surface transportation security inspectors.

40314. Surface transportation security technology information sharing.

40315. Transportation Security Administration personnel limitations.

40316. National explosives detection canine team training program.

40317. Third party domestic canines.

40318. Voluntary use of credentialing.

40319. Biometrics expansion.

40320. Roles of the Department and the Department of Transportation.

40321. Integrated and unified operations centers.

40322. Security awareness program.

17 **Subchapter I—Security Planning and**
18 **Information Sharing**

19 **§ 40301. National Domestic Preparedness Consortium**

20 (a) IN GENERAL.—The Secretary may establish, operate, and maintain
21 a National Domestic Preparedness Consortium in the Department.

22 (b) MEMBERS.—The National Domestic Preparedness Consortium con-
23 sists of—

24 (1) the Center for Domestic Preparedness;

25 (2) the National Energetic Materials Research and Testing Center,
26 New Mexico Institute of Mining and Technology;

1 (3) the National Center for Biomedical Research and Training, Lou-
2 isiana State University

3 (4) the National Emergency Response and Rescue Training Center,
4 Texas A&M University;

5 (5) the National Exercise, Test, and Training Center, Nevada Test
6 Site;

7 (6) the Transportation Technology Center, Incorporated, in Pueblo,
8 Colorado; and

9 (7) the National Disaster Preparedness Training Center, University
10 of Hawaii.

11 (c) DUTIES.—The National Domestic Preparedness Consortium shall
12 identify, develop, test, and deliver training to State, local, and tribal emer-
13 gency response providers, provide on-site and mobile training at the per-
14 formance and management and planning levels, and facilitate the delivery
15 of training by the training partners of the Department.

16 **§ 40302. National Transportation Security Center of Excel-**
17 **lence**

18 (a) ESTABLISHMENT.—The Secretary shall establish a National Trans-
19 portation Security Center of Excellence to conduct research and education
20 activities, and to develop or provide professional security training, including
21 the training of transportation employees and transportation professionals.

22 (b) DESIGNATION.—The Secretary shall select one of the institutions
23 identified in subsection (c) as the lead institution responsible for coordi-
24 nating the National Transportation Security Center of Excellence.

25 (c) MEMBER INSTITUTIONS.—

26 (1) CONSORTIUM.—The institution of higher education selected
27 under subsection (b) shall execute agreements with the other institu-
28 tions of higher education identified in this subsection and other institu-
29 tions designated by the Secretary to develop a consortium to assist in
30 accomplishing the goals of the Center.

31 (2) MEMBERS.—The National Transportation Security Center of Ex-
32 cellence consists of—

33 (A) Texas Southern University in Houston, Texas;

34 (B) the National Transit Institute at Rutgers, The State Uni-
35 versity of New Jersey;

36 (C) Tougaloo College;

37 (D) the Connecticut Transportation Institute at the University
38 of Connecticut;

39 (E) the Homeland Security Management Institute, Long Island
40 University;

1 (F) the Mack-Blackwell National Rural Transportation Study
2 Center at the University of Arkansas; and

3 (G) any additional institutions or facilities designated by the
4 Secretary.

5 (3) CERTAIN INCLUSIONS.—To the extent practicable, the Secretary
6 shall ensure that an appropriate number of additional consortium col-
7 leges or universities designated by the Secretary under this subsection
8 are Historically Black Colleges and Universities, Hispanic-serving insti-
9 tutions, and Indian tribally controlled colleges and universities.

10 **§ 40303. Immunity for reports of suspected terrorist activity**
11 **or suspicious behavior and response**

12 (a) DEFINITIONS.—In this section:

13 (1) AUTHORIZED OFFICIAL.—The term “authorized official”
14 means—

15 (A) an employee or agent of a passenger transportation system
16 or other person with responsibilities relating to the security of the
17 system;

18 (B) an officer, employee, or agent of the Department, the De-
19 partment of Transportation, or the Department of Justice with re-
20 sponsibilities relating to the security of passenger transportation
21 systems; or

22 (C) a Federal, State, or local law enforcement officer.

23 (2) COVERED ACTIVITY.—The term “covered activity” means a sus-
24 picious transaction, activity, or occurrence that involves, or is directed
25 against, a passenger transportation system or vehicle or its passengers
26 indicating that an individual may be engaging, or preparing to engage,
27 in a violation of law relating to—

28 (A) a threat to a passenger transportation system or passenger
29 safety or security; or

30 (B) an act of terrorism (as that term is defined in section 3077
31 of title 18).

32 (3) PASSENGER TRANSPORTATION.—The term “passenger transpor-
33 tation” means—

34 (A) public transportation, as defined in section 5302 of title 49;

35 (B) transportation by an over-the-road bus, as defined in section
36 40701 of this title, and school bus transportation;

37 (C) intercity rail passenger transportation, as defined in section
38 24102 of title 49;

39 (D) the transportation of passengers onboard a passenger ves-
40 sel, as defined in section 2101 of title 46;

1 (E) other regularly scheduled waterborne transportation service
2 of passengers by a vessel of at least 20 gross tons; and

3 (F) air transportation, as defined in section 40102 of title 49,
4 of passengers.

5 (4) PASSENGER TRANSPORTATION SYSTEM.—The term “passenger
6 transportation system” means an entity or entities organized to provide
7 passenger transportation using vehicles, including the infrastructure
8 used to provide the transportation.

9 (5) VEHICLE.—The term “vehicle” has the meaning given the term
10 in section 1992(d)(16) of title 18.

11 (b) IMMUNITY FOR REPORTS OF SUSPECTED TERRORIST ACTIVITY OR
12 SUSPICIOUS BEHAVIOR.—

13 (1) IN GENERAL.—A person who, in good faith and based on objec-
14 tively reasonable suspicion, makes, or causes to be made, a voluntary
15 report of covered activity to an authorized official shall be immune
16 from civil liability under Federal, State, and local law for the report.

17 (2) FALSE REPORTS.—Paragraph (1) shall not apply to any report
18 that the person knew to be false or was made with reckless disregard
19 for the truth at the time that person made that report.

20 (c) IMMUNITY FOR RESPONSE.—

21 (1) IN GENERAL.—An authorized official who observes, or receives
22 a report of, covered activity and takes reasonable action in good faith
23 to respond to the activity has qualified immunity from civil liability for
24 the action, consistent with applicable law in the relevant jurisdiction.
25 An authorized official (as defined by subsection (a)(1)(A)) not entitled
26 to assert the defense of qualified immunity is immune from civil liabil-
27 ity under Federal, State, and local law if the authorized official takes
28 reasonable action, in good faith, to respond to the reported activity.

29 (2) SAVINGS CLAUSE.—Nothing in this subsection affects the ability
30 of an authorized official to assert any defense, privilege, or immunity
31 that would otherwise be available, and this subsection shall not be con-
32 strued as affecting the defense, privilege, or immunity.

33 (d) ATTORNEY FEES AND COSTS.—A person or authorized official found
34 to be immune from civil liability under this section is entitled to recover
35 from the plaintiff all reasonable costs and attorney fees.

36 **Subchapter II—Security Enhancements**

37 **§ 40311. Definitions**

38 In this subchapter:

39 (1) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term “appro-
40 priate congressional committee” means the Committee on Commerce,
41 Science, and Transportation, the Committee on Banking, Housing, and

1 Urban Affairs, and the Committee on Homeland Security and Govern-
2 mental Affairs of the Senate and the Committee on Homeland Security
3 and the Committee on Transportation and Infrastructure of the House.

4 (2) STATE.—The term “State” means a State, the District of Co-
5 lumbia, Puerto Rico, the Northern Mariana Islands, the Virgin Islands,
6 Guam, American Samoa, and any other territory (including a posses-
7 sion) of the United States.

8 (3) TERRORISM.—The term “terrorism” has the meaning given the
9 term in section 10101 of this title.

10 (4) UNITED STATES.—The term “United States” means the States,
11 the District of Columbia, Puerto Rico, the Northern Mariana Islands,
12 the Virgin Islands, Guam, American Samoa, and any other territory
13 (including a possession) of the United States.

14 **§ 40312. Authorization of Visible Intermodal Prevention and**
15 **Response teams**

16 (a) IN GENERAL.—The Secretary, acting through the Administrator of
17 the Transportation Security Administration, may develop Visible Intermodal
18 Prevention and Response (in this section referred to as “VIPR”) teams to
19 augment the security of any mode of transportation at any location within
20 the United States. In forming a VIPR team, the Secretary—

21 (1) may use any asset of the Department, including Federal air mar-
22 shals, surface transportation security inspectors, canine detection
23 teams, and advanced screening technology;

24 (2) may determine when a VIPR team shall be deployed, as well as
25 the duration of the deployment;

26 (3) shall, prior to and during the deployment, consult with local se-
27 curity and law enforcement officials in the jurisdiction where the VIPR
28 team is or will be deployed, to develop and agree upon the appropriate
29 operational protocols and provide relevant information about the mis-
30 sion of the VIPR team, as appropriate;

31 (4) shall, prior to and during the deployment, consult with all trans-
32 portation entities directly affected by the deployment of a VIPR team
33 as to specific locations and times in the facilities of the entities at
34 which VIPR teams are to be deployed to maximize the effectiveness of
35 the deployment, as appropriate, including railroad carriers, air carriers,
36 airport owners, over-the-road bus operators and terminal owners and
37 operators, motor carriers, public transportation agencies, owners or op-
38 erators of highways, port operators and facility owners, vessel owners
39 and operators, and pipeline operators; and

40 (5) shall require, as appropriate based on risk, in the case of a VIPR
41 team deployed to an airport, that the VIPR team conduct operations—

1 (A) in the sterile area and any other areas to which only indi-
2 viduals issued security credentials have unrestricted access; and

3 (B) in nonsterile areas.

4 (b) PERFORMANCE MEASURES.—Not later than 1 year after October 5,
5 2018, the Administrator shall develop and implement a system of qualitative
6 performance measures and objectives to assess the roles, activities, and ef-
7 fectiveness of VIPR team operations on an ongoing basis, including a mech-
8 anism through which the transportation entities referred to in subsection
9 (a)(4) may submit feedback on VIPR team operations involving their sys-
10 tems or facilities.

11 (c) PLAN FOR ENSURING INTEROPERABILITY OF COMMUNICATIONS.—
12 Not later than 1 year after October 5, 2018, the Administrator shall develop
13 and implement a plan for ensuring the interoperability of communications
14 among VIPR team participants and between VIPR teams and transpor-
15 tation entities with systems or facilities that are involved in VIPR team op-
16 erations. The plan shall include an analysis of the costs and resources re-
17 quired to carry out the plan.

18 (d) NOTIFICATIONS TO CONGRESS.—

19 (1) NUMBER OF VIPR TEAMS AVAILABLE FOR DEPLOYMENT.—

20 (A) IN GENERAL.—Not later than 90 days after October 5,
21 2018, and annually thereafter, the Administrator shall notify the
22 Committees on Commerce, Science, and Transportation and
23 Homeland Security and Governmental Affairs of the Senate and
24 Committee on Homeland Security of the House of Representatives
25 of the number of VIPR teams available for deployment at trans-
26 portation facilities, including—

27 (i) the number of VIPR team operations that include explo-
28 sive detection canine teams; and

29 (ii) the distribution of VIPR team operations deployed
30 across different modes of transportation.

31 (B) ANNEX.—The notification under subparagraph (A) may
32 contain a classified annex.

33 (2) DEPLOYMENT OF PERSONNEL OR RESOURCES.—

34 (A) IN GENERAL.—If the Administrator deploys any counterter-
35 rorism personnel or resource, such as explosive detection sweeps,
36 random bag inspections, or patrols by VIPR teams, to enhance se-
37 curity at a transportation system or transportation facility for a
38 period of not less than 180 consecutive days, the Administrator
39 shall provide sufficient notification to the system or facility oper-
40 ator, as applicable, not less than 14 days prior to terminating the
41 deployment.

1 (B)EXCEPTION.—This paragraph shall not apply if the Admin-
2 istrator—

3 (i) determines there is an urgent security need for the per-
4 sonnel or resource described in subparagraph (A); and

5 (ii) notifies the Committees on Commerce, Science, and
6 Transportation and Homeland Security and Governmental
7 Affairs of the Senate and Committee on Homeland Security
8 of the House of Representatives of the determination under
9 subparagraph (A).

10 **§ 40313. Surface transportation security inspectors**

11 (a) IN GENERAL.—The Secretary, acting through the Administrator of
12 the Transportation Security Administration, may train, employ, and utilize
13 surface transportation security inspectors.

14 (b) MISSION.—The Secretary shall use surface transportation security in-
15 spectors to assist surface transportation carriers, operators, owners, entities,
16 and facilities to enhance their security against terrorist attack and other se-
17 curity threats and to assist the Secretary in enforcing applicable surface
18 transportation security regulations and directives.

19 (c) AUTHORITIES.—Surface transportation security inspectors employed
20 under this section shall be authorized powers and delegated responsibilities
21 that the Secretary determines appropriate, subject to subsection (e).

22 (d) REQUIREMENTS.—The Secretary shall require that surface transpor-
23 tation security inspectors have relevant transportation experience and other
24 security and inspection qualifications, as determined appropriate.

25 (e) LIMITATIONS.—

26 (1) INSPECTORS.—Surface transportation inspectors shall be prohib-
27 ited from issuing fines to public transportation agencies (as defined in
28 section 40501 of this title) for violations of the Department's regula-
29 tions or orders except through the process described in paragraph (2).

30 (2) CIVIL PENALTIES.—The Secretary shall be prohibited from as-
31 sessing civil penalties against public transportation agencies (as defined
32 in section 40501 of this title) for violations of the Department's regula-
33 tions or orders, except in accordance with the following:

34 (A) In the case of a public transportation agency that is found
35 to be in violation of a regulation or order issued by the Secretary,
36 the Secretary shall seek correction of the violation through a writ-
37 ten notice to the public transportation agency and shall give the
38 public transportation agency reasonable opportunity to correct the
39 violation or propose an alternative means of compliance acceptable
40 to the Secretary.

1 (B) If the public transportation agency does not correct the vio-
2 lation or propose an alternative means of compliance acceptable to
3 the Secretary within a reasonable time period that is specified in
4 the written notice, the Secretary may take any action authorized
5 in sections 11501 through 11505(b), 11506 through 11514,
6 11516(a) through (h), and 11519 of this title.

7 (3) LIMITATION ON SECRETARY.—The Secretary shall not initiate
8 civil enforcement actions for violations of administrative and procedural
9 requirements pertaining to the application for, and expenditure of,
10 funds awarded under transportation security grant programs under the
11 Implementing Recommendations of the 9/11 Commission Act of 2007
12 (Public Law 110–53, 121 Stat. 266).

13 (f) COORDINATION.—The Secretary shall ensure that the mission of the
14 surface transportation security inspectors is consistent with any relevant
15 risk assessments required by the Implementing Recommendations of the 9/
16 11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 266) or com-
17 pleted by the Department, the modal plans required under section 11514
18 of this title, the Memorandum of Understanding between the Department
19 and the Department of Transportation on Roles and Responsibilities, dated
20 September 28, 2004, and all subsequent annexes to this Memorandum of
21 Understanding, and other relevant documents setting forth the Depart-
22 ment’s transportation security strategy, as appropriate.

23 (g) CONSULTATION.—The Secretary shall periodically consult with the
24 surface transportation entities that are or may be inspected by the surface
25 transportation security inspectors, including, as appropriate, railroad car-
26 riers, over-the-road bus operators and terminal owners and operators, motor
27 carriers, public transportation agencies, owners or operators of highways,
28 and pipeline operators on—

29 (1) the inspectors’ duties, responsibilities, authorities, and mission;
30 and

31 (2) strategies to improve transportation security and to ensure com-
32 pliance with transportation security requirements.

33 **§ 40314. Surface transportation security technology infor-**
34 **mation sharing**

35 (a) IN GENERAL.—

36 (1) INFORMATION SHARING.—The Secretary, in consultation with
37 the Secretary of Transportation, shall establish a program to provide
38 appropriate information that the Department has gathered or devel-
39 oped on the performance, use, and testing of technologies that may be
40 used to enhance railroad, public transportation, and surface transpor-
41 tation security to surface transportation entities, including railroad car-

1 riers, over-the-road bus operators and terminal owners and operators,
2 motor carriers, public transportation agencies, owners or operators of
3 highways, pipeline operators, and State, local, and tribal governments
4 that provide security assistance to the entities.

5 (2) DESIGNATION OF QUALIFIED ANTI-TERRORISM TECH-
6 NOLOGIES.—The Secretary shall include in the information provided in
7 paragraph (1) whether the technology is designated as a qualified anti-
8 terrorism technology under subchapter II of chapter 109 of this title,
9 as appropriate.

10 (b) PURPOSE.—The purpose of the program is to assist eligible grant re-
11 cipients under this subtitle and others, as appropriate, to purchase and use
12 the best technology and equipment available to meet the security needs of
13 the Nation’s surface transportation system.

14 (c) COORDINATION.—The Secretary shall ensure that the program estab-
15 lished under this section makes use of and is consistent with other Depart-
16 ment technology testing, information sharing, evaluation, and standards-set-
17 ting programs, as appropriate.

18 **§ 40315. Transportation Security Administration personnel**
19 **limitations**

20 Any statutory limitation on the number of employees in the Transpor-
21 tation Security Administration does not apply to employees carrying out this
22 chapter, chapters 401, 405, and 407 of this title, and titles XII through
23 XV of the Implementing Recommendations of the 9/11 Commission Act of
24 2007 (Public Law 110–53, 121 Stat. 381).

25 **§ 40316. National explosives detection canine team training**
26 **program**

27 (a) DEFINITION OF EXPLOSIVES DETECTION CANINE TEAM.—In this
28 section, the term “explosives detection canine team” means a canine and a
29 canine handler that are trained to detect explosives, radiological materials,
30 chemical, nuclear or biological weapons, or other threats as defined by the
31 Secretary.

32 (b) IN GENERAL.—

33 (1) INCREASED CAPACITY.—The Secretary shall—

34 (A) begin to increase the number of explosives detection canine
35 teams certified by the Transportation Security Administration for
36 the purposes of transportation-related security by up to 200 ca-
37 nine teams annually by the end of 2010; and

38 (B) encourage State, local, and tribal governments and private
39 owners of high-risk transportation facilities to strengthen security
40 through the use of highly trained explosives detection canine
41 teams.

1 (2) WAYS TO INCREASE NUMBER OF EXPLOSIVES DETECTION CA-
2 NINE TEAMS.—The Secretary shall increase the number of explosives
3 detection canine teams by—

4 (A) using the Transportation Security Administration’s Na-
5 tional Explosives Detection Canine Team Training Center, includ-
6 ing expanding and upgrading existing facilities, procuring and
7 breeding additional canines, and increasing staffing and oversight
8 commensurate with the increased training and deployment capa-
9 bilities;

10 (B) partnering with other Federal, State, or local agencies, non-
11 profit organizations, universities, or the private sector to increase
12 the training capacity for canine detection teams;

13 (C) procuring explosives detection canines trained by nonprofit
14 organizations, universities, or the private sector, provided they are
15 trained in a manner consistent with the standards and require-
16 ments developed under subsection (c) or other criteria developed
17 by the Secretary; or

18 (D) employing a combination of subparagraphs (A), (B), and
19 (C), as appropriate.

20 (c) STANDARDS FOR EXPLOSIVES DETECTION CANINE TEAMS.—

21 (1) IN GENERAL.—Based on the feasibility of meeting the ongoing
22 demand for quality explosives detection canine teams, the Secretary
23 shall establish criteria, including canine training curricula, performance
24 standards, and other requirements approved by the Transportation Se-
25 curity Administration necessary to ensure that explosives detection ca-
26 nine teams trained by nonprofit organizations, universities, and private-
27 sector entities are adequately trained and maintained.

28 (2) EXPANSION.—In developing and implementing the curricula, per-
29 formance standards, and other requirements, the Secretary shall—

30 (A) coordinate with key stakeholders, including international,
31 Federal, State, and local officials, and private-sector and academic
32 entities to develop best practice guidelines for a standardized pro-
33 gram, as appropriate;

34 (B) require that explosives detection canine teams trained by
35 nonprofit organizations, universities, or private-sector entities that
36 are used or made available by the Secretary be trained consistent
37 with specific training criteria developed by the Secretary; and

38 (C) review the status of the private-sector programs on at least
39 an annual basis to ensure compliance with training curricula, per-
40 formance standards, and other requirements.

41 (d) DEPLOYMENT.—The Secretary shall—

1 (1) use the additional explosives detection canine teams as part of
2 the Department's efforts to strengthen security across the Nation's
3 transportation network, and may use the canine teams on a more lim-
4 ited basis to support other homeland security missions, as determined
5 appropriate by the Secretary;

6 (2) make available explosives detection canine teams to all modes of
7 transportation, for high-risk areas or to address specific threats, on an
8 as-needed basis and as otherwise determined appropriate by the Sec-
9 retary;

10 (3) encourage, but not require, any transportation facility or system
11 to deploy TSA-certified explosives detection canine teams developed
12 under this section; and

13 (4) consider specific needs and training requirements for explosives
14 detection canine teams to be deployed across the Nation's transpor-
15 tation network, including in venues of multiple modes of transportation,
16 as appropriate.

17 (e) CANINE PROCUREMENT.—The Secretary, acting through the Adminis-
18 trator of the Transportation Security Administration, shall work to ensure
19 that explosives detection canine teams are procured as efficiently as possible
20 and at the best price, while maintaining the needed level of quality, includ-
21 ing, if appropriate, through increased domestic breeding.

22 (f) REVIEW OF PROGRAM.—

23 (1) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In
24 this subsection, the term “appropriate committees of Congress”
25 means—

26 (A) the Committee on Commerce, Science, and Transportation
27 of the Senate;

28 (B) the Committee on Homeland Security and Governmental
29 Affairs of the Senate; and

30 (C) the Committee on Homeland Security of the House of Rep-
31 resentatives.

32 (2) IN GENERAL.—Not later than 90 days after the date on which
33 the Inspector General of the Department receives the report under sec-
34 tion 11353(e) of this title, the Inspector General of the Department
35 shall—

36 (A) review the explosives detection canine team program, includ-
37 ing—

38 (i) the development by the Transportation Security Admin-
39 istration of a deployment strategy for explosives detection ca-
40 nine teams;

1 (ii) the national explosives detection canine team training
2 program, including canine training, handler training, re-
3 fresher training, and updates to the training;

4 (iii) the use of the canine assets during an urgent security
5 need, including the reallocation of the program resources out-
6 side the transportation systems sector during an urgent secu-
7 rity need; and

8 (iv) the monitoring and tracking of canine assets; and

9 (B) submit to the appropriate committees of Congress a report
10 on the review, including any recommendations.

11 (3) CONSIDERATIONS.—In conducting the review of the deployment
12 strategy under paragraph (2)(A)(i), the Inspector General shall con-
13 sider whether the Transportation Security Administration’s method to
14 analyze the risk to transportation facilities and transportation systems
15 is appropriate.

16 (g) EXPANSION OF PROGRAM.—

17 (1) DEFINITION OF EXPLOSIVES DETECTION CANINE TEAMS.—In
18 this subsection, the term “explosives detection canine teams” means a
19 canine and a canine handler that are trained to detect explosives and
20 other threats as defined by the Secretary.

21 (2) ENCOURAGEMENT OF USE OF EXPLOSIVE DETECTION CANINE
22 TEAMS.—The Secretary, where appropriate, shall encourage State,
23 local, and tribal governments and private owners of high-risk transpor-
24 tation facilities to strengthen security through the use of explosives de-
25 tection canine teams.

26 (3) INCREASED CAPACITY.—

27 (A) BEFORE REPORT SUBMITTED.—Before the date on which
28 the Inspector General of the Department submits the report under
29 subsection (f), the Administrator may increase the number of
30 State and local surface and maritime transportation canines by
31 not more than 70 explosives detection canine teams.

32 (B) BEGINNING ON DATE REPORT SUBMITTED.—Beginning on
33 the date on which the Inspector General of the Department sub-
34 mits the report under subsection (f), the Secretary may increase
35 the State and local surface and maritime transportation canines
36 by up to 200 explosives detection canine teams unless more are
37 identified in the risk-based surface transportation security strategy
38 under section 40723 of this title, consistent with section 40724 of
39 this title or with the President’s most recent budget submitted
40 under section 1105 of title 31.

1 (C) RECOMMENDATIONS.—Before initiating an increase in the
2 number of explosives detection teams under subparagraph (B), the
3 Secretary shall consider any recommendations in the report under
4 subsection (f) on the efficacy and management of the explosives
5 detection canine program.

6 (4) DEPLOYMENT.—The Secretary shall—

7 (A) use the additional explosives detection canine teams, as de-
8 scribed in paragraph (3)(A), as part of the Department’s efforts
9 to strengthen security across the Nation’s surface and maritime
10 transportation networks;

11 (B) make available explosives detection canine teams to all
12 modes of transportation, subject to the requirements under section
13 40312(a) through (c) of this title, to address specific
14 vulnerabilities or risks, on an as-needed basis and as otherwise de-
15 termined appropriate by the Secretary; and

16 (C) consider specific needs and training requirements for explo-
17 sives detection canine teams to be deployed across the Nation’s
18 surface and maritime transportation networks, including in venues
19 of multiple modes of transportation, as the Secretary considers ap-
20 propriate.

21 (h) USE OF DIGITAL MONITORING SYSTEM TO FACILITATE IMPROVED
22 REVIEW, DATA ANALYSIS, AND RECORD KEEPING OF CANINE TESTING
23 PERFORMANCE AND PROGRAM ADMINISTRATION.—Not later than 180 days
24 after October 5, 2018, the Administrator shall use, to the extent practicable,
25 a digital monitoring system for all training, testing, and validation or certifi-
26 cation of public and private canine assets utilized or funded by the Trans-
27 portation Security Administration to facilitate improved review, data anal-
28 ysis, and record keeping of canine testing performance and program admin-
29 istration.

30 **§ 40317. Third party domestic canines**

31 (a) DEFINITIONS.—In this section:

32 (1) BEHAVIORAL STANDARDS.—The term “behavioral standards”
33 means standards for the evaluation of explosives detection working ca-
34 nines for certain factors, including canine temperament, work drive,
35 suitability for training, environmental factors used in evaluations, and
36 canine familiarity with natural or man-made surfaces or working condi-
37 tions relevant to the canine’s expected work area.

38 (2) MEDICAL STANDARDS.—The term “medical standards” means
39 standards for the evaluation of explosives detection working canines for
40 certain factors, including canine health, management of heredity health

1 conditions, breeding practices, genetics, pedigree, and long-term health
2 tracking.

3 (3) TECHNICAL STANDARDS.—The term “technical standards”
4 means standards for the evaluation of explosives detection working ca-
5 nines for certain factors, including canine search techniques, handler-
6 canine communication, detection testing conditions and logistics, and
7 learned explosive odor libraries.

8 (b) WORKING GROUP.—

9 (1) ESTABLISHMENT.—Not later than 90 days after October 5,
10 2018, the Administrator shall establish a working group to determine
11 ways to support decentralized, non-Federal domestic canine breeding
12 capacity to produce high quality explosives detection canines and mod-
13 ernize canine training standards.

14 (2) COMPOSITION.—The working group established under paragraph
15 (1) shall be comprised of representatives from the following:

16 (A) The Transportation Security Administration.

17 (B) The Science and Technology Directorate of the Department.

18 (C) National domestic canine associations with expertise in
19 breeding and pedigree.

20 (D) Universities with expertise related to explosives detection
21 canines and canine breeding.

22 (E) Domestic canine breeders and vendors.

23 (3) CHAIRPERSONS.—The Administrator shall approve of 2 individ-
24 uals from among the representatives of the working group specified in
25 paragraph (2) to serve as the Chairpersons of the working group as
26 follows:

27 (A) One Chairperson shall be from an entity specified in sub-
28 paragraph (A) or (B) of paragraph (2).

29 (B) One Chairperson shall be from an entity specified in sub-
30 paragraph (C), (D), or (E) of paragraph (2).

31 (4) PROPOSED STANDARDS AND RECOMMENDATIONS.—Not later
32 than 180 days after the date on which the working group is established
33 under paragraph (1), the working group shall submit to the Adminis-
34 trator—

35 (A) proposed behavioral standards, medical standards, and tech-
36 nical standards for domestic canine breeding and canine training
37 described in paragraph (1); and

38 (B) recommendations on how the Transportation Security Ad-
39 ministration can engage stakeholders to further the development
40 of the domestic non-Federal canine breeding capacity and training
41 described in paragraph (1).

1 (5) STRATEGY.—Not later than 180 days after the date the rec-
2 ommendations are submitted under paragraph (4), the Administrator
3 shall develop and submit to the appropriate committees of Congress a
4 strategy for working with non-Federal stakeholders to facilitate the ex-
5 panded domestic canine breeding capacity described in paragraph (1),
6 based on the recommendations.

7 (6) CONSULTATION.—In developing the strategy under paragraph
8 (5), the Administrator shall consult with the Under Secretary for
9 Science and Technology of the Department, the Commissioner for U.S.
10 Customs and Border Protection, the Director of the United States Se-
11 cret Service, and the heads of such other Federal departments or agen-
12 cies as the Administrator considers appropriate to incorporate, to the
13 extent practicable, mission needs across the Department for an ex-
14 panded non-Federal domestic explosives detection canine breeding ca-
15 pacity that can be leveraged to help meet the Department’s operational
16 needs.

17 (7) TERMINATION.—The working group established under paragraph
18 (1) shall terminate on the date on which the strategy is submitted
19 under paragraph (5), unless the Administrator extends the termination
20 date for the purposes of subsection (c).

21 (8) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5T.—Chapter 10
22 of title 5 shall not apply to the working group established under this
23 subsection.

24 (c) DEVELOPMENT AND ISSUANCE OF STANDARDS AND GUIDANCE.—

25 (1) IN GENERAL.—Not later than 1 year after October 5, 2018, to
26 enhance the efficiency and efficacy of transportation security by in-
27 creasing the supply of canine teams for use by the Transportation Se-
28 curity Administration and transportation stakeholders, the Adminis-
29 trator shall develop and issue behavioral standards, medical standards,
30 and technical standards, based on the recommendations of the working
31 group under subsection (b), that a third party explosives detection ca-
32 nine must satisfy to be certified for the screening of individuals and
33 property, including detection of explosive vapors among individuals and
34 articles of property, in public areas of an airport under section 44901
35 of title 49.

36 (2) AUGMENTING PUBLIC AREA SECURITY.—

37 (A) IN GENERAL.—The Administrator shall develop guidance on
38 the coordination of development and deployment of explosives de-
39 tection canine teams for use by transportation stakeholders to en-
40 hance public area security at transportation hubs, including air-
41 ports.

1 (B) CONSULTATION.—In developing the guidance under sub-
2 paragraph (A), the Administrator shall consult with—

- 3 (i) the working group established under subsection (b);
4 (ii) the officials responsible for carrying out subsection (e);
5 and
6 (iii) such transportation stakeholders, canine providers, law
7 enforcement, privacy groups, and transportation security pro-
8 viders as the Administrator considers relevant.

9 (3) AGREEMENT TO TEST AND CERTIFY CAPABILITIES OF CA-
10 NINES.—Subject to paragraphs (4), (5), and (6), not later than 270
11 days after the issuance of standards under paragraph (1), the Adminis-
12 trator shall, to the extent possible, enter into an agreement with at
13 least 1 third party to test and certify the capabilities of canines in ac-
14 cordance with the standards under paragraph (1).

15 (4) EXPEDITED DEPLOYMENT.—In entering into an agreement
16 under paragraph (3), the Administrator shall use—

- 17 (A) other transaction authority under section 11508 of this
18 title; or
19 (B) such other authority of the Administrator as the Adminis-
20 trator considers appropriate to expedite the deployment of addi-
21 tional canine teams.

22 (5) PROCESS.—Before entering into an agreement under paragraph
23 (3), the Administrator shall—

- 24 (A) evaluate and verify the third party's ability to effectively
25 evaluate the capabilities of canines;
26 (B) designate key elements required for appropriate evaluation
27 venues where third parties may conduct testing; and
28 (C) periodically assess the program at evaluation centers to en-
29 sure the proficiency of the canines beyond the initial testing and
30 certification by the third party.

31 (6) CONSULTATION.—To determine best practices for the use of
32 third parties to test and certify the capabilities of canines, the Adminis-
33 trator shall consult with the following persons before entering into an
34 agreement under paragraph (3):

- 35 (A) The Secretary of State.
36 (B) The Secretary of Defense.
37 (C) Non-profit organizations that train, certify, and provide the
38 services of canines for various purposes.
39 (D) Institutions of higher education with research programs re-
40 lated to use of canines for the screening of individuals and prop-

1 erty, including detection of explosive vapors among individuals and
2 articles of property.

3 (7) THIRD PARTY EXPLOSIVES DETECTION CANINE PROVIDER
4 LIST.—

5 (A) DEVELOPMENT AND MAINTENANCE.—Not later than 90
6 days after the date on which the Administrator enters into an
7 agreement under paragraph (3), the Administrator shall develop
8 and maintain a list of the names of each third party from which
9 the Transportation Security Administration procures explosive de-
10 tection canines, including for each third party the relevant con-
11 tractual period of performance.

12 (B) DISTRIBUTION.—The Administrator shall make the list
13 under subparagraph (A) available to appropriate transportation
14 stakeholders in such form and manner as the Administrator pre-
15 scribes.

16 (8) OVERSIGHT.—The Administrator shall establish a process to en-
17 sure appropriate oversight of the certification program and compliance
18 with the standards under paragraph (1), including periodic audits of
19 participating third parties.

20 (9) DEVELOPMENT AND IMPLEMENTATION OF PROCUREMENT PROC-
21 ESS.—The Administrator shall develop and implement a process for the
22 Transportation Security Administration to procure third party explo-
23 sives detection canines certified under this section.

24 (d) DEPLOYMENT TO AUGMENT PUBLIC AREA AT AIRPORT.—

25 (1) DEFINITIONS.—In this subsection:

26 (A) APPLICABLE LARGE HUB AIRPORT.—The term “applicable
27 large hub airport” means a large hub airport (as defined in sec-
28 tion 40102 of title 49) that has less than 100 percent of the allo-
29 cated passenger screening canine teams staffed by the Transpor-
30 tation Security Administration.

31 (B) AVIATION STAKEHOLDER.—The term “aviation stake-
32 holder” includes an airport, airport operator, and air carrier.

33 (2) AUTHORIZATION OF AVIATION STAKEHOLDER.—The Adminis-
34 trator shall authorize an aviation stakeholder, under the oversight of
35 and in coordination with the Federal Security Director at an applicable
36 airport, to contract with, procure or purchase, and deploy one or more
37 third party explosives detection canines certified under this section to
38 augment public area security at that airport.

39 (3) APPLICABLE LARGE HUB AIRPORTS.—

40 (A) PROVISION OF CERTIFIED CANINE FOR DEPLOYMENT.—Ex-
41 cept as provided under subparagraph (B), notwithstanding any

1 law to the contrary, and subject to the other provisions of this
2 paragraph and paragraph (2), an applicable large hub airport may
3 provide a certified canine described in paragraph (2) on an in-kind
4 basis to the Transportation Security Administration to be deployed
5 as a passenger screening canine at that airport unless the applica-
6 ble large hub airport consents to the use of that certified canine
7 elsewhere.

8 (B) EXCEPTION.—The Administrator may, on a case-by-case
9 basis, deploy a certified canine described in paragraph (2) to a
10 transportation facility other than the applicable large hub airport
11 described in subparagraph (A) for not more than 90 days per year
12 if the Administrator—

13 (i) determines that the deployment is necessary to meet
14 operational or security needs; and

15 (ii) notifies the applicable large hub airport described in
16 subparagraph (A).

17 (C) NONEMPLOYABLE CANINES.—A certified canine provided to
18 the Transportation Security Administration under subparagraph
19 (A) that does not complete training for deployment under subpara-
20 graph (A) shall be the responsibility of the large hub airport un-
21 less the Transportation Security Administration agrees to a dif-
22 ferent outcome.

23 (4) HANDLERS.—Not later than 30 days before a canine begins
24 training to become a certified canine under paragraph (3), the airport
25 shall notify the Transportation Security Administration of the training
26 and the Administrator shall assign a Transportation Security Adminis-
27 tration canine handler to participate in the training with that canine,
28 as appropriate.

29 (5) LIMITATION ON REDUCING STAFFING ALLOCATION MODEL.—The
30 Administrator may not reduce the staffing allocation model for an ap-
31 plicable large hub airport based on that airport's provision of a cer-
32 tified canine under this paragraph or paragraph (2).

33 (e) THIRD PARTY CANINE TEAMS FOR AIR CARGO SECURITY.—

34 (1) DEFINITIONS.—In this subsection:

35 (A) AIR CARRIER.—The term “air carrier” has the meaning
36 given the term in section 40102 of title 49.

37 (B) FOREIGN AIR CARRIER.—The term “foreign air carrier” has
38 the meaning given the term in section 40102 of title 49.

39 (C) THIRD PARTY EXPLOSIVES DETECTION CANINE ASSET.—
40 The term “third party explosives detection canine asset” means an

1 explosives detection canine or handler not owned or employed, re-
2 spectively, by the Transportation Security Administration.

3 (2) IN GENERAL.—To enhance the screening of air cargo and ensure
4 that third party explosives detection canine assets are leveraged for
5 that purpose, the Administrator shall, not later than 180 days after
6 October 5, 2018—

7 (A) develop and issue standards for the use of the third party
8 explosives detection canine assets for the primary screening of air
9 cargo;

10 (B) develop a process to identify qualified non-Federal entities
11 that will certify canine assets that meet the standards established
12 by the Administrator under subparagraph (A);

13 (C) ensure that entities qualified to certify canine assets shall
14 be independent from entities that will train and provide canines
15 to end users of the canine assets;

16 (D) establish a system of Transportation Security Administra-
17 tion audits of the process developed under subparagraph (B); and

18 (E) provide that canines certified for the primary screening of
19 air cargo can be used by air carriers, foreign air carriers, freight
20 forwarders, and shippers.

21 (3) IMPLEMENTATION.—Beginning on the date that the development
22 of the process under paragraph (2)(B) is complete, the Administrator
23 shall—

24 (A) facilitate the deployment of the assets that meet the certifi-
25 cation standards of the Administration, as determined by the Ad-
26 ministrator;

27 (B) make the standards available to vendors seeking to train
28 and deploy third party explosives detection canine assets; and

29 (C) ensure that all costs for the training and certification of ca-
30 nines, and for the use of supplied canines, are borne by private
31 industry and not the Federal Government.

32 **§ 40318. Voluntary use of credentialing**

33 (a) DEFINITIONS.—In this section:

34 (1) APPLICABLE INDIVIDUAL WHO IS SUBJECT TO CREDENTIALING
35 OR A BACKGROUND INVESTIGATION.—The term “applicable individual
36 who is subject to credentialing or a background investigation” means
37 only an individual who—

38 (A) because of employment is regulated by the Transportation
39 Security Administration, Department of Transportation, or Coast
40 Guard and is required to have a background records check to ob-

1 tain a hazardous materials endorsement on a commercial driver's
2 license issued by a State under section 5103a of title 49; or

3 (B) is required to have a credential and background records
4 check under section 10862(d)(2) of this title at a facility with ac-
5 tivities that are regulated by the Transportation Security Adminis-
6 tration, Department of Transportation, or Coast Guard.

7 (2) VALID TRANSPORTATION SECURITY CARD.—The term “valid
8 transportation security card” means a transportation security card that
9 is—

10 (A) issued under section 70105 of title 46;

11 (B) not expired;

12 (C) shows no signs of tampering; and

13 (D) bears a photograph of the individual representing the card.

14 (b) SATISFY REQUIREMENT.—An applicable individual who is subject to
15 credentialing or a background investigation may satisfy that requirement by
16 obtaining a valid transportation security card.

17 (c) ISSUANCE OF CARDS.—The Secretary—

18 (1) shall expand the transportation security card program, consistent
19 with section 70105 of title 46, to allow an applicable individual who
20 is subject to credentialing or a background investigation to apply for
21 a transportation security card; and

22 (2) may charge reasonable fees, in accordance with section 10398(a)
23 of this title, for providing the necessary credentialing and background
24 investigation.

25 (d) VETTING.—The Administrator shall develop and implement a plan to
26 utilize, in addition to any background check required for initial issue, the
27 Federal Bureau of Investigation's Rap Back Service and other vetting tools
28 as appropriate, including the No-Fly and Selectee lists, to get immediate no-
29 tification of any criminal activity relating to any person with a valid trans-
30 portation security card.

31 **§ 40319. Biometrics expansion**

32 (a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this
33 section, the term “appropriate committees of Congress” means—

34 (1) the Committee on Commerce, Science, and Transportation of the
35 Senate;

36 (2) the Committee on Homeland Security and Governmental Affairs
37 of the Senate; and

38 (3) the Committee on Homeland Security of the House of Represent-
39 atives.

1 (b) CONSULTATION.—The Administrator and the Commissioner of U.S.
2 Customs and Border Protection shall consult with each other on the deploy-
3 ment of biometric technologies.

4 (c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed
5 to permit the Commissioner of U.S. Customs and Border Protection to fa-
6 cilitate or expand the deployment of biometric technologies, or otherwise col-
7 lect, use, or retain biometrics, not authorized by a provision of this chapter
8 or a provision of or amendment made by the Intelligence Reform and Ter-
9 rorism Prevention Act of 2004 (Public Law 108–458, 118 Stat. 3638) or
10 the Implementing Recommendations of the 9/11 Commission Act of 2007
11 (Public Law 110–53, 121 Stat. 266).

12 (d) REPORT REQUIRED.—Not later than 270 days after October 5, 2018,
13 the Secretary shall submit to the appropriate committees of Congress, and
14 to any Member of Congress on request of that Member, a report that in-
15 cludes specific assessments from the Administrator and the Commissioner
16 of U.S. Customs and Border Protection with respect to the following:

17 (1) The operational and security impact of using biometric tech-
18 nology to identify travelers.

19 (2) The potential effects on privacy of the expansion of the use of
20 biometric technology under paragraph (1), including methods proposed
21 or implemented to mitigate any risks to privacy identified by the Ad-
22 ministrator or the Commissioner related to the active or passive collec-
23 tion of biometric data.

24 (3) Methods to analyze and address any matching performance er-
25 rors related to race, gender, or age identified by the Administrator with
26 respect to the use of biometric technology, including the deployment of
27 facial recognition technology.

28 (4) With respect to the biometric entry-exit program, the following:

29 (A) Assessments of—

30 (i) the error rates, including the rates of false positives and
31 false negatives, and accuracy of biometric technologies;

32 (ii) the effects of biometric technologies, to ensure that the
33 technologies do not unduly burden categories of travelers,
34 such as a certain race, gender, or nationality;

35 (iii) the extent to which and how biometric technologies
36 could address instances of travelers to the United States over-
37 staying their visas, including

38 (I) an estimate of how often biometric matches are
39 contained in an existing database;

1 (II) an estimate of the rate at which travelers using
2 fraudulent credentials identifications are accurately re-
3 jected; and

4 (III) an assessment of what percentage of the detec-
5 tion of fraudulent identifications could have been accom-
6 plished using conventional methods;

7 (iv) the effects on privacy of the use of biometric tech-
8 nologies, including methods to mitigate any risks to privacy
9 identified by the Administrator or the Commissioner of U.S.
10 Customs and Border Protection related to the active or pas-
11 sive collection of biometric data; and

12 (v) the number of individuals who stay in the United States
13 after the expiration of their visas each year.

14 (B) A description of—

15 (i) all audits performed to assess—

16 (I) error rates in the use of biometric technologies; or

17 (II) whether the use of biometric technologies and
18 error rates in the use of the technologies disproportion-
19 ately affect a certain race, gender, or nationality; and

20 (ii) the results of the audits described in clause (i).

21 (C) A description of the process by which domestic travelers are
22 able to opt-out of scanning using biometric technologies.

23 (D) A description of—

24 (i) what traveler data is collected through scanning using
25 biometric technologies, what agencies have access to the data,
26 and how long the agencies possess the data;

27 (ii) specific actions that the Department and other relevant
28 Federal departments and agencies take to safeguard the data;
29 and

30 (iii) a short-term goal for the prompt deletion of the data
31 of individual United States citizens after the data is used to
32 verify traveler identities.

33 (e) PUBLICATION OF ASSESSMENT.—The Secretary, the Administrator,
34 and the Commissioner shall, if practicable, publish a public version of the
35 assessment required by subsection (d)(2) on the websites of the Transpor-
36 tation Security Administration and of U.S. Customs and Border Protection.

37 **§ 40320. Roles of the Department and the Department of**
38 **Transportation**

39 (a) IN GENERAL.—The Secretary is the principal Federal official respon-
40 sible for transportation security.

1 (b) EQUIVALENT ROLES AND RESPONSIBILITIES.—In carrying out this
2 chapter, chapters 401, 405, and 407 of this title, and titles XII through
3 XV of the Implementing Recommendations of the 9/11 Commission Act of
4 2007 (Public Law 110–53, 121 Stat. 381), the roles and responsibilities of
5 the Department and the Department of Transportation are the same as
6 their roles and responsibilities under the following:

7 (1) The Aviation and Transportation Security Act (Public Law 107–
8 71, 115 Stat. 597).

9 (2) The Intelligence Reform and Terrorism Prevention Act of 2004
10 (Public Law 108–458, 118 Stat. 3638).

11 (3) The National Infrastructure Protection Plan required by Home-
12 land Security Presidential Directive–7.

13 (4) The Homeland Security Act of 2002 (Public Law 107–296, 116
14 Stat. 2135).

15 (5) The National Response Plan.

16 (6) Executive Order No. 13416, 71 Fed. Reg. 71033 (Dec. 5, 2006).

17 (7) The Memorandum of Understanding between the Department of
18 Homeland Security and the Department of Transportation on Roles
19 and Responsibilities, dated September 28, 2004, and any and all subse-
20 quent annexes to this Memorandum of Understanding and other rel-
21 evant agreements between the two Departments.

22 **§ 40321. Integrated and unified operations centers**

23 (a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this
24 section, the term “appropriate committees of Congress” means—

25 (1) the Committee on Commerce, Science, and Transportation of the
26 Senate;

27 (2) the Committee on Homeland Security and Governmental Affairs
28 of the Senate; and

29 (3) the Committee on Homeland Security of the House of Represent-
30 atives.

31 (b) FRAMEWORK FOR ESTABLISHING OPERATIONS CENTERS.—Not later
32 than 120 days after October 5, 2018, the Administrator, in consultation
33 with the heads of other appropriate offices or components of the Depart-
34 ment, shall make available to public and private stakeholders a framework
35 for establishing an integrated and unified operations center responsible for
36 overseeing daily operations of a transportation facility that promotes coordi-
37 nation for responses to terrorism, serious incidents, and other purposes, as
38 determined appropriate by the Administrator.

39 (c) REPORT.—Not later than 1 year after October 5, 2018, the Adminis-
40 trator shall brief the appropriate committees of Congress regarding the es-
41 tablishment and activities of integrated and unified operations centers at

1 transportation facilities at which the Transportation Security Administra-
2 tion has a presence.

3 **§ 40322. Security awareness program**

4 (a) DEFINITION OF FRONTLINE EMPLOYEE.—In this section, the term
5 “frontline employee” includes—

6 (1) an employee of a public transportation agency who is a transit
7 vehicle driver or operator, dispatcher, maintenance or maintenance sup-
8 port employee, security employee, or transit police employee, or any
9 other employee who has direct contact with riders on a regular basis,
10 and any other employee of a public transportation agency who the Ad-
11 ministrator determines should receive security training under this sec-
12 tion or who is receiving security training under other law;

13 (2) over-the-road bus drivers, security personnel, dispatchers, main-
14 tenance and maintenance support personnel, ticket agents, other ter-
15 minal employees, and other employees of an over-the-road bus operator
16 or terminal owner or operator who the Administrator determines should
17 receive security training under this section or who are receiving secu-
18 rity training under other law; or

19 (3) security personnel, dispatchers, locomotive engineers, conductors,
20 trainmen, other onboard employees, maintenance and maintenance sup-
21 port personnel, bridge tenders, and other employees of railroad carriers
22 who the Administrator determines should receive security training
23 under this section or who are receiving security training under other
24 law.

25 (b) ESTABLISHMENT.—The Administrator shall establish a program to
26 promote surface transportation security through the training of surface
27 transportation operators and frontline employees on each of the skills identi-
28 fied in subsection (d).

29 (c) APPLICATION.—The program established under subsection (b) shall
30 apply to all modes of surface transportation, including public transportation,
31 rail, highway, motor carrier, and pipeline.

32 (d) TRAINING.—The program established under subsection (b) shall
33 cover, at a minimum, the skills necessary to recognize, assess, and respond
34 to suspicious items or actions that could indicate a threat to transportation.

35 (e) ASSESSMENT.—

36 (1) IN GENERAL.—The Administrator shall conduct an assessment
37 of current training programs for surface transportation operators and
38 frontline employees.

39 (2) CONTENTS.—The assessment shall identify—

40 (A) whether other training is being provided, either voluntarily
41 or in response to other Federal requirements; and

- 1 (B) whether there are any gaps in existing training.
- 2 (f) UPDATES.—The Administrator shall ensure the program established
3 under subsection (b) is updated as necessary to address changes in risk and
4 terrorist methods and to close any gaps identified in the assessment under
5 subsection (e).
- 6 (g) SUSPICIOUS ACTIVITY REPORTING.—
- 7 (1) NATIONAL TELEPHONE NUMBER.—The Secretary shall maintain
8 a national telephone number for an individual to use to report sus-
9 picious activity under this section to the Transportation Security Ad-
10 ministration.
- 11 (2) PROCEDURES.—The Administrator shall establish procedures for
12 the Transportation Security Administration—
- 13 (A) to review and follow-up, as necessary, on each report re-
14 ceived under paragraph (1); and
- 15 (B) to share, as necessary and in accordance with law, the re-
16 port with appropriate Federal, State, local, and tribal entities.
- 17 (3) RULE OF CONSTRUCTION.—Nothing in this section may be con-
18 strued to—
- 19 (A) replace or affect in any way the use of 9–1–1 services in
20 an emergency; or
- 21 (B) replace or affect in any way the security training program
22 requirements specified in sections 1408, 1517, and 1534 of the
23 Implementing Recommendations of the 9/11 Commission Act of
24 2007 (6 U.S.C. 1137, 1167, 1184).

25 **Chapter 405—Public Transportation** 26 **Security**

Sec.

40501. Definitions.
40502. National Strategy for Public Transportation Security.
40503. Security assessments and plans.
40504. Public transportation security improvement grants.
40505. Security exercises.
40506. Security training program for public transportation employees.
40507. Security training program for law enforcement agencies.
40508. Public transportation research and development.
40509. Information sharing.
40510. Reporting requirements.
40511. Public transportation employee protections.
40512. Security background checks of covered individuals for public transportation.
40513. Limitation on fines and civil penalties.

27 **§ 40501. Definitions**

28 In this chapter:

- 29 (1) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term “appro-
30 priate congressional committee” means the Committee on Banking,
31 Housing, and Urban Affairs and the Committee on Homeland Security

1 and Governmental Affairs of the Senate and the Committee on Home-
2 land Security and the Committee on Transportation and Infrastructure
3 of the House.

4 (2) DISADVANTAGED BUSINESS CONCERN.—The term “disadvan-
5 taged business concern” means a small business that is owned and con-
6 trolled by socially and economically disadvantaged individuals as de-
7 fined in part 124, title 13, Code of Federal Regulations.

8 (3) FRONTLINE EMPLOYEE.—The term “frontline employee” means
9 an employee of a public transportation agency who is a transit vehicle
10 driver or operator, dispatcher, maintenance or maintenance support
11 employee, station attendant, customer service employee, security em-
12 ployee, or transit police employee, or any other employee who has direct
13 contact with riders on a regular basis, or any other employee of a pub-
14 lic transportation agency that the Secretary determines should receive
15 security training under section 40506 of this title.

16 (4) PUBLIC TRANSPORTATION AGENCY.—The term “public transpor-
17 tation agency” means a publicly owned operator of public transpor-
18 tation eligible to receive Federal assistance under chapter 53 of title
19 49.

20 **§ 40502. National Strategy for Public Transportation Secu-**
21 **rity**

22 (a) NATIONAL STRATEGY.—Based on the previous and ongoing security
23 assessments conducted by the Department and the Department of Trans-
24 portation, the Secretary, consistent with and as required by section 11514
25 of this title, shall develop and implement the modal plan for public transpor-
26 tation, entitled the “National Strategy for Public Transportation Security”
27 (in this section referred to as the “Strategy”).

28 (b) PURPOSE.—

29 (1) GUIDELINES.—In developing the Strategy, the Secretary shall es-
30 tablish guidelines for public transportation security that—

31 (A) minimize security threats to public transportation systems;

32 and

33 (B) maximize the abilities of public transportation systems to
34 mitigate damage resulting from a terrorist attack or other major
35 incident.

36 (2) ASSESSMENTS AND CONSULTATIONS.—In developing the Strat-
37 egy, the Secretary shall—

38 (A) use established and ongoing public transportation security
39 assessments as the basis of the Strategy; and

40 (B) consult with all relevant stakeholders, including public
41 transportation agencies, nonprofit labor organizations representing

1 public transportation employees, emergency responders, public
2 safety officials, and other relevant parties.

3 (e) CONTENTS.—In the Strategy, the Secretary shall describe prioritized
4 goals, objectives, policies, actions, and schedules to improve the security of
5 public transportation.

6 (d) RESPONSIBILITIES.—The Secretary shall include in the Strategy a de-
7 scription of the roles, responsibilities, and authorities of Federal, State, and
8 local agencies, tribal governments, and appropriate stakeholders. The Strat-
9 egy shall also include—

10 (1) the identification of, and a plan to address, gaps and unneces-
11 sary overlaps in the roles, responsibilities, and authorities of Federal
12 agencies; and

13 (2) a process for coordinating existing or future security strategies
14 and plans for public transportation, including—

15 (A) the National Infrastructure Protection Plan required by
16 Homeland Security Presidential Directive–7;

17 (B) Executive Order No. 13416, 71 Fed. Reg. 71033 (Dec. 5,
18 2006); and

19 (C) the Memorandum of Understanding between the Depart-
20 ment and the Department of Transportation on Roles and Respon-
21 sibilities dated September 28, 2004, and subsequent annexes and
22 agreements.

23 (e) ADEQUACY OF EXISTING PLANS AND STRATEGIES.—In developing the
24 Strategy, the Secretary shall use relevant existing risk assessments and
25 strategies developed by the Department or other Federal agencies, including
26 those developed or implemented under section 11514 of this title or Home-
27 land Security Presidential Directive–7.

28 **§ 40503. Security assessments and plans**

29 (a) PUBLIC TRANSPORTATION SECURITY ASSESSMENTS.—

30 (1) SUBMISSION.—The Administrator of the Federal Transit Admin-
31 istration shall submit all public transportation security assessments and
32 all other relevant information to the Secretary.

33 (2) SECRETARIAL REVIEW.—Not later than 60 days after receiving
34 the submission under paragraph (1), the Secretary shall review and
35 augment the security assessments received, and conduct additional se-
36 curity assessments as necessary to ensure that at a minimum, all high-
37 risk public transportation agencies, as determined by the Secretary, will
38 have a completed security assessment.

39 (3) CONTENT.—The Secretary shall ensure that each completed se-
40 curity assessment includes—

1 (A) identification of critical assets, infrastructure, and systems,
2 and their vulnerabilities; and

3 (B) identification of any other security weaknesses, including
4 weaknesses in emergency response planning and employee train-
5 ing.

6 (b) BUS AND RURAL PUBLIC TRANSPORTATION SYSTEMS.—The Sec-
7 retary shall—

8 (1) conduct security assessments, based on a representative sample,
9 to determine the specific needs of—

10 (A) local bus-only public transportation systems; and

11 (B) public transportation systems that receive funds under sec-
12 tion 5311 of title 49; and

13 (2) make the representative assessments available for use by simi-
14 larly situated systems.

15 (c) SECURITY PLANS.—

16 (1) REQUIREMENT FOR PLAN.—

17 (A) HIGH RISK AGENCIES.—The Secretary shall require public
18 transportation agencies determined by the Secretary to be at high
19 risk for terrorism to develop a comprehensive security plan. The
20 Secretary shall provide technical assistance and guidance to public
21 transportation agencies in preparing and implementing security
22 plans under this section.

23 (B) OTHER AGENCIES.—Subject to subparagraph (C), the Sec-
24 retary may also establish a security program for public transpor-
25 tation agencies not designated high risk by the Secretary, to assist
26 those public transportation agencies that request assistance, in-
27 cluding—

28 (i) guidance to assist agencies in conducting security as-
29 sessments and preparing and implementing security plans;
30 and

31 (ii) a process for the Secretary to review and approve as-
32 sessments and plans, as appropriate.

33 (C) PLAN NOT REQUIRED.—A public transportation agency that
34 has not been designated high risk may not be required to develop
35 a security plan.

36 (2) CONTENT.—The Secretary shall ensure that security plans in-
37 clude, as appropriate—

38 (A) a prioritized list of all items included in the public transpor-
39 tation agency's security assessment that have not yet been ad-
40 dressed;

1 (B) a detailed list of any additional capital and operational im-
2 provements identified by the Department or the public transpor-
3 tation agency and a certification of the public transportation agen-
4 cy's technical capacity for operating and maintaining security
5 equipment that may be identified in the list;

6 (C) specific procedures to be implemented or used by the public
7 transportation agency in response to a terrorist attack, including
8 evacuation and passenger communication plans and appropriate
9 evacuation and communication measures for the elderly and indi-
10 viduals with disabilities;

11 (D) a coordinated response plan that establishes procedures for
12 appropriate interaction with State and local law enforcement agen-
13 cies, emergency responders, and Federal officials in order to co-
14 ordinate security measures and plans for response in the event of
15 a terrorist attack or other major incident;

16 (E) a strategy and timeline for conducting training under sec-
17 tion 40506 of this title;

18 (F) plans for providing redundant and other appropriate backup
19 systems necessary to ensure the continued operation of critical ele-
20 ments of the public transportation system in the event of a ter-
21 rorist attack or other major incident;

22 (G) plans for providing service capabilities throughout the sys-
23 tem in the event of a terrorist attack or other major incident in
24 the city or region that the public transportation system serves;

25 (H) methods to mitigate damage within a public transportation
26 system in case of an attack on the system, including a plan for
27 communication and coordination with emergency responders; and

28 (I) other actions or procedures as the Secretary determines are
29 appropriate to address the security of the public transportation
30 system.

31 (3) REVIEW.—Not later than 6 months after receiving the plans re-
32 quired under this section, the Secretary shall—

33 (A) review each security plan submitted;

34 (B) require the public transportation agency to make any
35 amendments needed to ensure that the plan meets the require-
36 ments of this section; and

37 (C) approve any security plan that meets the requirements of
38 this section.

39 (4) EXEMPTION.—The Secretary may not require a public transpor-
40 tation agency to develop a security plan under paragraph (1) if the
41 agency does not receive a grant under section 40504 of this title.

1 (5) WAIVER.—The Secretary may waive the exemption provided in
2 paragraph (4) to require a public transportation agency to develop a
3 security plan under paragraph (1) in the absence of grant funds under
4 section 40504 of this title if not less than 3 days after making the de-
5 termination the Secretary provides the appropriate congressional com-
6 mittees and the public transportation agency written notification detail-
7 ing the need for the security plan, the reasons grant funding has not
8 been made available, and the reason the agency has been designated
9 high risk.

10 (d) CONSISTENCY WITH OTHER PLANS.—The Secretary shall ensure that
11 the security plans developed by public transportation agencies under this
12 section are consistent with the security assessments developed by the De-
13 partment and the National Strategy for Public Transportation Security de-
14 veloped under section 40502 of this title.

15 (e) UPDATES.—The Secretary annually shall—

16 (1) update the security assessments referred to in subsection (a);

17 (2) update the security improvement priorities required under sub-
18 section (f); and

19 (3) require public transportation agencies to update the security
20 plans required under subsection (e), as appropriate.

21 (f) SECURITY IMPROVEMENT PRIORITIES.—

22 (1) IN GENERAL.—Each fiscal year, the Secretary, after consultation
23 with management and nonprofit employee labor organizations rep-
24 resenting public transportation employees, as appropriate, and with ap-
25 propriate State and local officials, shall utilize the information devel-
26 oped or received in this section to establish security improvement prior-
27 ities unique to each individual public transportation agency that has
28 been assessed.

29 (2) ALLOCATIONS.—The Secretary shall use the security improve-
30 ment priorities established in paragraph (1) as the basis for allocating
31 risk-based grant funds under section 40504 of this title, unless the Sec-
32 retary notifies the appropriate congressional committees that the Sec-
33 retary has determined an adjustment is necessary to respond to an ur-
34 gent threat or other significant national security factors.

35 (g) SHARED FACILITIES.—The Secretary shall encourage the development
36 and implementation of coordinated assessments and security plans to the ex-
37 tent a public transportation agency shares facilities (such as tunnels,
38 bridges, stations, or platforms) with another public transportation agency,
39 a freight or passenger railroad carrier, or over-the-road bus operator that
40 is geographically close or otherwise co-located.

41 (h) NONDISCLOSURE OF INFORMATION.—

1 (1) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this
2 section shall be construed as authorizing the withholding of any infor-
3 mation from Congress.

4 (2) DISCLOSURE OF INDEPENDENTLY FURNISHED INFORMATION.—
5 Nothing in this section shall be construed as affecting any authority
6 or obligation of a Federal agency to disclose any record or information
7 that the Federal agency obtains from a public transportation agency
8 under any other Federal law.

9 (i) DETERMINATION.—In response to a petition by a public transpor-
10 tation agency or at the discretion of the Secretary, the Secretary may recog-
11 nize existing procedures, protocols, and standards of a public transportation
12 agency that the Secretary determines meet all or part of the requirements
13 of this section regarding security assessments or security plans.

14 **§ 40504. Public transportation security improvement grants**

15 (a) SECURITY ASSISTANCE PROGRAM.—

16 (1) IN GENERAL.—The Secretary shall establish a program for mak-
17 ing grants to eligible public transportation agencies for security im-
18 provements described in subsection (b).

19 (2) ELIGIBILITY.—A public transportation agency is eligible for a
20 grant under this section if the Secretary has performed a security as-
21 sessment or the agency has developed a security plan under section
22 40503 of this title. Grant funds shall only be awarded for permissible
23 uses under subsection (b) to—

- 24 (A) address items included in a security assessment; or
25 (B) further a security plan.

26 (b) USES OF FUNDS.—A recipient of a grant under subsection (a) shall
27 use the grant funds for one or more of the following:

28 (1) CAPITAL USES OF FUNDS, INCLUDING—

- 29 (A) tunnel protection systems;
30 (B) perimeter protection systems, including access control, in-
31 stallation of improved lighting, fencing, and barricades;
32 (C) redundant critical operations control systems;
33 (D) chemical, biological, radiological, or explosive detection sys-
34 tems, including the acquisition of canines used for detection;
35 (E) surveillance equipment;
36 (F) communications equipment, including mobile service equip-
37 ment to provide access to wireless Enhanced 911 (E911) emer-
38 gency services in an underground fixed guideway system;
39 (G) emergency response equipment, including personal protec-
40 tive equipment;
41 (H) fire suppression and decontamination equipment;

1 (I) global positioning or tracking and recovery equipment, and
2 other automated-vehicle-locator-type system equipment;

3 (J) evacuation improvements;

4 (K) purchase and placement of bomb-resistant trash cans
5 throughout public transportation facilities, including subway exits,
6 entrances, and tunnels;

7 (L) capital costs associated with security awareness, security
8 preparedness, and security response training, including training
9 under section 40506 of this title and exercises under section
10 40505 of this title;

11 (M) security improvements for public transportation systems,
12 including extensions thereto, in final design or under construction;

13 (N) security improvements for stations and other public trans-
14 portation infrastructure, including stations and other public trans-
15 portation infrastructure owned by State or local governments; and

16 (O) other capital security improvements determined appropriate
17 by the Secretary.

18 (2) OPERATING USES OF FUNDS, INCLUDING—

19 (A) security training and associated backfill, including training
20 under section 40506 of this title and training developed by institu-
21 tions of higher education and by nonprofit employee labor organi-
22 zations, for public transportation employees, including frontline
23 employees;

24 (B) live or simulated exercises under section 40505 of this title;

25 (C) public awareness campaigns for enhanced public transpor-
26 tation security;

27 (D) canine patrols for chemical, radiological, biological, or explo-
28 sives detection;

29 (E) development of security plans under section 40503 of this
30 title;

31 (F) overtime reimbursement including reimbursement of State,
32 local, and tribal governments, for costs for enhanced security per-
33 sonnel during significant national and international public events;

34 (G) operational costs, including reimbursement of State, local,
35 and tribal governments for costs for personnel assigned to full-
36 time or part-time security or counterterrorism duties related to
37 public transportation, provided that this expense totals no more
38 than 10 percent of the total grant funds received by a public
39 transportation agency in any 1 year; and

1 (H) other operational security costs determined appropriate by
2 the Secretary, excluding routine, ongoing personnel costs, other
3 than those set forth in this section.

4 (e) SECRETARY'S RESPONSIBILITIES.—In carrying out the responsibilities
5 under subsection (a), the Secretary shall—

6 (1) determine the requirements for recipients of grants under this
7 section, including application requirements;

8 (2) under subsection (a)(2), select the recipients of grants based
9 solely on risk; and

10 (3) under subsection (b), establish the priorities for which grant
11 funds may be used under this section.

12 (d) DISTRIBUTION OF GRANTS.—The Secretary and the Secretary of
13 Transportation shall determine the most effective and efficient way to dis-
14 tribute grant funds to the recipients of grants determined by the Secretary
15 under subsection (a). Subject to the determination made by the Secretaries,
16 the Secretary may transfer funds to the Secretary of Transportation for the
17 purposes of disbursing funds to the grant recipient.

18 (e) GRANT SUBJECT TO CERTAIN TERMS AND CONDITIONS.—Except as
19 otherwise specifically provided in this section, a grant provided under this
20 section is subject to the terms and conditions applicable to a grant made
21 under section 5307 of title 49, as in effect on January 1, 2007, and other
22 terms and conditions determined necessary by the Secretary.

23 (f) LIMITATION ON USES OF FUNDS.—Grants made under this section
24 may not be used to make any State or local government cost-sharing con-
25 tribution under any other Federal law.

26 (g) ANNUAL REPORTS.—Each recipient of a grant under this section
27 shall report annually to the Secretary on the use of the grant funds.

28 (h) GUIDELINES ON USE OF CONTRACTORS AND SUBCONTRACTORS.—
29 Before the distribution of funds to recipients of grants, the Secretary shall
30 issue guidelines to ensure that, to the extent that recipients of grants under
31 this section use contractors or subcontractors, the recipients shall use small,
32 minority, women-owned, or disadvantaged business concerns as contractors
33 or subcontractors to the extent practicable.

34 (i) COORDINATION WITH STATE HOMELAND SECURITY PLANS.—In es-
35 tablishing security improvement priorities under section 40503 of this title
36 and in awarding grants for capital security improvements and operational
37 security improvements under subsection (b), the Secretary shall act consist-
38 ently with relevant State homeland security plans.

39 (j) MULTISTATE TRANSPORTATION SYSTEMS.—In cases in which a public
40 transportation system operates in more than one State, the Secretary shall
41 give appropriate consideration to the risks of the entire system, including

1 those portions of the States into which the system crosses, in establishing
2 security improvement priorities under section 40503 of this title and in
3 awarding grants for capital security improvements and operational security
4 improvements under subsection (b).

5 (k) CONGRESSIONAL NOTIFICATION.—Not later than 3 days before the
6 award of any grant under this section, the Secretary shall notify simulta-
7 neously the appropriate congressional committees of the intent to award the
8 grant.

9 (l) RETURN OF MISSPENT GRANT FUNDS.—The Secretary shall establish
10 a process to require the return of any misspent grant funds received under
11 this section determined to have been spent for a purpose other than those
12 specified in the grant award.

13 (m) AVAILABILITY OF FUNDS.—

14 (1) IN GENERAL.—Except as provided in paragraph (2), funds pro-
15 vided pursuant to a grant awarded under this section for a use speci-
16 fied in subsection (b) shall remain available for use by a grant recipient
17 for a period of not fewer than 36 months.

18 (2) CERTAIN SECURITY IMPROVEMENTS.—Funds provided pursuant
19 to a grant awarded under this section for a use specified in subpara-
20 graph (M) or (N) of subsection (b)(1) shall remain available for use
21 by a grant recipient for a period of not fewer than 48 months.

22 § 40505. Security exercises

23 (a) IN GENERAL.—The Secretary shall establish a program for con-
24 ducting security exercises for public transportation agencies for the purpose
25 of assessing and improving the capabilities of entities described in sub-
26 section (b) to prevent, prepare for, mitigate against, respond to, and recover
27 from acts of terrorism.

28 (b) COVERED ENTITIES.—Entities to be assessed under the program in-
29 clude—

30 (1) Federal, State, and local agencies and tribal governments;

31 (2) public transportation agencies;

32 (3) governmental and nongovernmental emergency response pro-
33 viders and law enforcement personnel, including transit police; and

34 (4) any other organization or entity that the Secretary determines
35 appropriate.

36 (c) REQUIREMENTS.—The Secretary shall ensure that the program—

37 (1) requires, for public transportation agencies that the Secretary
38 considers appropriate, exercises to be conducted that are—

39 (A) scaled and tailored to the needs of specific public transpor-
40 tation systems, and include taking into account the needs of the
41 elderly and individuals with disabilities;

- 1 (B) live;
2 (C) coordinated with appropriate officials;
3 (D) as realistic as practicable and based on current risk assess-
4 ments, including credible threats, vulnerabilities, and con-
5 sequences;
6 (E) inclusive, as appropriate, of frontline employees and man-
7 agers; and
8 (F) consistent with the National Incident Management System,
9 the National Response Plan, the National Infrastructure Protec-
10 tion Plan, the National Preparedness Guidance, the National Pre-
11 paredness Goal, and other national initiatives of this type;

12 (2) provides that exercises described in paragraph (1) will be—

- 13 (A) evaluated by the Secretary against clear and consistent per-
14 formance measures;
15 (B) assessed by the Secretary to learn best practices, which
16 shall be shared with appropriate Federal, State, local, and tribal
17 officials, governmental and nongovernmental emergency response
18 providers, law enforcement personnel, including railroad and tran-
19 sit police, and appropriate stakeholders; and
20 (C) followed by remedial action by covered entities in response
21 to lessons learned;
22 (3) involves individuals in neighborhoods around the infrastructure
23 of a public transportation system; and
24 (4) assists State, local, and tribal governments and public transpor-
25 tation agencies in designing, implementing, and evaluating exercises
26 that conform to the requirements of paragraph (2).

27 (d) NATIONAL EXERCISE PROGRAM.—The Secretary shall ensure that the
28 exercise program developed under subsection (a) is a component of the na-
29 tional exercise program established under section 20508 of this title.

30 (e) FERRY SYSTEM EXEMPTION.—This section does not apply to a ferry
31 system for which drills are required to be conducted under section 70103
32 of title 46.

33 **§ 40506. Public transportation security training program**

34 (a) APPLICABILITY.—A public transportation agency that receives a grant
35 award under this chapter shall develop and implement a security training
36 program under this section.

37 (b) IN GENERAL.—The Secretary shall develop and issue detailed final
38 regulations for a public transportation security training program to prepare
39 public transportation employees, including frontline employees, for potential
40 security threats and conditions.

1 (c) CONSULTATION.—The Secretary shall develop the final regulations
2 under subsection (b) in consultation with—

3 (1) appropriate law enforcement, fire service, security, and terrorism
4 experts;

5 (2) representatives of public transportation agencies; and

6 (3) nonprofit employee labor organizations representing public trans-
7 portation employees or emergency response personnel.

8 (d) PROGRAM ELEMENTS.—The final regulations developed under sub-
9 section (b) shall require security training programs to include, at a min-
10 imum, elements to address the following:

11 (1) Determination of the seriousness of any occurrence or threat.

12 (2) Crew and passenger communication and coordination.

13 (3) Appropriate responses to defend oneself, including using non-
14 lethal defense devices.

15 (4) Use of personal protective devices and other protective equip-
16 ment.

17 (5) Evacuation procedures for passengers and employees, including
18 individuals with disabilities and the elderly.

19 (6) Training related to behavioral and psychological understanding
20 of, and responses to, terrorist incidents, including the ability to cope
21 with hijacker behavior, and passenger responses.

22 (7) Live situational training exercises regarding various threat condi-
23 tions, including tunnel evacuation procedures.

24 (8) Recognition and reporting of dangerous substances and sus-
25 picious packages, persons, and situations.

26 (9) Understanding of security incident procedures, including proce-
27 dures for communicating with governmental and nongovernmental
28 emergency response providers and for on-scene interaction with emer-
29 gency response providers.

30 (10) Operation and maintenance of security equipment and systems.

31 (11) Other security training activities that the Secretary considers
32 appropriate.

33 (e) REQUIRED PROGRAMS.—

34 (1) DEVELOPMENT AND SUBMISSION TO SECRETARY.—Not later
35 than 90 days after a public transportation agency meets the require-
36 ments under subsection (a), the public transportation agency shall de-
37 velop a security training program in accordance with the regulations
38 developed under subsection (b) and submit the program to the Sec-
39 retary for approval.

40 (2) APPROVAL.—Not later than 60 days after receiving a security
41 training program proposal under this subsection, the Secretary shall

1 approve the program or require the public transportation agency that
2 developed the program to make any revisions to the program that the
3 Secretary determines necessary for the program to meet the require-
4 ments of the regulations. A public transportation agency shall respond
5 to the Secretary's comments within 30 days after receiving them.

6 (3) TRAINING.—Not later than 1 year after the Secretary approves
7 a security training program proposal under this subsection, the public
8 transportation agency that developed the program shall complete the
9 training of all employees covered under the program.

10 (4) UPDATES OF REGULATIONS AND PROGRAM REVISIONS.—The
11 Secretary shall periodically review and update, as appropriate, the
12 training regulations issued under subsection (b) to reflect new or
13 changing security threats. Each public transportation agency shall re-
14 vise its training program accordingly and provide additional training as
15 necessary to its workers within a reasonable time after the regulations
16 are updated.

17 (f) LONG-TERM TRAINING REQUIREMENT.—A public transportation
18 agency required to develop a security training program under this section
19 shall provide routine and ongoing training for employees covered under the
20 program, regardless of whether the public transportation agency receives
21 subsequent grant awards.

22 (g) NATIONAL TRAINING PROGRAM.—The Secretary shall ensure that the
23 training program developed under subsection (a) is a component of the na-
24 tional training program established under section 20508 of this title.

25 (h) FERRY EXEMPTION.—This section shall not apply to a ferry system
26 for which training is required to be conducted under section 70103 of title
27 46.

28 **§ 40507. Security training program for law enforcement**
29 **agencies**

30 (a) DEFINITIONS.—In this section:

31 (1) PUBLIC AND PRIVATE SECTOR STAKEHOLDERS.—The term “pub-
32 lic and private sector stakeholders” has the meaning given the term in
33 section 11516(a).

34 (2) SURFACE TRANSPORTATION ASSET.—The term “surface trans-
35 portation asset” includes facilities, equipment, or systems used to pro-
36 vide transportation services by—

37 (A) a public transportation agency (as the term is defined
38 in section 40501 of this title);

39 (B) a railroad carrier (as the term is defined in section 20102
40 of title 49);

41 (C) an owner or operator of—

1 (i) an entity offering scheduled, fixed-route transportation
2 services by over-the-road bus (as the term is defined in section
3 40701 of this title); or

4 (ii) a bus terminal; or

5 (D) other transportation facilities, equipment, or systems, as de-
6 termined by the Secretary.

7 (3) TARGETED VIOLENCE.—The term “targeted violence” means an
8 incident of violence in which an attacker selected a particular target
9 to inflict mass injury or death with no discernable political or ideolog-
10 ical motivation beyond mass injury or death.

11 (4) TERRORISM.—The term “terrorism” means—

12 (A) domestic terrorism (as the term is defined in section 2331
13 of title 18); and

14 (B) international terrorism (as the term is defined in section
15 2331 of title 18).

16 (b) DEVELOPMENT.—The Secretary, in consultation with public and pri-
17 vate sector stakeholders, may in a manner consistent with the protection of
18 privacy rights, civil rights, and civil liberties, develop, through the Federal
19 Law Enforcement Training Centers, a training program to enhance the pro-
20 tection, preparedness, and response capabilities of law enforcement agencies
21 with respect to threats of terrorism and other threats, including targeted
22 violence, at a surface transportation asset.

23 (c) REQUIREMENTS.—The training program described in subsection (b)
24 that the Secretary may develop shall—

25 (1) be informed by current information regarding tactics used by ter-
26 rorists and others engaging in targeted violence;

27 (2) include tactical instruction tailored to the diverse nature of the
28 surface transportation asset operational environment; and

29 (3) prioritize training officers from law enforcement agencies that
30 are eligible for or receive grants under sections 12703 and 12704 of this
31 title and officers employed by railroad carriers that operate passenger
32 service, including interstate passenger service.

33 (d) REPORT.—If the Secretary develops the training program described
34 in subsection (b), not later than 1 year after the date on which the Sec-
35 retary first implements the program, and annually thereafter during each
36 year the Secretary carries out the program, the Secretary shall submit to
37 the Committee on Homeland Security of the House of Representatives and
38 the Committee on Homeland Security and Governmental Affairs of the Sen-
39 ate a report on the program. Each report shall include, for the year covered
40 by the report—

- 1 (1) a description of the curriculum for the training and any changes
- 2 to the curriculum;
- 3 (2) an identification of any contracts entered into for the develop-
- 4 ment or provision of training under the program;
- 5 (3) information on the law enforcement agencies the personnel of
- 6 which received the training, and for each agency, the number of partici-
- 7 pants; and
- 8 (4) a description of the measures used to ensure the program was
- 9 carried out to provide for protections of privacy rights, civil rights, and
- 10 civil liberties.

11 **§ 40508. Public transportation research and development**

12 (a) ESTABLISHMENT OF RESEARCH AND DEVELOPMENT PROGRAM.—The

13 Secretary shall carry out, through the Homeland Security Advanced Re-

14 search Projects Agency in the Science and Technology Directorate and in

15 consultation with the Transportation Security Administration and the Fed-

16 eral Transit Administration, a research and development program to im-

17 prove the security of transportation systems.

18 (b) AWARDING OF GRANTS AND CONTRACTS.—The Secretary shall award

19 grants or contracts to public or private entities to conduct research and

20 demonstrate technologies and methods to reduce and deter terrorist threats

21 or mitigate damages resulting from terrorist attacks against public trans-

22 portation systems.

23 (c) USE OF FUNDS.—Grants or contracts awarded under this section—

24 (1) shall be coordinated with activities of the Homeland Security Ad-

25 vanced Research Projects Agency; and

26 (2) may be used to—

27 (A) research chemical, biological, radiological, or explosive detec-

28 tion systems that do not significantly impede passenger access;

29 (B) research imaging technologies;

30 (C) conduct product evaluations and testing;

31 (D) improve security and redundancy for critical communica-

32 tions, electrical power, and computer and train control systems;

33 (E) develop technologies for securing tunnels, transit bridges,

34 and aerial structures;

35 (F) research technologies that mitigate damages in the event of

36 a cyberattack; and

37 (G) research other technologies or methods for reducing or de-

38 terring terrorist attacks against public transportation systems, or

39 mitigating damage from attacks.

40 (d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES.—

1 (1) CONSULTATION.—In carrying out research and development
2 projects under this section, the Secretary shall consult with the Chief
3 Privacy Officer of the Department and the Officer for Civil Rights and
4 Civil Liberties of the Department, as appropriate, and in accordance
5 with section 10520 of this title.

6 (2) PRIVACY IMPACT ASSESSMENTS.—In accordance with sections
7 10520 and 11705 of this title, the Chief Privacy Officer shall conduct
8 privacy impact assessments and the Officer for Civil Rights and Civil
9 Liberties shall conduct reviews, as appropriate, for research and devel-
10 opment initiatives developed under this section.

11 (e) REPORTING REQUIREMENT.—Each entity that is awarded a grant or
12 contract under this section shall report annually to the Department on the
13 use of grant or contract funds received under this section to ensure that
14 the awards made are expended in accordance with the purposes of this
15 chapter and the priorities developed by the Secretary.

16 (f) COORDINATION.—The Secretary shall ensure that the research is con-
17 sistent with the priorities established in the National Strategy for Public
18 Transportation Security and is coordinated, to the extent practicable, with
19 other Federal, State, local, tribal, and private-sector public transportation,
20 railroad, commuter railroad, and over-the-road bus research initiatives to le-
21 verage resources and avoid unnecessary duplicative efforts.

22 (g) RETURN OF MISSPENT GRANT OR CONTRACT FUNDS.—If the Sec-
23 retary determines that a grantee or contractor used any portion of the grant
24 or contract funds received under this section for a purpose other than the
25 allowable uses specified under subsection (c), the grantee or contractor shall
26 return that amount to the Treasury.

27 **§ 40509. Information sharing**

28 (a) INTELLIGENCE SHARING.—The Secretary shall ensure that the De-
29 partment of Transportation receives appropriate and timely notification of
30 all credible terrorist threats against public transportation assets in the
31 United States.

32 (b) INFORMATION SHARING AND ANALYSIS CENTER.—

33 (1) AUTHORIZATION.—The Secretary shall provide for the reasonable
34 costs of the Information Sharing and Analysis Center for Public Trans-
35 portation (in this subsection referred to as the “ISAC”).

36 (2) PARTICIPATION.—The Secretary—

37 (A) shall require public transportation agencies that the Sec-
38 retary determines to be at high risk of terrorist attack to partici-
39 pate in the ISAC;

40 (B) shall encourage all other public transportation agencies to
41 participate in the ISAC;

1 (C) shall encourage the participation of nonprofit employee
2 labor organizations representing public transportation employees,
3 as appropriate; and

4 (D) shall not charge a fee for participating in the ISAC.

5 **§ 40510. Reporting requirements**

6 (a) ANNUAL REPORT TO CONGRESS.—

7 (1) IN GENERAL.—Not later than March 31 of each year, the Sec-
8 retary shall submit a report, containing the information described in
9 paragraph (2), to the appropriate congressional committees.

10 (2) CONTENTS.—The report submitted under paragraph (1) shall in-
11 clude—

12 (A) a description of the implementation of this chapter;

13 (B) the amount of funds appropriated to carry out this chapter
14 that have not been expended or obligated;

15 (C) the National Strategy for Public Transportation Security
16 required under section 40502 of this title;

17 (D) an estimate of the cost to implement the National Strategy
18 for Public Transportation Security, which shall break out the ag-
19 gregated total cost of needed capital and operational security im-
20 provements for fiscal years 2008 through 2018; and

21 (E) the state of public transportation security in the United
22 States, which shall include detailing the status of security assess-
23 ments, the progress being made around the country in developing
24 prioritized lists of security improvements necessary to make public
25 transportation facilities and passengers more secure, the progress
26 being made by agencies in developing security plans and how those
27 plans differ from the security assessments, and a prioritized list
28 of security improvements being compiled by other agencies, as well
29 as a random sample of an equal number of large- and small-scale
30 projects currently underway.

31 (3) FORMAT.—The Secretary may submit the report in both classi-
32 fied and redacted formats if the Secretary determines that it is appro-
33 priate or necessary.

34 (b) ANNUAL REPORT TO CHIEF EXECUTIVE OFFICERS.—

35 (1) IN GENERAL.—Not later than March 31 of each year, the Sec-
36 retary shall submit a report to the chief executive officer of each State
37 with a public transportation agency that has received a grant under
38 this chapter.

39 (2) CONTENTS.—The report submitted under paragraph (1) shall
40 specify—

1 (A) the amount of grant funds distributed to each public trans-
2 portation agency; and

3 (B) the use of the grant funds.

4 **§ 40511. Public transportation employee protections**

5 (a) IN GENERAL.—A public transportation agency, a contractor or a sub-
6 contractor of the agency, or an officer or employee of the agency, shall not
7 discharge, demote, suspend, reprimand, or in any other way discriminate
8 against an employee if the discrimination is due, in whole or in part, to the
9 employee's lawful, good faith act done, or perceived by the employer to have
10 been done or about to be done—

11 (1) to provide information, directly cause information to be provided,
12 or otherwise directly assist in any investigation regarding any conduct
13 that the employee reasonably believes constitutes a violation of any
14 Federal law, rule, or regulation relating to public transportation safety
15 or security, or fraud, waste, or abuse of Federal grants or other public
16 funds intended to be used for public transportation safety or security,
17 if the information or assistance is provided to, or an investigation stem-
18 ming from the provided information is conducted by—

19 (A) a Federal, State, or local regulatory or law enforcement
20 agency (including an office of the Inspector General under chapter
21 4 of title 5);

22 (B) a Member of Congress, a committee of Congress, or the
23 Government Accountability Office; or

24 (C) an individual with supervisory authority over the employee,
25 or another individual who has the authority to investigate, dis-
26 cover, or terminate the misconduct;

27 (2) to refuse to violate or assist in the violation of any Federal law,
28 rule, or regulation relating to public transportation safety or security;

29 (3) to file a complaint or directly cause to be brought a proceeding
30 relating to the enforcement of this section or to testify in that pro-
31 ceeding;

32 (4) to cooperate with a safety or security investigation by the Sec-
33 retary of Transportation, the Secretary, or the National Transportation
34 Safety Board; or

35 (5) to furnish information to the Secretary of Transportation, the
36 Secretary, the National Transportation Safety Board, or another Fed-
37 eral, State, or local regulatory or law enforcement agency as to the
38 facts relating to any accident or incident resulting in injury or death
39 to an individual or damage to property occurring in connection with
40 public transportation.

41 (b) HAZARDOUS SAFETY OR SECURITY CONDITIONS.—

1 (1) IN GENERAL.—A public transportation agency, a contractor or
2 a subcontractor of the agency, or an officer or employee of the agency,
3 shall not discharge, demote, suspend, reprimand, or in any other way
4 discriminate against an employee for—

5 (A) reporting a hazardous safety or security condition;

6 (B) refusing to work when confronted by a hazardous safety or
7 security condition related to the performance of the employee's du-
8 ties, if the conditions described in paragraph (2) exist; or

9 (C) refusing to authorize the use of any safety- or security-re-
10 lated equipment, track, or structures, if the employee is respon-
11 sible for the inspection or repair of the equipment, track, or struc-
12 tures, when the employee believes that the equipment, track, or
13 structures are in a hazardous safety or security condition, if the
14 conditions described in paragraph (2) exist.

15 (2) PROTECTED REFUSAL.—A refusal is protected under subpara-
16 graphs (B) and (C) of paragraph (1) if—

17 (A) the refusal is made in good faith and no reasonable alter-
18 native to the refusal is available to the employee;

19 (B) a reasonable individual in the circumstances then con-
20 fronting the employee would conclude that—

21 (i) the hazardous condition presents an imminent danger of
22 death or serious injury; and

23 (ii) the urgency of the situation does not allow sufficient
24 time to eliminate the danger without the refusal; and

25 (C) the employee, where possible, has notified the public trans-
26 portation agency of the existence of the hazardous condition and
27 the intention not to perform further work, or not to authorize the
28 use of the hazardous equipment, track, or structures, unless the
29 condition is corrected immediately or the equipment, track, or
30 structures are repaired properly or replaced.

31 (3) LIMITED APPLICABILITY.—Only paragraph (1)(A) applies to se-
32 curity personnel, including transit police, employed or utilized by a pub-
33 lic transportation agency to protect riders, equipment, assets, or facili-
34 ties.

35 (c) ENFORCEMENT ACTION.—

36 (1) FILING AND NOTIFICATION.—An individual who believes that he
37 or she has been discharged or otherwise discriminated against by a per-
38 son in violation of subsection (a) or (b) may, not later than 180 days
39 after the date on which the violation occurs, file (or have a person file
40 on his or her behalf) a complaint with the Secretary of Labor alleging
41 the discharge or discrimination. On receipt of a complaint filed under

1 this paragraph, the Secretary of Labor shall notify, in writing, the indi-
2 vidual named in the complaint and the individual's employer of the fil-
3 ing of the complaint, the allegations contained in the complaint, the
4 substance of evidence supporting the complaint, and the opportunities
5 that will be afforded to the individual under paragraph (2).

6 (2) INVESTIGATION; PRELIMINARY ORDER.—

7 (A) IN GENERAL.—Not later than 60 days after the date of re-
8 ceipt of a complaint filed under paragraph (1) and after affording
9 the individual named in the complaint an opportunity to submit
10 to the Secretary of Labor a written response to the complaint and
11 an opportunity to meet with a representative of the Secretary of
12 Labor to present statements from witnesses, the Secretary of
13 Labor shall conduct an investigation and determine whether there
14 is reasonable cause to believe that the complaint has merit and no-
15 tify, in writing, the complainant and the person alleged to have
16 committed a violation of subsection (a) or (b) of the Secretary of
17 Labor's findings. If the Secretary of Labor concludes that there
18 is a reasonable cause to believe that a violation of subsection (a)
19 or (b) has occurred, the Secretary of Labor shall accompany the
20 Secretary of Labor's findings with a preliminary order providing
21 the relief prescribed by paragraph (3)(B). Not later than 30 days
22 after the date of notification of findings under this paragraph, ei-
23 ther the person alleged to have committed the violation or the
24 complainant may file objections to the findings or preliminary
25 order, or both, and request a hearing on the record. The filing of
26 objections shall not operate to stay a reinstatement remedy con-
27 tained in the preliminary order. Hearings shall be conducted expe-
28 ditiously. If a hearing is not requested in the 30-day period, the
29 preliminary order shall be deemed a final order that is not subject
30 to judicial review.

31 (B) REQUIREMENTS.—

32 (i) REQUIRED SHOWING BY COMPLAINANT.—The Secretary
33 of Labor shall dismiss a complaint filed under this subsection
34 and shall not conduct an investigation otherwise required
35 under subparagraph (A) unless the complainant makes a
36 prima facie showing that any behavior described in subsection
37 (a) or (b) was a contributing factor in the unfavorable per-
38 sonnel action alleged in the complaint.

39 (ii) SHOWING BY EMPLOYER.—Notwithstanding a finding
40 by the Secretary of Labor that the complainant has made the
41 showing required under clause (i), no investigation otherwise

1 required under paragraph (A) shall be conducted if the em-
2 ployer demonstrates, by clear and convincing evidence, that
3 the employer would have taken the same unfavorable per-
4 sonnel action in the absence of that behavior.

5 (iii) CRITERION FOR DETERMINATION BY SECRETARY OF
6 LABOR.—The Secretary of Labor may determine that a viola-
7 tion of subsection (a) or (b) has occurred only if the com-
8 plainant demonstrates that any behavior described in sub-
9 section (a) or (b) was a contributing factor in the unfavorable
10 personnel action alleged in the complaint.

11 (iv) PROHIBITION.—Relief may not be ordered under para-
12 graph (A) if the employer demonstrates by clear and con-
13 vincing evidence that the employer would have taken the same
14 unfavorable personnel action in the absence of that behavior.

15 (3) FINAL ORDER.—

16 (A) DEADLINE FOR ISSUANCE; SETTLEMENT AGREEMENTS.—
17 Not later than 120 days after the date of conclusion of a hearing
18 under paragraph (2), the Secretary of Labor shall issue a final
19 order providing the relief prescribed by this paragraph or denying
20 the complaint. At any time before issuance of a final order, a pro-
21 ceeding under this subsection may be terminated on the basis of
22 a settlement agreement entered into by the Secretary of Labor,
23 the complainant, and the person alleged to have committed the
24 violation.

25 (B) REMEDY.—If, in response to a complaint filed under para-
26 graph (1), the Secretary of Labor determines that a violation of
27 subsection (a) or (b) has occurred, the Secretary of Labor shall
28 order the person who committed the violation to—

- 29 (i) take affirmative action to abate the violation; and
30 (ii) provide the remedies described in subsection (d).

31 (C) ORDER.—If an order is issued under subparagraph (B), the
32 Secretary of Labor, at the request of the complainant, shall assess
33 against the person against whom the order is issued a sum equal
34 to the aggregate amount of all costs and expenses (including attor-
35 ney and expert witness fees) reasonably incurred, as determined
36 by the Secretary of Labor, by the complainant for, or in connec-
37 tion with, bringing the complaint on which the order was issued.

38 (D) FRIVOLOUS COMPLAINTS.—If the Secretary of Labor finds
39 that a complaint under paragraph (1) is frivolous or has been
40 brought in bad faith, the Secretary of Labor may award to the
41 prevailing employer reasonable attorney fees not exceeding \$1,000.

1 (4) REVIEW.—

2 (A) APPEAL TO COURT OF APPEALS.—A person adversely af-
3 fected or aggrieved by an order issued under paragraph (3) may
4 obtain review of the order in the United States Court of Appeals
5 for the circuit in which the violation, with respect to which the
6 order was issued, allegedly occurred or the circuit in which the
7 complainant resided on the date of the violation. The petition for
8 review must be filed not later than 60 days after the date of the
9 issuance of the final order of the Secretary of Labor. Review shall
10 conform to chapter 7 of title 5. The commencement of proceedings
11 under this subparagraph shall not, unless ordered by the court,
12 operate as a stay of the order.

13 (B) LIMITATION ON COLLATERAL ATTACK.—An order of the
14 Secretary of Labor with respect to which review could have been
15 obtained under subparagraph (A) shall not be subject to judicial
16 review in any criminal or other civil proceeding.

17 (5) ENFORCEMENT OF ORDER BY SECRETARY OF LABOR.—When a
18 person fails to comply with an order issued under paragraph (3), the
19 Secretary of Labor may file a civil action in the United States district
20 court for the district in which the violation was found to occur to en-
21 force the order. In actions brought under this paragraph, the district
22 courts have jurisdiction to grant all appropriate relief including injunc-
23 tive relief and compensatory damages.

24 (6) ENFORCEMENT OF ORDER BY PARTIES.—

25 (A) COMMENCEMENT OF ACTION.—An individual on whose be-
26 half an order was issued under paragraph (3) may commence a
27 civil action against the person to whom the order was issued to
28 require compliance with the order. The appropriate United States
29 district court has jurisdiction, without regard to the amount in
30 controversy or the citizenship of the parties, to enforce the order.

31 (B) ATTORNEY FEES.—The court, in issuing a final order under
32 this paragraph, may award costs of litigation (including reasonable
33 attorney and expert witness fees) to any party when the court de-
34 termines an award is appropriate.

35 (7) DE NOVO REVIEW.—With respect to a complaint under para-
36 graph (1), if the Secretary of Labor has not issued a final decision
37 within 210 days after the filing of the complaint and if the delay is
38 not due to the bad faith of the employee, the employee may bring an
39 original action at law or equity for de novo review in the appropriate
40 district court of the United States, which has jurisdiction over the ac-
41 tion without regard to the amount in controversy, and which action

1 shall, at the request of either party to the action, be tried by the court
2 with a jury. The action shall be governed by the same legal burdens
3 of proof specified in paragraph (2)(B) for review by the Secretary of
4 Labor.

5 (d) REMEDIES.—

6 (1) IN GENERAL.—An employee prevailing in any action under sub-
7 section (c) is entitled to all relief necessary to make the employee
8 whole.

9 (2) DAMAGES.—Relief in an action under subsection (c) (including
10 an action described in subsection (c)(7)) includes—

11 (A) reinstatement with the same seniority status that the em-
12 ployee would have had, but for the discrimination;

13 (B) any backpay, with interest; and

14 (C) compensatory damages, including compensation for any spe-
15 cial damages sustained as a result of the discrimination, including
16 litigation costs, expert witness fees, and reasonable attorney fees.

17 (3) PUNITIVE DAMAGES.—Relief in an action under subsection (c)
18 may include punitive damages in an amount not to exceed \$250,000.

19 (e) ELECTION OF REMEDIES.—An employee may not seek protection
20 under both this section and another provision of law for the same allegedly
21 unlawful act of the public transportation agency.

22 (f) NO PREEMPTION.—Nothing in this section preempts or diminishes
23 any other safeguards against discrimination, demotion, discharge, suspen-
24 sion, threats, harassment, reprimand, retaliation, or other manner of dis-
25 crimination provided by Federal or State law.

26 (g) RIGHTS RETAINED BY EMPLOYEE.—Nothing in this section shall be
27 construed to diminish the rights, privileges, or remedies of an employee
28 under Federal or State law or under a collective bargaining agreement. The
29 rights and remedies in this section may not be waived by an agreement, pol-
30 icy, form, or condition of employment.

31 (h) DISCLOSURE OF IDENTITY.—

32 (1) IN GENERAL.—Except as provided in paragraph (2), or with the
33 written consent of the employee, the Secretary of Transportation or the
34 Secretary may not disclose the name of an employee who has provided
35 information described in subsection (a)(1).

36 (2) EXCEPTION.—The Secretary of Transportation or the Secretary
37 shall disclose to the Attorney General the name of an employee de-
38 scribed in paragraph (1) if the matter is referred to the Attorney Gen-
39 eral for enforcement. The Secretary making the disclosure shall provide
40 reasonable advance notice to the affected employee if disclosure of that
41 individual's identity or identifying information is to occur.

1 (i) PROCESS FOR REPORTING SECURITY PROBLEMS TO THE DEPART-
2 MENT.—

3 (1) ESTABLISHMENT OF PROCESS.—The Secretary shall establish
4 through regulations after an opportunity for notice and comment, and
5 provide information to the public regarding, a process by which a per-
6 son may submit a report to the Secretary regarding public transpor-
7 tation security problems, deficiencies, or vulnerabilities.

8 (2) ACKNOWLEDGMENT OF RECEIPT.—If a report submitted under
9 paragraph (1) identifies the person making the report, the Secretary
10 shall respond promptly to the person and acknowledge receipt of the
11 report.

12 (3) STEPS TO ADDRESS PROBLEM.—The Secretary shall review and
13 consider the information provided in a report submitted under para-
14 graph (1) and shall take appropriate steps to address any problems or
15 deficiencies identified.

16 **§ 40512. Security background checks of covered individuals**
17 **for public transportation**

18 (a) DEFINITIONS.—In this section:

19 (1) COVERED INDIVIDUAL.—The term “covered individual” means
20 an employee of a public transportation agency or a contractor or sub-
21 contractor of a public transportation agency.

22 (2) SECURITY BACKGROUND CHECK.—The term “security back-
23 ground check” means reviewing the following for the purpose of identi-
24 fying an individual who may pose a threat to transportation security,
25 national security, or of terrorism:

26 (A) Relevant criminal history databases.

27 (B) In the case of an alien (as defined in section 101 of the
28 Immigration and Nationality Act (8 U.S.C. 1101)), the relevant
29 databases to determine the status of the alien under the immigra-
30 tion laws of the United States.

31 (C) Other relevant information or databases, as determined by
32 the Secretary.

33 (b) GUIDANCE.—

34 (1) IN GENERAL.—Guidance, recommendations, suggested action
35 items, and other widely disseminated voluntary action items issued by
36 the Secretary to a public transportation agency or a contractor or sub-
37 contractor of a public transportation agency relating to performing a
38 security background check of a covered individual shall contain rec-
39 ommendations on the appropriate scope and application of a security
40 background check, including the time period covered, the types of dis-

1 qualifying offenses, and a redress process for adversely impacted covered
2 individuals consistent with subsections (c) and (d).

3 (2) ADEQUATE REDRESS PROCESS.—If a public transportation agency
4 or a contractor or subcontractor of a public transportation agency
5 performs a security background check on a covered individual to fulfill
6 guidance issued by the Secretary under paragraph (1), the Secretary
7 shall not consider the guidance fulfilled unless an adequate redress
8 process as described in subsection (d) is provided to covered individuals.
9

10 (c) REQUIREMENTS.—If the Secretary issues a rule, regulation, or directive
11 requiring a public transportation agency or contractor or subcontractor
12 of a public transportation agency to perform a security background check
13 of a covered individual, then the Secretary shall prohibit a public transportation
14 agency or contractor or subcontractor of a public transportation
15 agency from making an adverse employment decision, including removal or
16 suspension of the employee, due to the rule, regulation, or directive with respect
17 to a covered individual unless the public transportation agency or contractor or subcontractor
18 of a public transportation agency determines that
19 the covered individual—

20 (1) has been convicted of, has been found not guilty of by reason
21 of insanity, or is under warrant, or indictment for a permanent
22 disqualifying criminal offense listed in part 1572 of title 49, Code of
23 Federal Regulations;

24 (2) was convicted of or found not guilty by reason of insanity of an
25 interim disqualifying criminal offense listed in part 1572 of title 49,
26 Code of Federal Regulations, within 7 years of the date that the public
27 transportation agency or contractor or subcontractor of the public
28 transportation agency performs the security background check; or

29 (3) was incarcerated for an interim disqualifying criminal offense
30 listed in part 1572 of title 49, Code of Federal Regulations, and released
31 from incarceration within 5 years of the date that the public
32 transportation agency or contractor or subcontractor of a public transportation
33 agency performs the security background check.

34 (d) REDRESS PROCESS.—If the Secretary issues a rule, regulation, or directive
35 requiring a public transportation agency or contractor or subcontractor
36 of a public transportation agency to perform a security background
37 check of a covered individual, the Secretary shall—

38 (1) provide an adequate redress process for a covered individual subjected
39 to an adverse employment decision, including removal or suspension
40 of the employee, due to the rule, regulation, or directive that is
41 consistent with the appeals and waiver process established for appli-

1 cants for commercial motor vehicle hazardous materials endorsements
2 and transportation workers at ports, as required by section 70105(c)
3 of title 46; and

4 (2) have the authority to order an appropriate remedy, including re-
5 instatement of the covered individual, should the Secretary determine
6 that a public transportation agency or contractor or subcontractor of
7 a public transportation agency wrongfully made an adverse employment
8 decision regarding a covered individual pursuant to the rule, regulation,
9 or directive.

10 (e) FALSE STATEMENTS.—A public transportation agency or a contractor
11 or subcontractor of a public transportation agency may not knowingly mis-
12 represent to an employee or other relevant person, including an arbiter in-
13 volved in a labor arbitration, the scope, application, or meaning of rules,
14 regulations, directives, or guidance issued by the Secretary related to secu-
15 rity background check requirements for covered individuals when conducting
16 a security background check. The Secretary shall issue a regulation that
17 prohibits a public transportation agency or a contractor or subcontractor of
18 a public transportation agency from knowingly misrepresenting to an em-
19 ployee or other relevant person, including an arbiter involved in a labor arbi-
20 tration, the scope, application, or meaning of rules, regulations, directives,
21 or guidance issued by the Secretary related to security background check
22 requirements for covered individuals when conducting a security background
23 check.

24 (f) RIGHTS AND RESPONSIBILITIES.—Nothing in this section shall be
25 construed to abridge a public transportation agency's or a contractor or
26 subcontractor of a public transportation agency's rights or responsibilities
27 to make adverse employment decisions permitted by other Federal, State,
28 or local laws. Nothing in this section shall be construed to abridge rights
29 and responsibilities of covered individuals, a public transportation agency,
30 or a contractor or subcontractor of a public transportation agency under
31 any other Federal, State, or local laws or collective bargaining agreement.

32 (g) NO PREEMPTION OF FEDERAL OR STATE LAW.—Nothing in this sec-
33 tion shall be construed to preempt a Federal, State, or local law that re-
34 quires criminal history background checks, immigration status checks, or
35 other background checks of covered individuals.

36 (h) STATUTORY CONSTRUCTION.—Nothing in this section shall be con-
37 strued to affect the process for review established under section 70105(c)
38 of title 46, including regulations issued under that section.

39 **§ 40513. Limitation on fines and civil penalties**

40 (a) INSPECTORS.—Surface transportation inspectors shall be prohibited
41 from issuing fines to public transportation agencies for violations of the De-

1 department's regulations or orders except through the process described in
2 subsection (b)

3 (b) CIVIL PENALTIES.—The Secretary shall be prohibited from assessing
4 civil penalties against public transportation agencies for violations of the
5 Department's regulations or orders, except in accordance with the following:

6 (1) VIOLATION OF REGULATION OR ORDER.—In the case of a public
7 transportation agency that is found to be in violation of a regulation
8 or order issued by the Secretary, the Secretary shall seek correction of
9 the violation through a written notice to the public transportation agen-
10 cy and shall give the public transportation agency reasonable oppor-
11 tunity to correct the violation or propose an alternative means of com-
12 pliance acceptable to the Secretary.

13 (2) NO CORRECTION OR PROPOSED ALTERNATIVE COMPLIANCE.—If
14 the public transportation agency does not correct the violation or pro-
15 pose an alternative means of compliance acceptable to the Secretary
16 within a reasonable time period that is specified in the written notice,
17 the Secretary may take an action authorized in chapter 115 of this
18 title.

19 (c) LIMITATION ON SECRETARY.—The Secretary shall not initiate civil
20 enforcement actions for violations of administrative and procedural require-
21 ments pertaining to the application for and expenditure of funds awarded
22 under transportation security grant programs under this chapter.

23 **Chapter 407—Surface Transportation** 24 **Security**

Subchapter I—General

Part A—Definitions

Sec.

40701. Chapter definitions.

Part B—Duties of Secretary

40711. Oversight and grant procedures.

40712. Public awareness and outreach.

40713. Nuclear material and explosive detection technology.

Part C—Duties of Administrator

40721. Definition of appropriate committees of Congress.

40722. Surface Transportation Security Advisory Committee.

40723. Surface transportation security assessment and implementation of risk-based strategy.

40724. Risk-based budgeting and resource allocation.

40725. Transparency.

Subchapter II—Railroad Security

40741. Railroad transportation security risk assessment and National Strategy.

40742. Railroad carrier assessments and plans.

40743. Railroad security assistance.

40744. Systemwide Amtrak security upgrades.

40745. Railroad carrier exercises.

40746. Railroad security training program.

40747. Railroad security research and development.

40748. Railroad tank car security testing.

40749. Security background checks of covered individuals.

40750. International railroad security program.

Subchapter III—Over-the-Road Bus Security

- 40761. Assessments and plans.
- 40762. Assistance.
- 40763. Exercises.
- 40764. Training program.
- 40765. Research and development.

Subchapter IV—Hazardous Material and Pipeline Security

- 40781. Railroad routing of security-sensitive materials.
- 40782. Railroad security-sensitive material tracking.
- 40783. Motor carrier security-sensitive material tracking.
- 40784. Use of transportation security card in hazmat licensing.
- 40785. Pipeline security inspections and enforcement.
- 40786. Pipeline security and incident recovery plan.

Subchapter I—General
Part A—Definitions

§ 40701. Chapter definitions

In this chapter (except part C of this subchapter):

(1) AMTRAK.—The term “Amtrak” means the National Railroad Passenger Corporation.

(2) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term “appropriate congressional committee” means the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House.

(3) DISADVANTAGED BUSINESS CONCERN.—The term “disadvantaged business concern” means a small business that is owned and controlled by socially and economically disadvantaged individuals as defined in part 124, title 13, Code of Federal Regulations.

(4) OVER-THE-ROAD BUS.—The term “over-the-road bus” means a bus characterized by an elevated passenger deck located over a baggage compartment.

(5) OVER-THE-ROAD BUS FRONTLINE EMPLOYEE.—The term “over-the-road bus frontline employee” means an over-the-road bus driver, security employee, dispatcher, maintenance or maintenance support employee, ticket agent, other terminal employee, or any other employee of an over-the-road bus operator or terminal owner or operator that the Secretary determines should receive security training under this title.

(6) RAILROAD.—The term “railroad” has the meaning given the term in section 20102 of title 49.

(7) RAILROAD CARRIER.—The term “railroad carrier” has the meaning given the term in section 20102 of title 49.

(8) RAILROAD FRONTLINE EMPLOYEE.—The term “railroad frontline employee” means a security employee, dispatcher, locomotive engineer, conductor, trainman, other onboard employee, maintenance or maintenance support employee, bridge tender, or any other employee of a rail-

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33

1 road carrier that the Secretary determines should receive security
2 training under this chapter.

3 (9) SECURITY-SENSITIVE MATERIAL.—The term “security-sensitive
4 material” means a material, or a group or class of material, in a par-
5 ticular amount and form that the Secretary, in consultation with the
6 Secretary of Transportation, determines, through a rulemaking with
7 opportunity for public comment, poses a significant risk to national se-
8 curity while being transported in commerce due to the potential use of
9 the material in an act of terrorism. In making a designation, the Sec-
10 retary shall, at a minimum, consider the following:

11 (A) Class 7 radioactive materials.

12 (B) Division 1.1, 1.2, or 1.3 explosives.

13 (C) Materials poisonous or toxic by inhalation, including Divi-
14 sion 2.3 gases and Division 6.1 materials.

15 (D) A select agent or toxin regulated by the Centers for Disease
16 Control and Prevention under part 73 of title 42, Code of Federal
17 Regulations.

18 (10) STATE.—The term “State” means a State, the District of Co-
19 lumbia, Puerto Rico, the Northern Mariana Islands, the Virgin Islands,
20 Guam, American Samoa, and any other territory (including a posses-
21 sion) of the United States.

22 (11) TERRORISM.—The term “terrorism” has the meaning given the
23 term in section 10101 of this title.

24 (12) TRANSPORTATION.—The term “transportation”, as used with
25 respect to an over-the-road bus, means the movement of passengers or
26 property by an over-the-road bus—

27 (A) in the jurisdiction of the United States between a place in
28 a State and a place outside the State (including a place outside
29 the United States); or

30 (B) in a State that affects trade, traffic, and transportation de-
31 scribed in subparagraph (A).

32 (13) UNITED STATES.—The term “United States” means the
33 States, the District of Columbia, Puerto Rico, the Northern Mariana
34 Islands, the Virgin Islands, Guam, American Samoa, and any other ter-
35 ritory (including a possession) of the United States.

36 **Part B—Duties of Secretary**

37 **§ 40711. Oversight and grant procedures**

38 (a) SECRETARIAL OVERSIGHT.—The Secretary, in coordination with the
39 Secretary of Transportation for grants awarded to Amtrak, shall establish
40 necessary procedures, including monitoring and audits, to ensure that
41 grants made under this chapter are expended in accordance with the pur-

1 poses of this chapter and the priorities and other criteria developed by the
2 Secretary.

3 (b) ADDITIONAL AUDITS AND REVIEWS.—The Secretary, and the Sec-
4 retary of Transportation for grants awarded to Amtrak, may award con-
5 tracts to undertake additional audits and reviews of the safety, security,
6 procurement, management, and financial compliance of a recipient of
7 amounts under this chapter.

8 (c) PROCEDURES FOR GRANT AWARD.—The Secretary shall prescribe
9 procedures and schedules for the awarding of grants under this chapter, in-
10 cluding application and qualification procedures, and a record of decision on
11 applicant eligibility. The procedures shall include the execution of a grant
12 agreement between the grant recipient and the Secretary and shall be con-
13 sistent, to the extent practicable, with the grant procedures established
14 under section 70107(i) and (j) of title 46.

15 (d) ADDITIONAL AUTHORITY.—

16 (1) ISSUANCE.—The Secretary may issue non-binding letters of in-
17 tent to recipients of a grant under this chapter, to commit funding
18 from future budget authority of an amount, not more than the Federal
19 Government's share of the project's cost, for a capital improvement
20 project.

21 (2) SCHEDULE.—The letter of intent under this subsection shall es-
22 tablish a schedule under which the Secretary will reimburse the recipi-
23 ent for the Government's share of the project's costs, as amounts be-
24 come available, if the recipient, after the Secretary issues that letter,
25 carries out the project without receiving amounts under a grant issued
26 under this chapter.

27 (3) NOTICE TO SECRETARY.—A recipient that has been issued a let-
28 ter of intent under this section shall notify the Secretary of the recipi-
29 ent's intent to carry out a project before the project begins.

30 (4) NOTICE TO CONGRESS.—The Secretary shall transmit to the ap-
31 propriate congressional committees a written notification at least 5
32 days before the issuance of a letter of intent under this subsection.

33 (5) LIMITATIONS.—A letter of intent issued under this subsection is
34 not an obligation of the Federal Government under section 1501 of
35 title 31, and the letter is not deemed to be an administrative commit-
36 ment for financing. An obligation or administrative commitment may
37 be made only as amounts are provided in authorization and appropria-
38 tions laws.

39 (e) RETURN OF MISSPENT GRANT FUNDS.—As part of the grant agree-
40 ment under subsection (c), the Secretary shall require grant applicants to
41 return misspent grant funds received under this chapter that the Secretary

1 considers to have been spent for a purpose other than one of those specified
2 in the grant award. The Secretary shall take all necessary actions to recover
3 those funds.

4 (f) CONGRESSIONAL NOTIFICATION.—Not later than 5 days before the
5 award of a grant is made under this chapter, the Secretary shall notify the
6 appropriate congressional committees of the intent to award the grant.

7 (g) GUIDELINES.—The Secretary shall ensure, to the extent practicable,
8 that grant recipients under this chapter who use contractors or subcontractors
9 use small, minority, women-owned, or disadvantaged business concerns
10 as contractors or subcontractors when appropriate.

11 **§ 40712. Public awareness and outreach**

12 The Secretary shall implement a national plan for railroad and over-the-
13 road bus security public outreach and awareness. The plan shall—

14 (1) be designed to increase awareness of measures that the general
15 public, passengers, and employees of railroad carriers and over-the-road
16 bus operators can take to increase the security of the national railroad
17 and over-the-road bus transportation systems; and

18 (2) provide outreach to railroad carriers and over-the-road bus oper-
19 ators and their employees to improve their awareness of available tech-
20 nologies, ongoing research and development efforts, and available Fed-
21 eral funding sources to improve security.

22 **§ 40713. Nuclear material and explosive detection tech-** 23 **nology**

24 The Secretary, in coordination with the Director of the National Institute
25 of Standards and Technology and the head of each relevant Federal depart-
26 ment or agency researching nuclear material detection systems or explosive
27 detection systems, shall research, facilitate, and, to the extent practicable,
28 deploy next generation technologies, including active neutron interrogation,
29 to detect nuclear material and explosives in transportation systems and
30 transportation facilities.

31 **Part C—Duties of Administrator**

32 **§ 40721. Definition of appropriate committees of Congress**

33 In this subchapter, the term “appropriate committees of Congress”
34 means—

35 (1) the Committee on Commerce, Science, and Transportation of the
36 Senate;

37 (2) the Committee on Homeland Security and Governmental Affairs
38 of the Senate; and

39 (3) the Committee on Homeland Security of the House of Represent-
40 atives.

1 **§ 40722. Surface Transportation Security Advisory Com-**
2 **mittee**

3 (a) ESTABLISHMENT.—The Administrator shall establish in the Trans-
4 portation Security Administration the Surface Transportation Security Ad-
5 visory Committee (in this section referred to as the “Advisory Committee”).

6 (b) MEMBERSHIP.—

7 (1) IN GENERAL.—The Advisory Committee shall be composed of—

8 (A) voting members appointed by the Administrator under para-
9 graph (2); and

10 (B) nonvoting members, serving in an advisory capacity, who
11 shall be designated by—

12 (i) the Transportation Security Administration;

13 (ii) the Department of Transportation;

14 (iii) the Coast Guard; and

15 (iv) such other Federal department or agency as the Ad-
16 ministrator considers appropriate.

17 (2) APPOINTMENT.—The Administrator shall appoint voting mem-
18 bers from among stakeholders representing each mode of surface trans-
19 portation, such as passenger rail, freight rail, mass transit, pipelines,
20 highways, over-the-road bus, school bus industry, and trucking, includ-
21 ing representatives from—

22 (A) associations representing those modes of surface transpor-
23 tation;

24 (B) labor organizations representing those modes of surface
25 transportation;

26 (C) groups representing the users of those modes of surface
27 transportation, including asset manufacturers, as appropriate;

28 (D) relevant law enforcement, first responders, and security ex-
29 perts; and

30 (E) such other groups as the Administrator considers appro-
31 prium.

32 (3) TERM OF OFFICE.—

33 (A) IN GENERAL.—The term of each voting member of the Ad-
34 visory Committee shall be 2 years, but a voting member may con-
35 tinue to serve until the Administrator appoints a successor.

36 (B) REAPPOINTMENT.—A voting member of the Advisory Com-
37 mittee may be reappointed.

38 (4) CHAIRPERSON.—The Advisory Committee shall select a chair-
39 person from among its voting members.

1 (5) PROHIBITION ON COMPENSATION.—The members of the Advisory
2 Committee shall not receive compensation from the Government by rea-
3 son of their service on the Advisory Committee.

4 (6) REMOVAL.—The Administrator may review the participation of
5 a member of the Advisory Committee and remove the member for cause
6 at any time.

7 (7) VOTING MEMBER ACCESS TO CLASSIFIED AND SENSITIVE SEC-
8 RITY INFORMATION.—

9 (A) DETERMINATIONS.—Not later than 60 days after the date
10 on which a voting member is appointed to the Advisory Committee
11 and before that voting member may be granted any access to clas-
12 sified information or sensitive security information, the Adminis-
13 trator shall determine if the voting member should be restricted
14 from reviewing, discussing, or possessing classified information or
15 sensitive security information.

16 (B) ACCESS.—

17 (i) SENSITIVE SECURITY INFORMATION.—If a voting mem-
18 ber is not restricted from reviewing, discussing, or possessing
19 sensitive security information under subparagraph (A) and
20 voluntarily signs a nondisclosure agreement, the voting mem-
21 ber may be granted access to sensitive security information
22 that is relevant to the voting member's service on the Advi-
23 sory Committee.

24 (ii) CLASSIFIED INFORMATION.—Access to classified mate-
25 rials shall be managed in accordance with Executive Order
26 13526 of December 29, 2009 (75 Fed. Reg. 707), or a subse-
27 quent corresponding Executive order.

28 (C) PROTECTIONS.—

29 (i) SENSITIVE SECURITY INFORMATION.—Voting members
30 shall protect sensitive security information in accordance with
31 part 1520 of title 49, Code of Federal Regulations.

32 (ii) CLASSIFIED INFORMATION.—Voting members shall pro-
33 tect classified information in accordance with the applicable
34 requirements for the particular level of classification.

35 (D) REMOVAL BECAUSE OF RESTRICTED ACCESS.—The Admin-
36 istrator may remove a member of the Advisory Committee whom
37 the Administrator determines should be restricted from reviewing,
38 discussing, or possessing classified information or sensitive secu-
39 rity information under subparagraph (A).

40 (e) Duties.—The Advisory Committee—

1 (1) may advise, consult with, report to, and make recommendations
2 to the Administrator on surface transportation security matters, includ-
3 ing the development, refinement, and implementation of policies, pro-
4 grams, initiatives, rulemakings, and security directives pertaining to
5 surface transportation security; and

6 (2) shall consider risk-based security approaches in the performance
7 of its duties.

8 (d) MEETINGS.—

9 (1) IN GENERAL.—

10 (A) FREQUENCY.—The Administrator shall require the Advisory
11 Committee to meet at least semiannually in person or through web
12 conferencing and may convene additional meetings as necessary.

13 (B) PUBLIC MEETINGS.—At least 1 of the meetings of the Advi-
14 sory Committee each year shall be—

15 (i) announced in the Federal Register;

16 (ii) announced on a public website; and

17 (iii) open to the public.

18 (C) ATTENDANCE.—The Advisory Committee shall maintain a
19 record of the individuals present at each meeting.

20 (D) MINUTES.—

21 (i) IN GENERAL.—Unless otherwise prohibited by other
22 Federal law, minutes of the meetings shall be published on
23 the public website under subsection (g)(5).

24 (ii) PROTECTION OF CLASSIFIED AND SENSITIVE INFORMA-
25 TION.—The Advisory Committee may redact or summarize,
26 as necessary, minutes of the meetings to protect classified or
27 other sensitive information in accordance with law.

28 (2) JOINT COMMITTEE MEETINGS.—The Advisory Committee may
29 meet with 1 or more of the following advisory committees to discuss
30 multimodal security issues and other security-related issues of common
31 concern:

32 (A) The Aviation Security Advisory Committee established
33 under section 40963 of title 49.

34 (B) The Maritime Security Advisory Committee established
35 under section 70112 of title 46.

36 (C) The Railroad Safety Advisory Committee established by the
37 Federal Railroad Administration.

38 (e) SUBJECT MATTER EXPERTS.—The Advisory Committee may request
39 the assistance of subject matter experts with expertise related to the juris-
40 diction of the Advisory Committee.

41 (f) REPORTS.—

1 (1) PERIODIC REPORTS.—The Advisory Committee shall periodically
2 submit reports to the Administrator on matters requested by the Ad-
3 ministrator or by a majority of the members of the Advisory Com-
4 mittee.

5 (2) ANNUAL REPORTS.—

6 (A) SUBMISSION.—The Advisory Committee shall submit to the
7 Administrator and the appropriate congressional committees an
8 annual report that provides information on the activities, findings,
9 and recommendations of the Advisory Committee during the pre-
10 ceding year.

11 (B) PUBLICATION.—Not later than 6 months after the date on
12 which the Administrator receives an annual report under subpara-
13 graph (A), the Administrator shall publish a public version of the
14 report, in accordance with section 552a(b) of title 5.

15 (g) ADMINISTRATOR'S RESPONSE.—

16 (1) CONSIDERATION OF INFORMATION, ADVICE, AND RECOMMENDA-
17 TIONS.—The Administrator shall consider the information, advice, and
18 recommendations of the Advisory Committee in formulating policies,
19 programs, initiatives, rulemakings, and security directives pertaining to
20 surface transportation security.

21 (2) FEEDBACK.—Not later than 90 days after the date on which the
22 Administrator receives a recommendation from the Advisory Committee
23 under subsection (d)(2), the Administrator shall submit to the Advisory
24 Committee written feedback on the recommendation, including—

25 (A) if the Administrator agrees with the recommendation, a
26 plan describing the actions that the Administrator has taken, will
27 take, or recommends that the head of another Federal department
28 or agency take to implement the recommendation; or

29 (B) if the Administrator disagrees with the recommendation, a
30 justification for that determination.

31 (3) NOTIFICATION AND BRIEFING.—Not later than 30 days after the
32 date on which the Administrator submits feedback under paragraph
33 (2), the Administrator shall—

34 (A) notify the appropriate congressional committees of the feed-
35 back, including the determination under subparagraph (A) or (B)
36 of paragraph (2), as applicable; and

37 (B) provide the appropriate congressional committees with a
38 briefing upon request.

39 (4) UPDATES.—Not later than 90 days after the date on which the
40 Administrator receives a recommendation from the Advisory Committee
41 under subsection (f)(2) that the Administrator agrees with, and quar-

1 (A) to develop and implement a cross-cutting, risk-based surface
2 transportation security strategy that includes—

- 3 (i) all surface transportation modes;
4 (ii) a mitigating strategy that aligns with each vulnerability
5 and risk identified in subsection (a);
6 (iii) a planning process to inform resource allocation;
7 (iv) priorities, milestones, and performance metrics to
8 measure the effectiveness of the risk-based surface transpor-
9 tation security strategy; and
10 (v) processes for sharing relevant and timely intelligence
11 threat information with appropriate stakeholders;

12 (B) to develop a management oversight strategy that—

- 13 (i) identifies the parties responsible for the implementation,
14 management, and oversight of the risk-based surface trans-
15 portation security strategy; and
16 (ii) includes a plan for implementing the risk-based surface
17 transportation security strategy; and

18 (C) to modify the risk-based budget and resource allocations, in
19 accordance with section 40724(e) of this title, for the Transpor-
20 tation Security Administration.

21 (2) COORDINATED APPROACH.—In developing and implementing the
22 risk-based surface transportation security strategy under paragraph
23 (1), the Administrator shall coordinate with the heads of other relevant
24 Federal departments or agencies, and stakeholders, as appropriate—

25 (A) to evaluate existing surface transportation security pro-
26 grams, policies, and initiatives, including the explosives detection
27 canine teams, for consistency with the risk-based security strategy
28 and, to the extent practicable, avoid unnecessary duplication of ef-
29 fort;

30 (B) to determine the extent to which stakeholder security pro-
31 grams, policies, and initiatives address the vulnerabilities of, and
32 risks to, surface transportation systems identified in subsection
33 (a); and

34 (C) subject to subparagraph (B), to mitigate each vulnerability
35 and risk to surface transportation systems identified in subsection
36 (a).

37 (e) REPORT.—

38 (1) IN GENERAL.—Not later than 180 days after the date the secu-
39 rity assessment under subsection (a) is complete, the Administrator
40 shall submit to the appropriate committees of Congress and the Inspec-
41 tor General of the Department a report that—

1 (A) describes the process used to complete the security assess-
2 ment;

3 (B) describes the process used to develop the risk-based security
4 strategy;

5 (C) describes the risk-based security strategy;

6 (D) includes the management oversight strategy;

7 (E) includes—

8 (i) the findings of the security assessment;

9 (ii) a description of the actions recommended or taken by
10 the Administrator to mitigate the vulnerabilities and risks
11 identified in subsection (a)(2), including interagency coordina-
12 tion;

13 (iii) recommendations for improving the coordinated ap-
14 proach to mitigating vulnerabilities and risks to surface
15 transportation systems; and

16 (iv) recommended changes to the National Infrastructure
17 Protection Plan, the modal annexes to the National Infra-
18 structure Protection Plan, or relevant surface transportation
19 security programs, policies, or initiatives; and

20 (F) may contain a classified annex.

21 (2) PROTECTIONS AGAINST DISCLOSURE.—In preparing the report,
22 the Administrator shall take appropriate actions to safeguard informa-
23 tion described by section 552(b) of title 5 or protected from disclosure
24 by any other law of the United States.

25 (d) UPDATES.—Not less frequently than semiannually, the Administrator
26 shall report to, or brief, the appropriate committees of Congress on the
27 vulnerabilities of, and risks to, surface transportation systems and how
28 those vulnerabilities and risks affect the risk-based security strategy.

29 **§ 40724. Risk-based budgeting and resource allocation**

30 (a) REPORT.—In conjunction with the submission of the Department's
31 annual budget request to the Office of Management and Budget, the Ad-
32 ministrator shall submit to the appropriate committees of Congress a report
33 that describes a risk-based budget and resource allocation plan for surface
34 transportation sectors, within and across modes, that—

35 (1) reflects the risk-based surface transportation security strategy
36 under section 40723(b) of this title; and

37 (2) is organized by appropriations account, program, project, and
38 initiative.

39 (b) BUDGET TRANSPARENCY.—In submitting the annual budget of the
40 United States Government under section 1105 of title 31, the President

1 shall clearly distinguish the resources requested for surface transportation
2 security from the resources requested for aviation security.

3 (c) RESOURCE REALLOCATION.—

4 (1) IN GENERAL.—Not less than 15 days after the date on which
5 the Transportation Security Administration allocates resources or per-
6 sonnel, including personnel sharing, detailing, or assignment, or the use
7 of facilities, technology systems, or vetting resources, for a nontrans-
8 portation security purpose or National Special Security Event (as de-
9 fined in section 12701 of this title), the Secretary shall provide the no-
10 tification described in paragraph (2) to the appropriate committees of
11 Congress.

12 (2) NOTIFICATION.—A notification described in this paragraph shall
13 include—

14 (A) the reason for, and a justification of, the resource or per-
15 sonnel allocation;

16 (B) the expected end date of the resource or personnel alloca-
17 tion; and

18 (C) the proposed cost to the Transportation Security Adminis-
19 tration of the resource or personnel allocation.

20 (d) FIVE-YEAR CAPITAL INVESTMENT PLAN.—Not later than 180 days
21 after October 5, 2018, the Administrator shall submit to the Committee on
22 Commerce, Science, and Transportation of the Senate and the Committee
23 on Homeland Security of the House of Representatives a 5-year capital in-
24 vestment plan, consistent with the 5-year technology investment plan under
25 section 11542 of this title.

26 **§ 40725. Transparency**

27 (a) REGULATIONS.—

28 (1) PUBLICATION OF STATUS OF REGULATIONS.—Not later than 180
29 days after October 5, 2018, and every 180 days thereafter, the Admin-
30 istrator shall publish on a public website information regarding the sta-
31 tus of each regulation relating to surface transportation security that
32 is directed by law to be issued and that has not been issued if not less
33 than 2 years have passed since the date of enactment of the law.

34 (2) CONTENTS.—Information published under paragraph (1) shall
35 include—

36 (A) an updated rulemaking schedule for the outstanding regula-
37 tion;

38 (B) current staff allocations;

39 (C) data collection or research relating to the development of
40 the rulemaking;

1 (D) current efforts, if any, with security experts, advisory com-
2 mittees, and other stakeholders; and

3 (E) other relevant details associated with the development of the
4 rulemaking that impact the progress of the rulemaking.

5 (b) INSPECTOR GENERAL REVIEW.—Not later than 180 days after Octo-
6 ber 5, 2016, and every 2 years thereafter until all the requirements under
7 this chapter, chapters 401 through 405 of this title, titles XIII, XIV, and
8 XV of the Implementing Recommendations of the 9/11 Commission Act of
9 2007 (Public Law 110–53, 121 Stat. 389, and the TSA Modernization Act
10 (Public Law 115–254, div. K, 132 Stat. 3542) have been fully implemented,
11 the Inspector General of the Department shall submit to the appropriate
12 committees of Congress a report that—

13 (1) identifies the requirements under this chapter, chapters 401
14 through 405 of this title, titles XIII, XIV, and XV of the Implementing
15 Recommendations of the 9/11 Commission Act of 2007 (Public Law
16 110–53, 121 Stat. 389, and the TSA Modernization Act (Public Law
17 115–254, div. K, 132 Stat. 3542) that have not been fully imple-
18 mented;

19 (2) describes what, if any, additional action is necessary; and

20 (3) includes recommendations regarding whether any of the require-
21 ments under this chapter, chapters 401 through 405 of this title, titles
22 XIII, XIV, and XV of the Implementing Recommendations of the 9/
23 11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 389, and
24 the TSA Modernization Act (Public Law 115–254, div. K, 132 Stat.
25 3542) should be amended or repealed.

26 **Subchapter II—Railroad Security**

27 **§ 40741. Railroad transportation security risk assessment** 28 **and National Strategy**

29 (a) RISK ASSESSMENT.—The Secretary shall establish a Federal task
30 force, including the Transportation Security Administration and other agen-
31 cies in the Department, the Department of Transportation, and other ap-
32 propriate Federal agencies, to complete a nationwide risk assessment of a
33 terrorist attack on railroad carriers. The assessment shall include—

34 (1) a methodology for conducting the risk assessment, including
35 timelines, that addresses how the Department will work with the enti-
36 ties described in subsection (c) and make use of existing Federal exper-
37 tise in the Department, the Department of Transportation, and other
38 appropriate agencies;

39 (2) identification and evaluation of critical assets and infrastructure,
40 including tunnels used by railroad carriers in high-threat urban areas;

41 (3) identification of risks to those assets and infrastructure;

1 (4) identification of risks that are specific to the transportation of
2 hazardous materials via railroad;

3 (5) identification of risks to passenger and cargo security, transpor-
4 tation infrastructure protection systems, operations, communications
5 systems, and any other area identified by the assessment;

6 (6) an assessment of employee training and emergency response
7 planning;

8 (7) an assessment of public and private operational recovery plans,
9 taking into account the plans for the maritime sector required under
10 section 70103 of title 46, to expedite, to the maximum extent prac-
11 ticable, the return of an adversely affected railroad transportation sys-
12 tem or facility to its normal performance level after a major terrorist
13 attack or other security event on that system or facility; and

14 (8) an account of actions taken or planned by both public and pri-
15 vate entities to address identified railroad security issues and an as-
16 sessment of the effective integration of the actions.

17 (b) NATIONAL STRATEGY.—

18 (1) REQUIREMENT.—Based upon the assessment conducted under
19 subsection (a), the Secretary, consistent with and as required by sec-
20 tion 11514 of this title, shall develop and implement the modal plan
21 for railroad transportation, entitled the “National Strategy for Rail-
22 road Transportation Security”.

23 (2) CONTENTS.—The modal plan shall include prioritized goals, ac-
24 tions, objectives, policies, mechanisms, and schedules for, at a min-
25 imum—

26 (A) improving the security of railroad tunnels, railroad bridges,
27 railroad switching and car storage areas, other railroad infrastruc-
28 ture and facilities, information systems, and other areas identified
29 by the Secretary as posing significant railroad-related risks to
30 public safety and the movement of interstate commerce, taking
31 into account the impact that a proposed security measure might
32 have on the provision of railroad service or on operations served
33 or otherwise affected by railroad service;

34 (B) deploying equipment and personnel to detect security
35 threats, including those posed by explosives and hazardous chem-
36 ical, biological, and radioactive substances, and appropriate coun-
37 termeasures;

38 (C) consistent with section 40746 of this title, training railroad
39 employees in terrorism prevention, preparedness, passenger evacu-
40 ation, and response activities;

1 (D) conducting public outreach campaigns for railroads regard-
2 ing security, including educational initiatives designed to inform
3 the public on how to prevent, prepare for, respond to, and recover
4 from a terrorist attack on railroad transportation;

5 (E) providing additional railroad security support for railroads
6 at high or severe threat levels of alert;

7 (F) ensuring, in coordination with freight and intercity and
8 commuter passenger railroads, the continued movement of freight
9 and passengers in the event of an attack affecting the railroad sys-
10 tem, including the possibility of rerouting traffic due to the loss
11 of critical infrastructure, such as a bridge, tunnel, yard, or station;

12 (G) coordinating existing and planned railroad security initia-
13 tives undertaken by the public and private sectors;

14 (H) assessing—

15 (i) the usefulness of covert testing of railroad security sys-
16 tems;

17 (ii) the ability to integrate security into infrastructure de-
18 sign; and

19 (iii) the implementation of random searches of passengers
20 and baggage; and

21 (I) identifying the immediate and long-term costs of measures
22 that may be required to address those risks and public- and pri-
23 vate-sector sources to fund the measures.

24 (3) RESPONSIBILITIES.—The Secretary shall include in the modal
25 plan a description of the roles, responsibilities, and authorities of Fed-
26 eral, State, and local agencies, government-sponsored entities, tribal
27 governments, and appropriate stakeholders described in subsection (c).
28 The plan also shall include—

29 (A) the identification of, and a plan to address, gaps and unnec-
30 essary overlaps in the roles, responsibilities, and authorities de-
31 scribed in this paragraph;

32 (B) a methodology for how the Department will work with the
33 entities described in subsection (c), and make use of existing Fed-
34 eral expertise within the Department, the Department of Trans-
35 portation, and other appropriate agencies;

36 (C) a process for facilitating security clearances for the purpose
37 of intelligence and information sharing with the entities described
38 in subsection (c), as appropriate;

39 (D) a strategy and timeline, coordinated with the research and
40 development program established under section 40747 of this title,
41 for the Department, the Department of Transportation, other ap-

1 appropriate Federal agencies, and private entities to research and
2 develop new technologies for securing railroad systems; and

3 (E) a process for coordinating existing or future security strate-
4 gies and plans for railroad transportation, including—

5 (i) the National Infrastructure Protection Plan required by
6 Homeland Security Presidential Directive–7;

7 (ii) Executive Order No. 13416, 71 Fed. Reg. 71033 (Dec.
8 5, 2006); and

9 (iii) the Memorandum of Understanding between the De-
10 partment and the Department of Transportation on Roles
11 and Responsibilities, dated September 28, 2004, subsequent
12 annexes to this Memorandum of Understanding, and other
13 relevant agreements between the two Departments.

14 (c) CONSULTATION WITH STAKEHOLDERS.—In developing the National
15 Strategy required under this section, the Secretary shall consult with rail-
16 road management, nonprofit employee organizations representing railroad
17 employees, owners or lessors of railroad cars used to transport hazardous
18 materials, emergency responders, offerors of security-sensitive materials,
19 public safety officials, and other relevant parties.

20 (d) ADEQUACY OF EXISTING PLANS AND STRATEGIES.—In developing
21 the risk assessment and National Strategy required under this section, the
22 Secretary shall utilize relevant existing plans, strategies, and risk assess-
23 ments developed by the Department or other Federal agencies, including
24 those developed or implemented under section 11514 of this title, or Home-
25 land Security Presidential Directive–7, and, as appropriate, assessments de-
26 veloped by other public and private stakeholders.

27 (e) ANNUAL UPDATES.—Consistent with the requirements of section
28 11514 of this title, the Secretary shall update the assessment and National
29 Strategy each year and transmit a report, which may be submitted in both
30 classified and redacted formats, to the appropriate congressional commit-
31 tees, containing the updated assessment and recommendations.

32 **§ 40742. Railroad carrier assessments and plans**

33 (a) IN GENERAL.—The Secretary shall issue regulations that—

34 (1) require each railroad carrier assigned to a high-risk tier under
35 this section to—

36 (A) conduct a vulnerability assessment under subsections (c)
37 and (d); and

38 (B) prepare, submit to the Secretary for approval, and imple-
39 ment a security plan under this section that addresses security
40 performance requirements; and

- 1 (vii) employee training; and
2 (viii) other matters the Secretary determines appropriate;
3 and

4 (D) identification of redundant and backup systems required to
5 ensure the continued operation of critical elements of a railroad
6 carrier's system in the event of an attack or other incident, includ-
7 ing disruption of commercial electric power or a communications
8 network.

9 (2) THREAT INFORMATION.—The Secretary shall provide in a timely
10 manner to the appropriate employees of a railroad carrier, as des-
11 ignated by the railroad carrier, threat information that is relevant to
12 the carrier when preparing and submitting a vulnerability assessment
13 and security plan, including an assessment of the most likely methods
14 that could be used by terrorists to exploit weaknesses in railroad secu-
15 rity.

16 (e) SECURITY PLANS.—

17 (1) REQUIREMENTS.—The Secretary shall provide technical assist-
18 ance and guidance to railroad carriers in preparing and implementing
19 security plans under this section, and shall require that each security
20 plan of a railroad carrier assigned to a high-risk tier under this section
21 include, as applicable—

22 (A) identification of a security coordinator having authority—

- 23 (i) to implement security actions under the plan;
24 (ii) to coordinate security improvements; and
25 (iii) to receive immediate communications from appropriate

26 Federal officials regarding railroad security;

27 (B) a list of needed capital and operational improvements;

28 (C) procedures to be implemented or used by the railroad car-
29 rier in response to a terrorist attack, including evacuation and
30 passenger communication plans that include individuals with dis-
31 abilities as appropriate;

32 (D) identification of steps taken with State and local law en-
33 forcement agencies, emergency responders, and Federal officials to
34 coordinate security measures and plans for response to a terrorist
35 attack;

36 (E) a strategy and timeline for conducting training under sec-
37 tion 40746 of this title;

38 (F) enhanced security measures to be taken by the railroad car-
39 rier when the Secretary declares a period of heightened security
40 risk;

1 (G) plans for providing redundant and backup systems required
2 to ensure the continued operation of critical elements of the rail-
3 road carrier's system in the event of a terrorist attack or other
4 incident;

5 (H) a strategy for implementing enhanced security for ship-
6 ments of security-sensitive materials, including plans for quickly
7 locating and securing the shipments in the event of a terrorist at-
8 tack or security incident; and

9 (I) other actions or procedures the Secretary determines are ap-
10 propriate to address the security of railroad carriers.

11 (2) SECURITY COORDINATOR REQUIREMENTS.—The Secretary shall
12 require that the individual serving as the security coordinator identified
13 in paragraph (1)(A) is a citizen of the United States. The Secretary
14 may waive this requirement with respect to an individual if the Sec-
15 retary determines that it is appropriate to do so based on a background
16 check of the individual and a review of the consolidated terrorist
17 watchlist.

18 (3) CONSISTENCY WITH OTHER PLANS.—The Secretary shall ensure
19 that the security plans developed by railroad carriers under this section
20 are consistent with the risk assessment and National Strategy for Rail-
21 road Transportation Security developed under section 40741 of this
22 title.

23 (f) DEADLINE FOR REVIEW PROCESS.—Not later than 6 months after re-
24 ceiving the assessments and plans required under this section, the Secretary
25 shall—

26 (1) review each vulnerability assessment and security plan submitted
27 to the Secretary under subsection (c);

28 (2) require amendments to a security plan that does not meet the
29 requirements of this section; and

30 (3) approve a vulnerability assessment or security plan that meets
31 the requirements of this section.

32 (g) TIER ASSIGNMENT.—

33 (1) IN GENERAL.—Utilizing the risk assessment and National Strat-
34 egy for Railroad Transportation Security required under section 40741
35 of this title, the Secretary shall assign each railroad carrier to a risk-
36 based tier established by the Secretary.

37 (2) PROVIDING INFORMATION.—The Secretary may request, and a
38 railroad carrier shall provide, information necessary for the Secretary
39 to assign a railroad carrier to the appropriate tier under this sub-
40 section.

1 (3) NOTIFICATION.—Not later than 60 days after the date a railroad
2 carrier is assigned to a tier under this subsection, the Secretary shall
3 notify the railroad carrier of the tier to which it is assigned and the
4 reasons for the assignment.

5 (4) HIGH-RISK TIERS.—At least one of the tiers established by the
6 Secretary under this subsection shall be designated a tier for high-risk
7 railroad carriers.

8 (5) REASSIGNMENT.—The Secretary may reassign a railroad carrier
9 to another tier, as appropriate, in response to changes in risk. The Sec-
10 retary shall notify the railroad carrier not later than 60 days after the
11 reassignment and provide the railroad carrier with the reasons for the
12 reassignment.

13 (h) NONDISCLOSURE OF INFORMATION.—

14 (1) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this
15 section shall be construed as authorizing the withholding of information
16 from Congress.

17 (2) DISCLOSURE OF INDEPENDENTLY FURNISHED INFORMATION.—
18 Nothing in this section shall be construed as affecting the authority or
19 obligation of a Federal agency to disclose a record or information that
20 the Federal agency obtains from a railroad carrier under another Fed-
21 eral law.

22 (i) EXISTING PROCEDURES, PROTOCOLS, AND STANDARDS.—

23 (1) DETERMINATION.—In response to a petition by a railroad carrier
24 or at the discretion of the Secretary, the Secretary may determine that
25 existing procedures, protocols, and standards meet all or part of the
26 requirements of this section, including regulations issued under sub-
27 section (a), regarding vulnerability assessments and security plans.

28 (2) ELECTION.—Upon review and written determination by the Sec-
29 retary that existing procedures, protocols, or standards of a railroad
30 carrier satisfy the requirements of this section, the railroad carrier may
31 elect to comply with those procedures, protocols, or standards instead
32 of the requirements of this section.

33 (3) PARTIAL APPROVAL.—If the Secretary determines that the exist-
34 ing procedures, protocols, or standards of a railroad carrier satisfy only
35 part of the requirements of this section, the Secretary may accept the
36 submission, but shall require submission by the railroad carrier of addi-
37 tional information relevant to the vulnerability assessment and security
38 plan of the railroad carrier to ensure that the remaining requirements
39 of this section are fulfilled.

40 (4) NOTIFICATION.—If the Secretary determines that particular ex-
41 isting procedures, protocols, or standards of a railroad carrier under

1 this subsection do not satisfy the requirements of this section, the Sec-
2 retary shall provide to the railroad carrier a written notification that
3 includes an explanation of the determination.

4 (5) REVIEW.—Nothing in this subsection shall relieve the Secretary
5 of the obligation—

6 (A) to review the vulnerability assessment and security plan
7 submitted by a railroad carrier under this section; and

8 (B) to approve or disapprove each submission on an individual
9 basis.

10 (j) PERIODIC EVALUATION BY RAILROAD CARRIERS REQUIRED.—

11 (1) SUBMISSION.—Not later than 3 years after the date on which
12 a vulnerability assessment or security plan required to be submitted to
13 the Secretary under subsection (c) is approved, and at least once every
14 5 years after the approval (or on another schedule the Secretary may
15 establish by regulation), a railroad carrier that submitted a vulner-
16 ability assessment and security plan and that is still assigned to the
17 high-risk tier must submit to the Secretary an evaluation of the ade-
18 quacy of the vulnerability assessment and security plan that includes
19 a description of material changes made to the vulnerability assessment
20 or security plan.

21 (2) REVIEW.—Not later than 180 days after the date on which an
22 evaluation is submitted, the Secretary shall review the evaluation and
23 notify the railroad carrier submitting the evaluation of the Secretary's
24 approval or disapproval of the evaluation.

25 (k) SHARED FACILITIES.—The Secretary may permit under this section
26 the development and implementation of coordinated vulnerability assess-
27 ments and security plans to the extent that a railroad carrier shares facili-
28 ties with, or is co-located with, other transportation entities or providers
29 that are required to develop vulnerability assessments and security plans
30 under Federal law.

31 (l) CONSULTATION.—In carrying out this section, the Secretary shall con-
32 sult with railroad carriers, nonprofit employee labor organizations represen-
33 tation railroad employees, and public safety and law enforcement officials.

34 **§ 40743. Railroad security assistance**

35 (a) SECURITY IMPROVEMENT GRANTS.—

36 (1) IN GENERAL.—The Secretary, in consultation with the Adminis-
37 trator of the Transportation Security Administration and other appro-
38 priate agencies or officials, may make grants to railroad carriers, the
39 Alaska Railroad, security-sensitive materials offerors who ship by rail-
40 road, owners of railroad cars used in the transportation of security-sen-
41 sitive materials, State and local governments (for railroad passenger fa-

1 cilities and infrastructure not owned by Amtrak), and Amtrak for
2 intercity passenger railroad and freight railroad security improvements
3 described in subsection (b) as approved by the Secretary.

4 (2) GRANT ELIGIBILITY.—A railroad carrier is eligible for a grant
5 under this section if the carrier has completed a vulnerability assess-
6 ment and developed a security plan that the Secretary has approved
7 under section 40742 of this title.

8 (3) USE OF GRANTS.—A recipient of a grant under this section may
9 use grant funds only for permissible uses under subsection (b) to fur-
10 ther a railroad security plan that meets the requirements of paragraph
11 (2).

12 (4) GRANTS FOR ASSESSMENTS AND PLANS.—Notwithstanding the
13 requirement for eligibility and uses of funds in paragraphs (2) and (3),
14 a railroad carrier is eligible for a grant under this section if the carrier
15 uses the funds solely for the development of assessments or security
16 plans under section 40742 of this title.

17 (b) USES OF FUNDS.—A recipient of a grant under this section shall use
18 the grant funds for one or more of the following:

19 (1) Security and redundancy for critical communications, computer,
20 and train control systems essential for secure railroad operations, in-
21 cluding communication interoperability where appropriate with relevant
22 outside agencies and entities.

23 (2) Accommodation of railroad cargo or passenger security inspection
24 facilities, related infrastructure, and operations at or near United
25 States international borders or other ports of entry.

26 (3) The security of security-sensitive materials transportation by rail-
27 road.

28 (4) Chemical, biological, radiological, or explosive detection, including
29 canine patrols for detection.

30 (5) The security and preparedness of intercity passenger railroad
31 stations, trains, and infrastructure, including security capital improve-
32 ment projects that the Secretary determines enhance railroad station
33 security.

34 (6) Technologies to reduce the vulnerabilities of railroad cars, includ-
35 ing structural modification of railroad cars transporting security-sen-
36 sitive materials to improve their resistance to acts of terrorism.

37 (7) The sharing of intelligence and information about security
38 threats and preparedness, including connectivity to the National Ter-
39 rorist Screening Center.

1 (8) The obtaining of train tracking and communications equipment,
2 including equipment that is interoperable with Federal, State, and local
3 agencies and tribal governments.

4 (9) The hiring, training, and employment of police, security, and pre-
5 paredness officers, including canine units, assigned to full-time security
6 or counterterrorism duties related to railroad transportation.

7 (10) Overtime reimbursement, including reimbursement of State,
8 local, and tribal governments for costs, for enhanced security personnel
9 assigned to duties related to railroad security during periods of high
10 or severe threat levels and National Special Security Events or other
11 periods of heightened security as determined by the Secretary.

12 (11) Perimeter protection systems, including access control, installa-
13 tion of improved lighting, fencing, and barricades at railroad facilities.

14 (12) Tunnel protection systems.

15 (13) Passenger evacuation and evacuation-related capital improve-
16 ments.

17 (14) Railroad security inspection technologies, including verified vis-
18 ual inspection technologies using hand-held readers.

19 (15) Surveillance equipment.

20 (16) Cargo or passenger screening equipment.

21 (17) Emergency response equipment, including fire suppression and
22 decontamination equipment, personal protective equipment, and
23 defibrillators.

24 (18) Operating and capital costs associated with security awareness,
25 preparedness, and response training, including training under section
26 40746 of this title, and training developed by universities, institutions
27 of higher education, and nonprofit employee labor organizations, for
28 railroad employees, including frontline employees.

29 (19) Live or simulated exercises, including exercises described in sec-
30 tion 40745 of this title.

31 (20) Public awareness campaigns for enhanced railroad security.

32 (21) Development of assessments or security plans under section
33 40742 of this title.

34 (22) Other security improvements—

35 (A) identified, required, or recommended under sections 40741
36 and 40742 of this title, including infrastructure, facilities, and
37 equipment upgrades; or

38 (B) that the Secretary considers appropriate.

39 (e) DEPARTMENTAL RESPONSIBILITIES.—In carrying out the responsibil-
40 ities under subsection (a), the Secretary shall—

41 (1) determine the requirements for recipients of grants;

- 1 (2) establish priorities for uses of funds for grant recipients;
- 2 (3) award the funds authorized by this section based on risk, as
3 identified by the plans required under sections 40741 and 40742 of
4 this title;
- 5 (4) take into account whether stations or facilities are used by com-
6 muter railroad passengers as well as intercity railroad passengers in re-
7 viewing grant applications;
- 8 (5) encourage non-Federal financial participation in projects funded
9 by grants; and
- 10 (6) not later than 5 business days after awarding a grant to Amtrak
11 under this section, transfer grant funds to the Secretary of Transpor-
12 tation to be disbursed to Amtrak.
- 13 (d) MULTIYEAR AWARDS.—Grant funds awarded under this section may
14 be awarded for projects that span multiple years.
- 15 (e) LIMITATION ON USES OF FUNDS.—A grant made under this section
16 may not be used to make a State or local government cost-sharing contribu-
17 tion under any other Federal law.
- 18 (f) ANNUAL REPORTS.—Each recipient of a grant under this section shall
19 report annually to the Secretary on the use of grant funds.
- 20 (g) SUBJECT TO CERTAIN STANDARDS.—A recipient of a grant under
21 this section and section 40744 of this title shall be required to comply with
22 the standards of section 24312 of title 49, as in effect on January 1, 2007,
23 with respect to the project, in the same manner as Amtrak is required to
24 comply with the standards for construction work financed under an agree-
25 ment made under section 24308(a) of title 49.

26 **§ 40744. Systemwide Amtrak security upgrades**

- 27 (a) IN GENERAL.—
- 28 (1) GRANTS.—Subject to subsection (b), the Secretary, in consulta-
29 tion with the Administrator of the Transportation Security Administra-
30 tion, may make grants to Amtrak under this section.
- 31 (2) GENERAL PURPOSES.—The Secretary may make grants for the
32 purposes of—
- 33 (A) protecting underwater and underground assets and systems;
- 34 (B) protecting high-risk and high-consequence assets identified
35 through system-wide risk assessments;
- 36 (C) providing counterterrorism or security training;
- 37 (D) providing both visible and unpredictable deterrence; and
- 38 (E) conducting emergency preparedness drills and exercises.
- 39 (3) SPECIFIC PROJECTS.—The Secretary shall make grants—
- 40 (A) to secure major tunnel access points and ensure tunnel in-
41 tegrity in New York, New Jersey, Maryland, and Washington, DC;

- 1 (B) to secure Amtrak trains;
- 2 (C) to secure Amtrak stations;
- 3 (D) to obtain a watchlist identification system approved by the
4 Secretary, or to connect to the National Terrorist Screening Cen-
5 ter watchlist;
- 6 (E) to obtain train tracking and interoperable communications
7 systems that are coordinated with Federal, State, and local agen-
8 cies and tribal governments to the maximum extent possible;
- 9 (F) to hire, train, and employ police and security officers, in-
10 cluding canine units, assigned to full-time security or counterter-
11 rorism duties related to railroad transportation;
- 12 (G) for operating and capital costs associated with security
13 awareness, preparedness, and response training, including training
14 under section 40746 of this title, and training developed by univer-
15 sities, institutions of higher education, and nonprofit employee
16 labor organizations, for railroad employees, including frontline em-
17 ployees;
- 18 (H) for live or simulated exercises, including exercises described
19 in section 40745 of this title;
- 20 (I) for improvements to passenger verification systems;
- 21 (J) for improvements to employee and contractor verification
22 systems, including identity verification technology; and
- 23 (K) for improvements to the security of Amtrak computer sys-
24 tems, including cybersecurity assessments and programs.
- 25 (b) CONDITIONS.—The Secretary shall award grants to Amtrak under
26 this section for projects contained in a system-wide security plan approved
27 by the Secretary developed under section 40742 of this title. Not later than
28 5 business days after awarding a grant to Amtrak under this section, the
29 Secretary shall transfer the grant funds to the Secretary of Transportation
30 to be disbursed to Amtrak.
- 31 (c) EQUITABLE GEOGRAPHIC ALLOCATION.—The Secretary shall ensure
32 that, subject to meeting the highest security needs on Amtrak’s entire sys-
33 tem and consistent with the risk assessment required under section 40741
34 of this title and Amtrak’s vulnerability assessment and security plan devel-
35 oped under section 40742 of this title, stations and facilities located outside
36 of the Northeast Corridor receive an equitable share of the security funds
37 authorized by this section.
- 38 (d) PASSENGER RAIL VETTING.—
- 39 (1) DECISION BY ADMINISTRATOR.—Not later than 180 days after
40 the date on which the Amtrak Board of Directors submits a request
41 to the Administrator, the Administrator shall issue a decision on the

1 use by Amtrak of the Transportation Security Administration's Secure
2 Flight Program or a similar passenger vetting system to enhance pas-
3 senger rail security.

4 (2) CONSIDERATIONS.—In making a decision under paragraph (1),
5 the Administrator shall—

6 (A) consider the technological, privacy, operational, and security
7 impacts of the decision; and

8 (B) describe the impacts in a strategic plan developed under
9 paragraph (3).

10 (3) STRATEGIC PLAN.—If the Administrator decides to grant the re-
11 quest by Amtrak under paragraph (1), the decision shall include a stra-
12 tegic plan for working with rail stakeholders to enhance passenger rail
13 security—

14 (A) by vetting passengers using terrorist watch lists maintained
15 by the Federal Government or a similar passenger vetting system
16 maintained by the Transportation Security Administration; and

17 (B) where applicable and in consultation with the Commissioner
18 of U.S. Customs and Border Protection, by assessing whether the
19 vetting process shall be integrated into preclearance operations es-
20 tablished under section 813 of the Preclearance Authorization Act
21 of 2015 (19 U.S.C. 4432).

22 (4) NOTICE.—

23 (B) IN GENERAL.—The Administrator shall notify the Commit-
24 tees on Commerce, Science, and Transportation and Homeland Se-
25 curity and Governmental Affairs of the Senate and Committee on
26 Homeland Security of the House of Representatives of any deci-
27 sion made under paragraph (1) and the details of the strategic
28 plan under paragraph (3).

29 (5) AUTHORITY OF ADMINISTRATOR NOT LIMITED.—Nothing in this
30 subsection shall be considered to limit the Administrator's authority to
31 set the access to, or the terms and conditions of using, the Secure
32 Flight Program or similar passenger vetting systems.

33 **§ 40745. Railroad carrier exercises**

34 (a) IN GENERAL.—The Secretary shall establish a program for con-
35 ducting security exercises for railroad carriers for the purpose of assessing
36 and improving the capabilities of entities described in subsection (b) to pre-
37 vent, prepare for, mitigate, respond to, and recover from acts of terrorism.

38 (b) COVERED ENTITIES.—Entities to be assessed under the program in-
39 clude—

40 (1) Federal, State, and local agencies and tribal governments;

41 (2) railroad carriers;

1 (3) governmental and nongovernmental emergency response pro-
2 viders, law enforcement agencies, and railroad and transit police, as ap-
3 propriate; and

4 (4) any other organization or entity that the Secretary determines
5 appropriate.

6 (c) REQUIREMENTS.—The Secretary shall ensure that the program—

7 (1) consolidates existing security exercises for railroad carriers ad-
8 ministered by the Department and the Department of Transportation,
9 as jointly determined by the Secretary and the Secretary of Transpor-
10 tation, unless the Secretary waives this consolidation requirement as
11 appropriate;

12 (2) consists of exercises that are—

13 (A) scaled and tailored to the needs of the carrier, including ad-
14 dressing the needs of the elderly and individuals with disabilities;

15 (B) live, in the case of the facilities most at risk to a terrorist
16 attack;

17 (C) coordinated with appropriate officials;

18 (D) as realistic as practicable and based on current risk assess-
19 ments, including credible threats, vulnerabilities, and con-
20 sequences;

21 (E) inclusive, as appropriate, of railroad frontline employees;
22 and

23 (F) consistent with the National Incident Management System,
24 the National Response Plan, the National Infrastructure Protec-
25 tion Plan, the National Preparedness Guidance, the National Pre-
26 paredness Goal, and other national initiatives of this type;

27 (3) provides that exercises described in paragraph (2) will be—

28 (A) evaluated by the Secretary against clear and consistent per-
29 formance measures;

30 (B) assessed by the Secretary to identify best practices, which
31 shall be shared, as appropriate, with railroad carriers, nonprofit
32 employee organizations that represent railroad carrier employees,
33 Federal, State, local, and tribal officials, governmental and non-
34 governmental emergency response providers, law enforcement per-
35 sonnel, including railroad carrier and transit police, and other
36 stakeholders; and

37 (C) used to develop recommendations, as appropriate, from the
38 Secretary to railroad carriers on remedial action to be taken in re-
39 sponse to lessons learned;

40 (4) allows for proper advanced notification of communities and local
41 governments in which exercises are held, as appropriate; and

1 (5) assists State, local, and tribal governments and railroad carriers
2 in designing, implementing, and evaluating additional exercises that
3 conform to the requirements of paragraph (2).

4 (d) NATIONAL EXERCISE PROGRAM.—The Secretary shall ensure that the
5 exercise program developed under subsection (c) is a component of the na-
6 tional exercise program established under section 20508 of this title.

7 **§ 40746. Railroad security training program**

8 (a) IN GENERAL.—The Secretary shall develop and issue regulations for
9 a training program to prepare railroad frontline employees for potential se-
10 curity threats and conditions. The regulations shall take into consideration
11 current security training requirements or best practices.

12 (b) CONSULTATION.—The Secretary shall develop the regulations under
13 subsection (a) in consultation with—

14 (1) appropriate law enforcement, fire service, emergency response,
15 security, and terrorism experts;

16 (2) railroad carriers;

17 (3) railroad shippers; and

18 (4) nonprofit employee labor organizations representing railroad em-
19 ployees or emergency response personnel.

20 (c) PROGRAM ELEMENTS.—The regulations developed under subsection
21 (a) shall require security training programs described in subsection (a) to
22 include, at a minimum, elements to address the following, as applicable:

23 (1) The determination of the seriousness of an occurrence or threat.

24 (2) Crew and passenger communication and coordination.

25 (3) Appropriate responses to defend or protect oneself.

26 (4) The use of personal and other protective equipment.

27 (5) Evacuation procedures for passengers and railroad employees, in-
28 cluding individuals with disabilities and the elderly.

29 (6) The psychology, behavior, and methods of terrorists, including
30 observation and analysis.

31 (7) Training related to psychological responses to terrorist incidents,
32 including the ability to cope with hijacker behavior and passenger re-
33 sponses.

34 (8) Live situational training exercises regarding various threat condi-
35 tions, including tunnel evacuation procedures.

36 (9) The recognition and reporting of dangerous substances, sus-
37 picious packages, and situations.

38 (10) The understanding of security incident procedures, including
39 procedures for communicating with governmental and nongovernmental
40 emergency response providers and for on-scene interaction with emer-
41 gency response providers.

1 (11) The operation and maintenance of security equipment and sys-
2 tems.

3 (12) Other security training activities that the Secretary considers
4 appropriate.

5 (d) SUBMITTING PROGRAM TO SECRETARY FOR APPROVAL.—Each rail-
6 road carrier shall develop a security training program under this section and
7 submit the program to the Secretary for approval. Not later than 60 days
8 after receiving a security training program proposal under this subsection,
9 the Secretary shall approve the program or require the railroad carrier that
10 developed the program to make revisions to the program that the Secretary
11 considers necessary for the program to meet the requirements of this sec-
12 tion. A railroad carrier shall respond to the Secretary's comments within 30
13 days after receiving them.

14 (e) TRAINING.—Not later than 1 year after the Secretary approves a se-
15 curity training program under subsection (d), the railroad carrier that devel-
16 oped the program shall complete the training of all railroad frontline em-
17 ployees who were hired by a carrier more than 30 days preceding the ap-
18 proval date. For employees employed by a carrier for fewer than 30 days
19 preceding the approval date, training shall be completed within the first 60
20 days of employment.

21 (f) UPDATES OF REGULATIONS AND PROGRAM REVISIONS.—The Sec-
22 retary periodically shall review and update as appropriate the training regu-
23 lations issued under subsection (a) to reflect new or changing security
24 threats. Each railroad carrier shall revise its training program accordingly
25 and provide additional training as necessary to its frontline employees with-
26 in a reasonable time after the regulations are updated.

27 (g) PROGRAM COMPONENT OF NATIONAL TRAINING PROGRAM.—The
28 Secretary shall ensure that the training program developed under subsection
29 (a) is a component of the national training program established under sec-
30 tion 20508 of this title.

31 (h) OTHER EMPLOYEES.—The Secretary shall issue guidance and best
32 practices for a railroad shipper employee security program containing the
33 elements listed under subsection (c).

34 **§ 40747. Railroad security research and development**

35 (a) ESTABLISHMENT OF RESEARCH AND DEVELOPMENT PROGRAM.—The
36 Secretary, acting through the Under Secretary for Science and Technology
37 and the Administrator of the Transportation Security Administration, shall
38 carry out a research and development program for the purpose of improving
39 the security of railroad transportation systems.

40 (b) ELIGIBLE PROJECTS.—The research and development program may
41 include projects—

1 (1) to reduce the vulnerability of passenger trains, stations, and
2 equipment to explosives and hazardous chemical, biological, and radio-
3 active substances, including the development of technology to screen
4 passengers in large numbers at peak commuting times with minimal in-
5 terference and disruption;

6 (2) to test new emergency response and recovery techniques and
7 technologies, including those used at international borders;

8 (3) to develop improved railroad security technologies, including—

9 (A) technologies for sealing or modifying railroad tank cars;

10 (B) automatic inspection of railroad cars;

11 (C) communication-based train control systems;

12 (D) emergency response training, including training in a tunnel
13 environment;

14 (E) security and redundancy for critical communications, elec-
15 trical power, computer, and train control systems; and

16 (F) technologies for securing bridges and tunnels;

17 (4) to test wayside detectors that can detect tampering;

18 (5) to support enhanced security for the transportation of security-
19 sensitive materials by railroad;

20 (6) to mitigate damages in the event of a cyberattack; and

21 (7) to address other vulnerabilities and risks identified by the Sec-
22 retary.

23 (c) COORDINATION WITH OTHER RESEARCH INITIATIVES.—The Sec-
24 retary—

25 (1) shall ensure that the research and development program is con-
26 sistent with the National Strategy for Railroad Transportation Security
27 developed under section 40741 of this title and other transportation se-
28 curity research and development programs required by section 30304
29 and chapters 401 through 407 of this title;

30 (2) shall, to the extent practicable, coordinate the research and de-
31 velopment activities of the Department with other ongoing research and
32 development security-related initiatives, including research being con-
33 ducted by—

34 (A) the Department of Transportation, including University
35 Transportation Centers and other institutes, centers, and simula-
36 tors funded by the Department of Transportation;

37 (B) the National Academy of Sciences;

38 (C) the Technical Support Working Group;

39 (D) other Federal departments and agencies; and

40 (E) other Federal and private research laboratories, research
41 entities, and universities and institutions of higher education, in-

1 including Historically Black Colleges and Universities, Hispanic-
2 serving institutions, or Indian tribally controlled colleges and uni-
3 versities;

4 (3) shall carry out a research and development project authorized by
5 this section through a reimbursable agreement with an appropriate
6 Federal agency, if the agency—

7 (A) is currently sponsoring a research and development project
8 in a similar area; or

9 (B) has a unique facility or capability that would be useful in
10 carrying out the project;

11 (4) may award grants to, or enter into cooperative agreements, con-
12 tracts, other transactions, or reimbursable agreements with, the entities
13 described in paragraph (2) and eligible grant recipients under section
14 40743 of this title; and

15 (5) shall make reasonable efforts to enter into memoranda of under-
16 standing, contracts, grants, cooperative agreements, or other trans-
17 actions with railroad carriers willing to contribute both physical space
18 and other resources.

19 (d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES.—

20 (1) CONSULTATION.—In carrying out research and development
21 projects under this section, the Secretary shall consult with the Chief
22 Privacy Officer of the Department and the Officer for Civil Rights and
23 Civil Liberties of the Department as appropriate and under section
24 10520 of this title.

25 (2) PRIVACY IMPACT ASSESSMENTS.—In accordance with sections
26 10520 and 11705 of this title, the Chief Privacy Officer shall conduct
27 privacy impact assessments, and the Officer for Civil Rights and Civil
28 Liberties shall conduct reviews, as appropriate, for research and devel-
29 opment initiatives developed under this section that the Secretary de-
30 termines could have an impact on privacy, civil rights, or civil liberties.

31 **§ 40748. Railroad tank car security testing**

32 (a) VULNERABILITY ASSESSMENT.—

33 (1) LIKELY METHODS AND SUCCESS.—The Secretary shall assess the
34 likely methods of a deliberate terrorist attack against a railroad tank
35 car used to transport toxic-inhalation-hazard materials, and for each
36 method assessed, the degree to which it may be successful in causing
37 death, injury, or serious adverse effects to human health, the environ-
38 ment, critical infrastructure, national security, the national economy, or
39 public welfare.

40 (2) THREATS.—In carrying out paragraph (1), the Secretary shall
41 consider the most current threat information as to likely methods of

1 a successful terrorist attack on a railroad tank car transporting toxic-
2 inhalation-hazard materials, and may consider the following:

3 (A) Explosive devices placed along the tracks or attached to a
4 railroad tank car.

5 (B) The use of missiles, grenades, rockets, mortars, or other
6 high-caliber weapons against a railroad tank car.

7 (3) PHYSICAL TESTING.—In developing the assessment required
8 under paragraph (1), the Secretary shall conduct physical testing of the
9 vulnerability of railroad tank cars used to transport toxic-inhalation-
10 hazard materials to different methods of a deliberate attack, using
11 technical information and criteria to evaluate the structural integrity
12 of railroad tank cars.

13 (b) DISPERSION MODELING.—

14 (1) IN GENERAL.—The Secretary, acting through the National Infra-
15 structure Simulation and Analysis Center, shall conduct an air disper-
16 sion modeling analysis of release scenarios of toxic-inhalation-hazard
17 materials resulting from a terrorist attack on a loaded railroad tank
18 car carrying these materials in urban and rural environments.

19 (2) CONSIDERATIONS.—The analysis under this subsection shall take
20 into account the following considerations:

21 (A) The most likely means of attack and the resulting dispersal
22 rate.

23 (B) Different times of day, to account for differences in cloud
24 coverage and other atmospheric conditions in the environment
25 being modeled.

26 (C) Differences in population size and density.

27 (D) Historically accurate wind speeds, temperatures, and wind
28 directions.

29 (E) Differences in dispersal rates or other relevant factors re-
30 lated to whether a railroad tank car is in motion or stationary.

31 (F) Emergency response procedures by local officials.

32 (G) Other considerations the Secretary believes would develop
33 an accurate, plausible dispersion model for toxic-inhalation-hazard
34 materials released from a railroad tank car as a result of a ter-
35 rorist act.

36 (3) CONSULTATION.—In conducting the dispersion modeling under
37 paragraph (1), the Secretary shall consult with the Secretary of Trans-
38 portation, hazardous materials experts, railroad carriers, nonprofit em-
39 ployee labor organizations representing railroad employees, appropriate
40 State, local, and tribal officials, and other Federal agencies, as appro-
41 priate.

1 (4) INFORMATION SHARING.—On completion of the analysis required
2 under paragraph (1), the Secretary shall share the information devel-
3 oped with the appropriate stakeholders, given appropriate information
4 protection provisions as may be required by the Secretary.

5 **§ 40749. Security background checks of covered individuals**

6 (a) DEFINITIONS.—In this section:

7 (1) COVERED INDIVIDUAL.—The term “covered individual” means
8 an employee of a railroad carrier or a contractor or subcontractor of
9 a railroad carrier.

10 (2) SECURITY BACKGROUND CHECK.—The term “security back-
11 ground check” means for the purpose of identifying individuals who
12 may pose a threat to transportation security or national security, or of
13 terrorism—

14 (A) relevant criminal history databases;

15 (B) in the case of an alien (as defined in section 101 of the Im-
16 migration and Nationality Act (8 U.S.C. 1101)), the relevant
17 databases to determine the status of the alien under the immigra-
18 tion laws of the United States; and

19 (C) other relevant information or databases, as determined by
20 the Secretary.

21 (b) GUIDANCE.—

22 (1) IN GENERAL.—Guidance, recommendations, suggested action
23 items, and other widely disseminated voluntary action items issued by
24 the Secretary to a railroad carrier or a contractor or subcontractor of
25 a railroad carrier relating to performing a security background check
26 of a covered individual shall contain recommendations on the appro-
27 priate scope and application of a security background check, including
28 the time period covered, the types of disqualifying offenses, and a re-
29 dress process for adversely impacted covered individuals consistent with
30 subsections (c) and (d).

31 (2) UPDATE OF EXISTING GUIDANCE.—Guidance, recommendations,
32 suggested action items, and other widely disseminated voluntary action
33 items issued by the Secretary prior to August 3, 2007, to a railroad
34 carrier or a contractor or subcontractor of a railroad carrier relating
35 to performing a security background check of a covered individual shall
36 be updated in compliance with paragraph (1).

37 (3) NECESSARY REDRESS PROCEDURE.—If a railroad carrier or a
38 contractor or subcontractor of a railroad carrier performs a security
39 background check on a covered individual to fulfill guidance issued by
40 the Secretary under paragraph (1) or (2), the Secretary shall not con-

1 sider the guidance fulfilled unless an adequate redress process as de-
2 scribed in subsection (d) is provided to covered individuals.

3 (c) REQUIREMENTS.—If the Secretary issues a rule, regulation, or direc-
4 tive requiring a railroad carrier or contractor or subcontractor of a railroad
5 carrier to perform a security background check of a covered individual, the
6 Secretary shall prohibit the railroad carrier or contractor or subcontractor
7 of a railroad carrier from making an adverse employment decision, including
8 removal or suspension of the covered individual, due to the rule, regulation,
9 or directive with respect to a covered individual unless the railroad carrier
10 or contractor or subcontractor of a railroad carrier determines that the cov-
11 ered individual—

12 (1) has been convicted of, has been found not guilty by reason of
13 insanity, or is under want, warrant, or indictment for a permanent dis-
14 qualifying criminal offense listed in part 1572 of title 49, Code of Fed-
15 eral Regulations;

16 (2) was convicted of or found not guilty by reason of insanity of an
17 interim disqualifying criminal offense listed in part 1572 of title 49,
18 Code of Federal Regulations, within 7 years of the date that the rail-
19 road carrier or contractor or subcontractor of a railroad carrier per-
20 forms the security background check; or

21 (3) was incarcerated for an interim disqualifying criminal offense
22 listed in part 1572 of title 49, Code of Federal Regulations, and re-
23 leased from incarceration within 5 years of the date that the railroad
24 carrier or contractor or subcontractor of a railroad carrier performs the
25 security background check.

26 (d) REDRESS PROCESS.—If the Secretary issues a rule, regulation, or di-
27 rective requiring a railroad carrier or contractor or subcontractor of a rail-
28 road carrier to perform a security background check of a covered individual,
29 the Secretary shall—

30 (1) provide an adequate redress process for a covered individual sub-
31 jected to an adverse employment decision, including removal or suspen-
32 sion of the employee, due to the rule, regulation, or directive that is
33 consistent with the appeals and waiver process established for appli-
34 cants for commercial motor vehicle hazardous materials endorsements
35 and transportation employees at ports, as required by section 70105(c)
36 of title 46; and

37 (2) have the authority to order an appropriate remedy, including re-
38 instatement of the covered individual, should the Secretary determine
39 that a railroad carrier or contractor or subcontractor of a railroad car-
40 rier wrongfully made an adverse employment decision regarding a cov-
41 ered individual pursuant to the rule, regulation, or directive.

1 (e) FALSE STATEMENTS.—A railroad carrier or a contractor or subcon-
2 tractor of a railroad carrier may not knowingly misrepresent to an employee
3 or other relevant person, including an arbiter involved in a labor arbitration,
4 the scope, application, or meaning of rules, regulations, directives, or guid-
5 ance issued by the Secretary related to security background check require-
6 ments for covered individuals when conducting a security background check.
7 The Secretary shall issue a regulation that prohibits a railroad carrier or
8 a contractor or subcontractor of a railroad carrier from knowingly misrepre-
9 senting to an employee or other relevant person, including an arbiter in-
10 volved in a labor arbitration, the scope, application, or meaning of rules,
11 regulations, directives, or guidance issued by the Secretary related to secu-
12 rity background check requirements for covered individuals when conducting
13 a security background check.

14 (f) RIGHTS AND RESPONSIBILITIES.—Nothing in this section shall be
15 construed to abridge a railroad carrier’s or a contractor or subcontractor
16 of a railroad carrier’s rights or responsibilities to make adverse employment
17 decisions permitted by other Federal, State, or local laws. Nothing in this
18 section shall be construed to abridge rights and responsibilities of covered
19 individuals, a railroad carrier, or a contractor or subcontractor of a railroad
20 carrier, under other Federal, State, or local laws or under a collective bar-
21 gaining agreement.

22 (g) NO PREEMPTION OF FEDERAL OR STATE LAW.—Nothing in this sec-
23 tion shall be construed to preempt a Federal, State, or local law that re-
24 quires criminal history background checks, immigration status checks, or
25 other background checks, of covered individuals.

26 (h) PROCESS FOR REVIEW NOT AFFECTED.—Nothing in this section
27 shall be construed to affect the process for review established under section
28 70105(c) of title 46, including regulations issued under that section.

29 **§ 40750. International railroad security program**

30 (a) DEFINITIONS.—In this section:

31 (1) INSPECTION.—The term “inspection” means the comprehensive
32 process used by U.S. Customs and Border Protection to assess goods
33 entering the United States to appraise them for duty purposes, to de-
34 tect the presence of restricted or prohibited items, and to ensure com-
35 pliance with all applicable laws.

36 (2) INTERNATIONAL SUPPLY CHAIN.—The term “international sup-
37 ply chain” means the end-to-end process for shipping goods to or from
38 the United States, beginning at the point of origin (including manufac-
39 turer, supplier, or vendor) through a point of distribution to the des-
40 tination.

1 (3) RADIATION DETECTION EQUIPMENT.—The term “radiation de-
2 tecting equipment” means technology that is capable of detecting or
3 identifying nuclear and radiological material or nuclear and radiological
4 explosive devices.

5 (b) IN GENERAL.—

6 (1) DETECTION SYSTEM.—The Secretary shall develop a system to
7 detect both undeclared passengers and contraband, with a primary
8 focus on the detection of nuclear and radiological materials entering
9 the United States by railroad.

10 (2) SYSTEM REQUIREMENTS.—In developing the system under para-
11 graph (1), the Secretary may, in consultation with the Domestic Nu-
12 clear Detection Office, U.S. Customs and Border Protection, and
13 Transportation Security Administration—

14 (A) deploy radiation detection equipment and nonintrusive im-
15 aging equipment at locations where railroad shipments cross an
16 international border to enter the United States;

17 (B) consider the integration of radiation detection technologies
18 with other nonintrusive inspection technologies where feasible;

19 (C) ensure appropriate training, operations, and response proto-
20 cols are established for Federal, State, and local personnel;

21 (D) implement alternative procedures to check railroad ship-
22 ments at locations where the deployment of nonintrusive inspection
23 imaging equipment is determined to not be practicable;

24 (E) ensure, to the extent practicable, that the technologies de-
25 ployed can detect terrorists or weapons, including weapons of mass
26 destruction; and

27 (F) take other actions, as appropriate, to develop the system.

28 (c) ADDITIONAL INFORMATION.—The Secretary shall—

29 (1) identify and seek the submission of additional data elements for
30 improved high-risk targeting related to the movement of cargo through
31 the international supply chain utilizing a railroad prior to importation
32 into the United States;

33 (2) utilize data collected and maintained by the Secretary of Trans-
34 portation in the targeting of high-risk cargo identified under paragraph
35 (1); and

36 (3) analyze the data provided in this subsection to identify high-risk
37 cargo for inspection.

38 **Subchapter III—Over-the-Road Bus** 39 **Security**

40 **§ 40761. Assessments and plans**

41 (a) IN GENERAL.—The Secretary shall issue regulations that—

1 (1) require each over-the-road bus operator assigned to a high-risk
2 tier under this section—

3 (A) to conduct a vulnerability assessment under subsections (c)
4 and (d); and

5 (B) to prepare, submit to the Secretary for approval, and imple-
6 ment a security plan under subsection (e); and

7 (2) establish standards and guidelines for developing and imple-
8 menting the vulnerability assessments and security plans for carriers
9 assigned to high-risk tiers consistent with this section.

10 (b) NON-HIGH-RISK PROGRAMS.—The Secretary may establish a security
11 program for over-the-road bus operators not assigned to a high-risk tier, in-
12 cluding—

13 (1) guidance for operators in conducting vulnerability assessments
14 and preparing and implementing security plans, as determined appro-
15 priate by the Secretary; and

16 (2) a process to review and approve the assessments and plans, as
17 appropriate.

18 (c) SUBMISSION OF ASSESSMENTS AND SECURITY PLANS.—The vulner-
19 ability assessments and security plans required by the regulations for over-
20 the-road bus operators assigned to a high-risk tier shall be completed and
21 submitted to the Secretary for review and approval.

22 (d) VULNERABILITY ASSESSMENTS.—

23 (1) REQUIREMENTS.—The Secretary shall provide technical assist-
24 ance and guidance to over-the-road bus operators in conducting vulner-
25 ability assessments under this section and shall require that each vul-
26 nerability assessment of an operator assigned to a high-risk tier under
27 this section includes, as appropriate—

28 (A) identification and evaluation of critical assets and infra-
29 structure, including platforms, stations, terminals, and information
30 systems;

31 (B) identification of the vulnerabilities of those assets and infra-
32 structure; and

33 (C) identification of weaknesses in—

34 (i) physical security;

35 (ii) passenger and cargo security;

36 (iii) the security of programmable electronic devices, com-
37 puters, or other automated systems which are used in pro-
38 viding over-the-road bus transportation;

39 (iv) alarms, cameras, and other protection systems;

40 (v) communications systems and utilities needed for over-
41 the-road bus security purposes, including dispatching systems;

- 1 (vi) emergency response planning;
- 2 (vii) employee training; and
- 3 (viii) other matters the Secretary determines appropriate.

4 (2) THREAT INFORMATION.—The Secretary shall provide in a timely
5 manner to the appropriate employees of an over-the-road bus operator,
6 as designated by the over-the-road bus operator, threat information
7 that is relevant to the operator when preparing and submitting a vul-
8 nerability assessment and security plan, including an assessment of the
9 most likely methods that could be used by terrorists to exploit weak-
10 nesses in over-the-road bus security.

11 (e) SECURITY PLANS.—

12 (1) REQUIREMENTS.—The Secretary shall provide technical assist-
13 ance and guidance to over-the-road bus operators in preparing and im-
14 plementing security plans under this section and shall require that each
15 security plan of an over-the-road bus operator assigned to a high-risk
16 tier under this section includes, as appropriate—

17 (A) the identification of a security coordinator having author-
18 ity—

- 19 (i) to implement security actions under the plan;
- 20 (ii) to coordinate security improvements; and
- 21 (iii) to receive communications from appropriate Federal
22 officials regarding over-the-road bus security;

23 (B) a list of needed capital and operational improvements;

24 (C) procedures to be implemented or used by the over-the-road
25 bus operator in response to a terrorist attack, including evacuation
26 and passenger communication plans that include individuals with
27 disabilities, as appropriate;

28 (D) the identification of steps taken with State and local law
29 enforcement agencies, emergency responders, and Federal officials
30 to coordinate security measures and plans for response to a ter-
31 rorist attack;

32 (E) a strategy and timeline for conducting training under sec-
33 tion 40764 of this title;

34 (F) enhanced security measures to be taken by the over-the-
35 road bus operator when the Secretary declares a period of height-
36 ened security risk;

37 (G) plans for providing redundant and backup systems required
38 to ensure the continued operation of critical elements of the over-
39 the-road bus operator's system in the event of a terrorist attack
40 or other incident; and

1 (H) other actions or procedures the Secretary determines are
2 appropriate to address the security of over-the-road bus operators.

3 (2) SECURITY COORDINATOR REQUIREMENTS.—The Secretary shall
4 require that the individual serving as the security coordinator identified
5 in paragraph (1)(A) is a citizen of the United States. The Secretary
6 may waive this requirement with respect to an individual if the Sec-
7 retary determines that it is appropriate to do so based on a background
8 check of the individual and a review of the consolidated terrorist
9 watchlist.

10 (f) DEADLINE FOR REVIEW PROCESS.—Not later than 6 months after re-
11 ceiving the assessments and plans required under this section, the Secretary
12 shall—

13 (1) review each vulnerability assessment and security plan submitted
14 to the Secretary under subsection (c);

15 (2) require amendments to a security plan that does not meet the
16 requirements of this section; and

17 (3) approve a vulnerability assessment or security plan that meets
18 the requirements of this section.

19 (g) TIER ASSIGNMENT.—

20 (1) IN GENERAL.—The Secretary shall assign each over-the-road bus
21 operator to a risk-based tier established by the Secretary.

22 (2) PROVIDING INFORMATION.—The Secretary may request, and an
23 over-the-road bus operator shall provide, information necessary for the
24 Secretary to assign an over-the-road bus operator to the appropriate
25 tier under this subsection.

26 (3) NOTIFICATION.—Not later than 60 days after the date an over-
27 the-road bus operator is assigned to a tier under this section, the Sec-
28 retary shall notify the operator of the tier to which it is assigned and
29 the reasons for the assignment.

30 (4) HIGH-RISK TIERS.—At least one of the tiers established by the
31 Secretary under this section shall be a tier designated for high-risk
32 over-the-road bus operators.

33 (5) REASSIGNMENT.—The Secretary may reassign an over-the-road
34 bus operator to another tier, as appropriate, in response to changes in
35 risk, and the Secretary shall notify the over-the-road bus operator with-
36 in 60 days after the reassignment and provide the operator with the
37 reasons for the reassignment.

38 (h) EXISTING PROCEDURES, PROTOCOLS, AND STANDARDS.—

39 (1) DETERMINATION.—In response to a petition by an over-the-road
40 bus operator or at the discretion of the Secretary, the Secretary may
41 determine that existing procedures, protocols, and standards meet all

1 or part of the requirements of this section regarding vulnerability as-
2 sessments and security plans.

3 (2) ELECTION.—On review and written determination by the Sec-
4 retary that existing procedures, protocols, or standards of an over-the-
5 road bus operator satisfy the requirements of this section, the over-the-
6 road bus operator may elect to comply with those procedures, protocols,
7 or standards instead of the requirements of this section.

8 (3) PARTIAL APPROVAL.—If the Secretary determines that the exist-
9 ing procedures, protocols, or standards of an over-the-road bus oper-
10 ator satisfy only part of the requirements of this section, the Secretary
11 may accept a submission, but shall require submission by the operator
12 of additional information relevant to the vulnerability assessment and
13 security plan of the operator to ensure that the remaining requirements
14 of this section are fulfilled.

15 (4) NOTIFICATION.—If the Secretary determines that particular ex-
16 isting procedures, protocols, or standards of an over-the-road bus oper-
17 ator under this subsection do not satisfy the requirements of this sec-
18 tion, the Secretary shall provide to the operator a written notification
19 that includes an explanation of the reasons for non-acceptance.

20 (5) REVIEW.—Nothing in this subsection shall relieve the Secretary
21 of the obligation—

22 (A) to review the vulnerability assessment and security plan
23 submitted by an over-the-road bus operator under this section; and

24 (B) to approve or disapprove each submission on an individual
25 basis.

26 (i) PERIODIC EVALUATION BY OVER-THE-ROAD BUS PROVIDER RE-
27 QUIRED.—

28 (1) SUBMISSION.—Not later than 3 years after the date on which
29 a vulnerability assessment or security plan required to be submitted to
30 the Secretary under subsection (c) is approved, and at least once every
31 5 years thereafter (or on another schedule the Secretary may establish
32 by regulation), an over-the-road bus operator who submitted a vulner-
33 ability assessment and security plan and who is still assigned to the
34 high-risk tier shall also submit to the Secretary an evaluation of the
35 adequacy of the vulnerability assessment and security plan that in-
36 cludes a description of material changes made to the vulnerability as-
37 sessment or security plan.

38 (2) REVIEW.—Not later than 180 days after the date on which an
39 evaluation is submitted, the Secretary shall review the evaluation and
40 notify the over-the-road bus operator submitting the evaluation of the
41 Secretary's approval or disapproval of the evaluation.

1 (j) SHARED FACILITIES.—The Secretary may permit under this section
2 the development and implementation of coordinated vulnerability assess-
3 ments and security plans to the extent that an over-the-road bus operator
4 shares facilities with, or is co-located with, other transportation entities or
5 providers that are required to develop vulnerability assessments and security
6 plans under Federal law.

7 (k) NONDISCLOSURE OF INFORMATION.—

8 (1) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this
9 section shall be construed as authorizing the withholding of information
10 from Congress.

11 (2) DISCLOSURE OF INDEPENDENTLY FURNISHED INFORMATION.—
12 Nothing in this section shall be construed as affecting the authority or
13 obligation of a Federal agency to disclose a record or information that
14 the Federal agency obtains from an over-the-road bus operator under
15 any other Federal law.

16 **§ 40762. Assistance**

17 (a) IN GENERAL.—The Secretary shall establish a program for making
18 grants to eligible private operators providing transportation by an over-the-
19 road bus for security improvements described in subsection (b).

20 (b) USES OF FUNDS.—A recipient of a grant received under subsection
21 (a) shall use the grant funds for one or more of the following:

22 (1) Constructing and modifying terminals, garages, and facilities, in-
23 cluding terminals and other over-the-road bus facilities owned by State
24 or local governments, to increase their security.

25 (2) Modifying over-the-road buses to increase their security.

26 (3) Protecting or isolating the driver of an over-the-road bus.

27 (4) Acquiring, upgrading, installing, or operating equipment, soft-
28 ware, or accessorial services for collection, storage, or exchange of pas-
29 senger and driver information through ticketing systems or other
30 means and for information links with government agencies, for security
31 purposes.

32 (5) Installing cameras and video surveillance equipment on over-the-
33 road buses and at terminals, garages, and over-the-road bus facilities.

34 (6) Establishing and improving an emergency communications sys-
35 tem linking drivers and over-the-road buses to the recipient's oper-
36 ations center or linking the operations center to law enforcement and
37 emergency personnel.

38 (7) Implementing and operating passenger screening programs for
39 weapons and explosives.

40 (8) Public awareness campaigns for enhanced over-the-road bus se-
41 curity.

1 (9) Operating and capital costs associated with over-the-road bus se-
2 curity awareness, preparedness, and response training, including train-
3 ing under section 40764 of this title and training developed by institu-
4 tions of higher education and by nonprofit employee labor organiza-
5 tions, for over-the-road bus employees, including frontline employees.

6 (10) Chemical, biological, radiological, or explosive detection, includ-
7 ing canine patrols for detection.

8 (11) Overtime reimbursement, including reimbursement of State,
9 local, and tribal governments for costs, for enhanced security personnel
10 assigned to duties related to over-the-road bus security during periods
11 of high or severe threat levels, National Special Security Events, or
12 other periods of heightened security as determined by the Secretary.

13 (12) Live or simulated exercises, including those described in section
14 40763 of this title.

15 (13) Operational costs to hire, train, and employ police and security
16 officers, including canine units, assigned to full-time security or
17 counterterrorism duties related to over-the-road bus transportation, in-
18 cluding reimbursement of State, local, and tribal government costs for
19 the personnel.

20 (14) Development of assessments or security plans under section
21 40761 of this title.

22 (15) Other improvements the Secretary considers appropriate.

23 (c) DUE CONSIDERATION.—In making grants under this section, the Sec-
24 retary shall prioritize grant funding based on security risks to bus pas-
25 sengers and the ability of a project to reduce, or enhance response to, that
26 risk, and shall not penalize private operators of over-the-road buses that
27 took measures to enhance over-the-road bus transportation security prior to
28 September 11, 2001.

29 (d) SECRETARY'S RESPONSIBILITIES.—In carrying out the responsibilities
30 under subsection (a), the Secretary shall—

31 (1) determine the requirements for recipients of grants under this
32 section, including application requirements;

33 (2) select grant recipients;

34 (3) award the funds authorized by this section based on risk, as
35 identified by the plans required under section 40761 of this title or an
36 assessment or plan described in subsection (f)(2); and

37 (4) under subsection (c), establish priorities for the use of funds for
38 grant recipients.

39 (e) DISTRIBUTION OF GRANTS.—The Secretary and the Secretary of
40 Transportation shall determine the most effective and efficient way to dis-
41 tribute grant funds to the recipients of grants determined by the Secretary

1 under subsection (a). Subject to the determination made by the Secretaries,
2 the Secretary may transfer funds to the Secretary of Transportation for the
3 purposes of disbursing funds to the grant recipient.

4 (f) ELIGIBILITY.—

5 (1) IN GENERAL.—A private operator providing transportation by an
6 over-the-road bus is eligible for a grant under this section if the oper-
7 ator has completed a vulnerability assessment and developed a security
8 plan that the Secretary has approved under section 40761 of this title.
9 Grant funds may only be used for permissible uses under subsection
10 (b) to further an over-the-road bus security plan.

11 (2) INTERIM ELIGIBILITY.—Notwithstanding the requirements for
12 eligibility and uses in paragraph (1), the Secretary may award grants
13 under this section for over-the-road bus security improvements listed
14 under subsection (b) based on over-the-road bus vulnerability assess-
15 ments and security plans that the Secretary considers sufficient for the
16 purposes of this section but have not been approved by the Secretary
17 under section 40761 of this title.

18 (g) GRANT TERMS AND CONDITIONS.—Except as otherwise specifically
19 provided in this section, a grant made under this section shall be subject
20 to the terms and conditions applicable to subrecipients who provide over-
21 the-road bus transportation under 5311(f) of title 49 and other terms and
22 conditions that the Secretary determines are necessary.

23 (h) LIMITATION ON USES OF FUNDS.—A grant made under this section
24 may not be used to make a State or local government cost-sharing contribu-
25 tion under any other Federal law.

26 (i) ANNUAL REPORTS.—Each recipient of a grant under this section shall
27 report annually to the Secretary on the use of the grant funds.

28 (j) CONSULTATION.—In carrying out this section, the Secretary shall con-
29 sult with over-the-road bus operators and nonprofit employee labor organi-
30 zations representing over-the-road bus employees and public safety and law
31 enforcement officials.

32 **§ 40763. Exercises**

33 (a) IN GENERAL.—The Secretary shall establish a program for con-
34 ducting security exercises for over-the-road bus transportation for the pur-
35 pose of assessing and improving the capabilities of entities described in sub-
36 section (b) to prevent, prepare for, mitigate, respond to, and recover from
37 acts of terrorism.

38 (b) COVERED ENTITIES.—Entities to be assessed under the program in-
39 clude—

40 (1) Federal, State, and local agencies and tribal governments;

1 (2) over-the-road bus operators and over-the-road bus terminal own-
2 ers and operators;

3 (3) governmental and nongovernmental emergency response pro-
4 viders and law enforcement agencies; and

5 (4) other organizations or entities that the Secretary determines ap-
6 propriate.

7 (e) REQUIREMENTS.—The Secretary shall ensure that the program—

8 (1) consolidates existing security exercises for over-the-road bus op-
9 erators and terminals administered by the Department and the Depart-
10 ment of Transportation, as jointly determined by the Secretary and the
11 Secretary of Transportation, unless the Secretary waives this consolida-
12 tion requirement, as appropriate;

13 (2) consists of exercises that are—

14 (A) scaled and tailored to the needs of the over-the-road bus op-
15 erators and terminals, including addressing the needs of the elder-
16 ly and individuals with disabilities;

17 (B) live, in the case of the facilities most at risk to a terrorist
18 attack;

19 (C) coordinated with appropriate officials;

20 (D) as realistic as practicable and based on current risk assess-
21 ments, including credible threats, vulnerabilities, and con-
22 sequences;

23 (E) inclusive, as appropriate, of over-the-road bus frontline em-
24 ployees; and

25 (F) consistent with the National Incident Management System,
26 the National Response Plan, the National Infrastructure Protec-
27 tion Plan, the National Preparedness Guidance, the National Pre-
28 paredness Goal, and other such national initiatives;

29 (3) provides that exercises described in paragraph (2) will be—

30 (A) evaluated by the Secretary against clear and consistent per-
31 formance measures;

32 (B) assessed by the Secretary to identify best practices, which
33 shall be shared, as appropriate, with operators providing over-the-
34 road bus transportation, nonprofit employee organizations that
35 represent over-the-road bus employees, Federal, State, local, and
36 tribal officials, governmental and nongovernmental emergency re-
37 sponse providers, and law enforcement personnel; and

38 (C) used to develop recommendations, as appropriate, provided
39 to over-the-road bus operators and terminal owners and operators
40 on remedial action to be taken in response to lessons learned;

1 (4) allows for proper advanced notification of communities and local
2 governments in which exercises are held, as appropriate; and

3 (5) assists State, local, and tribal governments and over-the-road bus
4 operators and terminal owners and operators in designing, imple-
5 menting, and evaluating additional exercises that conform to the re-
6 quirements of paragraph (2).

7 (d) CONSISTENT WITH NATIONAL EXERCISE PROGRAM.—The Secretary
8 shall ensure that the exercise program developed under subsection (c) is
9 consistent with the national exercise program established under section
10 20508 of this title.

11 **§ 40764. Training program**

12 (a) IN GENERAL.—The Secretary shall develop and issue regulations for
13 an over-the-road bus training program to prepare over-the-road bus front-
14 line employees for potential security threats and conditions. The regulations
15 shall take into consideration current security training requirements or best
16 practices.

17 (b) CONSULTATION.—The Secretary shall develop regulations under sub-
18 section (a) in consultation with—

19 (1) appropriate law enforcement, fire service, emergency response,
20 security, and terrorism experts;

21 (2) operators providing over-the-road bus transportation; and

22 (3) nonprofit employee labor organizations representing over-the-road
23 bus employees and emergency response personnel.

24 (c) PROGRAM ELEMENTS.—The regulations developed under subsection
25 (a) shall require security training programs to include, at a minimum, ele-
26 ments to address the following, as applicable:

27 (1) Determination of the seriousness of an occurrence or threat.

28 (2) Driver and passenger communication and coordination.

29 (3) Appropriate responses to defend or protect oneself.

30 (4) Use of personal and other protective equipment.

31 (5) Evacuation procedures for passengers and over-the-road bus em-
32 ployees, including individuals with disabilities and the elderly.

33 (6) Psychology, behavior, and methods of terrorists, including obser-
34 vation and analysis.

35 (7) Training related to psychological responses to terrorist incidents,
36 including the ability to cope with hijacker behavior and passenger re-
37 sponses.

38 (8) Live situational training exercises regarding various threat condi-
39 tions, including tunnel evacuation procedures.

40 (9) Recognition and reporting of dangerous substances, suspicious
41 packages, and situations.

1 (10) Understanding security incident procedures, including proce-
2 dures for communicating with emergency response providers and for
3 on-scene interaction with emergency response providers.

4 (11) Operation and maintenance of security equipment and systems.

5 (12) Other security training activities that the Secretary considers
6 appropriate.

7 (d) REQUIRED PROGRAMS.—

8 (1) DEVELOPMENT AND SUBMISSION TO SECRETARY.—Not later
9 than 90 days after the Secretary issues the regulations under sub-
10 section (a), each over-the-road bus operator shall develop a security
11 training program in accordance with the regulations and submit the
12 program to the Secretary for approval.

13 (2) APPROVAL.—Not later than 60 days after receiving a security
14 training program proposal under this subsection, the Secretary shall
15 approve the program or require the over-the-road bus operator that de-
16 veloped the program to make revisions to the program that the Sec-
17 retary considers necessary for the program to meet the requirements
18 of the regulations. An over-the-road bus operator shall respond to the
19 Secretary's comments not later than 30 days after receiving them.

20 (3) TRAINING.—Not later than 1 year after the Secretary approves
21 a security training program under this subsection, the over-the-road
22 bus operator that developed the program shall complete the training of
23 all over-the-road bus frontline employees who were hired by the oper-
24 ator more than 30 days preceding the approval date. For employees
25 employed by an operator for fewer than 30 days preceding the approval
26 date, training shall be completed within the first 60 days of employ-
27 ment.

28 (4) UPDATES OF REGULATIONS AND PROGRAM REVISIONS.—The
29 Secretary shall periodically review and update, as appropriate, the
30 training regulations issued under subsection (a) to reflect new or
31 changing security threats. Each over-the-road bus operator shall revise
32 its training program accordingly and provide additional training as nec-
33 essary to its employees within a reasonable time after the regulations
34 are updated.

35 (e) NATIONAL TRAINING PROGRAM.—The Secretary shall ensure that the
36 training program developed under subsection (a) is a component of the na-
37 tional training program established under section 20508 of this title.

38 **§ 40765. Research and development**

39 (a) IN GENERAL.—The Secretary, acting through the Under Secretary
40 for Science and Technology and the Administrator of the Transportation

1 Security Administration, shall carry out a research and development pro-
2 gram for the purpose of improving the security of over-the-road buses.

3 (b) ELIGIBLE PROJECTS.—The research and development program may
4 include projects—

5 (1) to reduce the vulnerability of over-the-road buses, stations, termi-
6 nals, and equipment to explosives and hazardous chemical, biological,
7 and radioactive substances, including the development of technology to
8 screen passengers in large numbers with minimal interference and dis-
9 ruption;

10 (2) to test new emergency response and recovery techniques and
11 technologies, including those used at international borders;

12 (3) to develop improved technologies, including those for—

13 (A) emergency response training, including training in a tunnel
14 environment, if appropriate; and

15 (B) security and redundancy for critical communications, elec-
16 trical power, computer, and over-the-road bus control systems; and

17 (4) to address other vulnerabilities and risks identified by the Sec-
18 retary.

19 (c) COORDINATION WITH OTHER RESEARCH INITIATIVES.—The Sec-
20 retary—

21 (1) shall ensure that the research and development program is con-
22 sistent with the other transportation security research and development
23 programs required by section 30304 and chapters 401 through 407 of
24 this title;

25 (2) shall, to the extent practicable, coordinate the research and de-
26 velopment activities of the Department with other ongoing research and
27 development security-related initiatives, including research being con-
28 ducted by—

29 (A) the Department of Transportation, including University
30 Transportation Centers and other institutes, centers, and simula-
31 tors funded by the Department of Transportation;

32 (B) the National Academy of Sciences;

33 (C) the Technical Support Working Group;

34 (D) other Federal departments and agencies; and

35 (E) other Federal and private research laboratories, research
36 entities, and institutions of higher education, including Historically
37 Black Colleges and Universities, Hispanic-serving institutions, and
38 Indian tribally controlled colleges and universities;

39 (3) shall carry out a research and development project authorized by
40 this section through a reimbursable agreement with an appropriate
41 Federal agency, if the agency—

1 (A) is currently sponsoring a research and development project
2 in a similar area; or

3 (B) has a unique facility or capability that would be useful in
4 carrying out the project;

5 (4) may award grants to, and enter into cooperative agreements,
6 contracts, other transactions, or reimbursable agreements with, the en-
7 tities described in paragraph (2) and eligible recipients under section
8 40762 of this title; and

9 (5) shall make reasonable efforts to enter into memoranda of under-
10 standing, contracts, grants, cooperative agreements, or other trans-
11 actions with private operators providing over-the-road bus transpor-
12 tation willing to contribute assets, physical space, and other resources.

13 (d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES.—

14 (1) CONSULTATION.—In carrying out research and development
15 projects under this section, the Secretary shall consult with the Chief
16 Privacy Officer of the Department and the Officer for Civil Rights and
17 Civil Liberties of the Department as appropriate and under section
18 10520 of this title.

19 (2) PRIVACY IMPACT ASSESSMENTS.—In accordance with sections
20 10520 and 11705 of this title, the Chief Privacy Officer shall conduct
21 privacy impact assessments, and the Officer for Civil Rights and Civil
22 Liberties shall conduct reviews, as appropriate, of research and devel-
23 opment initiatives developed under this section that the Secretary de-
24 termines could have an impact on privacy, civil rights, or civil liberties.

25 **Subchapter IV—Hazardous Material and** 26 **Pipeline Security**

27 **§ 40781. Railroad routing of security-sensitive materials**

28 (a) DEFINITIONS.—In this section:

29 (1) HIGH-CONSEQUENCE TARGET.—The term “high-consequence tar-
30 get” means a property, natural resource, location, area, or other target
31 designated by the Secretary that is a viable terrorist target of national
32 significance, which may include a facility or specific critical infrastruc-
33 ture, the attack of which by railroad could result in—

34 (A) catastrophic loss of life;

35 (B) significant damage to national security or defense capabili-
36 ties; or

37 (C) national economic harm.

38 (2) ROUTE.—The term “route” includes storage facilities and track-
39 age used by railroad cars in transportation in commerce.

40 (b) SECURITY-SENSITIVE MATERIALS COMMODITY DATA.—The Secretary
41 of Transportation shall ensure that the final rule published as provided in

1 section 1551(a) of the Implementing Recommendations of the 9/11 Commis-
2 sion Act of 2007 (Public Law 110–53, 121 Stat. 469) requires each railroad
3 carrier transporting security-sensitive materials in commerce to, no later
4 than 90 days after the end of each calendar year, compile security-sensitive
5 materials commodity data. The data must be collected by route, line seg-
6 ment, or series of line segments, as aggregated by the railroad carrier.
7 Within the railroad-carrier-selected route, the commodity data must identify
8 the geographic location of the route and the total number of shipments by
9 the United Nations identification number for the security-sensitive mate-
10 rials.

11 (c) RAILROAD TRANSPORTATION ROUTE ANALYSIS FOR SECURITY-SEN-
12 SITIVE MATERIALS.—The Secretary of Transportation shall ensure that the
13 final rule requires each railroad carrier transporting security-sensitive mate-
14 rials in commerce to, for each calendar year, provide a written analysis of
15 the safety and security risks for the transportation routes identified in the
16 security-sensitive materials commodity data collected as required by sub-
17 section (b). The safety and security risks present shall be analyzed for the
18 route, railroad facilities, railroad storage facilities, and high-consequence
19 targets along or in proximity to the route.

20 (d) ALTERNATIVE ROUTE ANALYSIS FOR SECURITY-SENSITIVE MATE-
21 RIALS.—The Secretary of Transportation shall ensure that the final rule re-
22 quires each railroad carrier transporting security-sensitive materials in com-
23 merce to—

24 (1) for each calendar year—

25 (A) identify practicable alternative routes over which the rail-
26 road carrier has authority to operate as compared to the current
27 route for a shipment analyzed under subsection (c); and

28 (B) perform a safety and security risk assessment of the alter-
29 native route for comparison to the route analysis specified in sub-
30 section (c);

31 (2) ensure that the analysis under paragraph (1) includes—

32 (A) identification of safety and security risks for an alternative
33 route;

34 (B) comparison of those risks identified under subparagraph
35 (A) to the primary railroad transportation route, including the risk
36 of a catastrophic release from a shipment traveling along the alter-
37 nate route compared to the primary route;

38 (C) remediation or mitigation measures implemented on the pri-
39 mary or alternative route; and

40 (D) potential economic effects of using an alternative route; and

1 (3) consider when determining the practicable alternative routes
2 under paragraph (1)(A) the use of interchange agreements with other
3 railroad carriers.

4 (e) ALTERNATIVE ROUTE SELECTION FOR SECURITY-SENSITIVE MATE-
5 RIALS.—The Secretary of Transportation shall ensure that the final rule re-
6 quires each railroad carrier transporting security-sensitive materials in com-
7 merce to use the analyses required by subsections (c) and (d) to select the
8 safest and most secure route to be used in transporting security-sensitive
9 materials.

10 (f) REVIEW.—The Secretary of Transportation shall ensure that the final
11 rule requires each railroad carrier transporting security-sensitive materials
12 in commerce to annually review and select the practicable route posing the
13 least overall safety and security risk under this section. The railroad carrier
14 must retain in writing all route review and selection decision documentation
15 and restrict the distribution, disclosure, and availability of information con-
16 tained in the route analysis to appropriate persons. This documentation
17 should include, but is not limited to, comparative analyses, charts, graphics,
18 or railroad system maps.

19 (g) RETROSPECTIVE ANALYSIS.—The Secretary of Transportation shall
20 ensure that the final rule requires each railroad carrier transporting secu-
21 rity-sensitive materials in commerce to, not less than once every 3 years,
22 analyze the route selection determinations required under this section. The
23 analysis shall include a comprehensive, system-wide review of all operational
24 changes, infrastructure modifications, traffic adjustments, changes in the
25 nature of high-consequence targets located along or in proximity to the
26 route, or other changes affecting the safety and security of the movements
27 of security-sensitive materials that were implemented since the previous
28 analysis was completed.

29 (h) CONSULTATION.—In carrying out subsection (c), railroad carriers
30 transporting security-sensitive materials in commerce shall seek relevant in-
31 formation from State, local, and tribal officials, as appropriate, regarding
32 security risks to high-consequence targets along or in proximity to a route
33 used by a railroad carrier to transport security-sensitive materials.

34 **§ 40782. Railroad security-sensitive material tracking**

35 (a) IN GENERAL.—In conjunction with the research and development pro-
36 gram established under section 40747 of this title and consistent with the
37 results of research relating to wireless and other tracking technologies, the
38 Secretary, in consultation with the Administrator of the Transportation Se-
39 curity Administration, shall develop a program that will encourage the
40 equipping of railroad cars transporting security-sensitive materials, as de-
41 fined in section 40701 of this title, with technology that provides—

- 1 (1) car position location and tracking capabilities; and
2 (2) notification of railroad car depressurization, breach, unsafe tem-
3 perature, or release of hazardous materials, as appropriate.

4 (b) COORDINATION.—In developing the program required by subsection
5 (a), the Secretary shall—

6 (1) consult with the Secretary of Transportation to coordinate the
7 program with ongoing or planned efforts for railroad car tracking at
8 the Department of Transportation; and

9 (2) ensure that the program is consistent with recommendations and
10 findings of the Department of Homeland Security’s hazardous material
11 railroad tank car tracking pilot programs.

12 **§ 40783. Motor carrier security-sensitive material tracking**

13 (a) COMMUNICATIONS.—

14 (1) IN GENERAL.—Consistent with the findings of the Transpor-
15 tation Security Administration’s hazardous materials truck security
16 pilot program, the Secretary, through the Administrator of the Trans-
17 portation Security Administration and in consultation with the Sec-
18 retary of Transportation, shall develop a program to facilitate the
19 tracking of motor carrier shipments of security-sensitive materials and
20 to equip vehicles used in the shipments with technology that provides—

- 21 (A) frequent or continuous communications;
22 (B) vehicle position location and tracking capabilities; and
23 (C) a feature that allows a driver of the vehicles to broadcast
24 an emergency distress signal.

25 (2) CONSIDERATIONS.—In developing the program required by para-
26 graph (1), the Secretary shall—

27 (A) consult with the Secretary of Transportation to coordinate
28 the program with ongoing or planned efforts for motor carrier or
29 security-sensitive materials tracking at the Department of Trans-
30 portation;

31 (B) take into consideration the recommendations and findings
32 of the report on the hazardous material safety and security oper-
33 ational field test released by the Federal Motor Carrier Safety Ad-
34 ministration on November 11, 2004; and

35 (C) evaluate—

- 36 (i) new information related to the costs and benefits of de-
37 ploying, equipping, and utilizing tracking technology, includ-
38 ing portable tracking technology, for motor carriers trans-
39 porting security-sensitive materials not included in the haz-
40 ardous material safety and security operational field test re-

1 port released by the Federal Motor Carrier Safety Adminis-
2 tration on November 11, 2004;

3 (ii) the ability of tracking technology to resist tampering
4 and disabling;

5 (iii) the capability of tracking technology to collect, display,
6 and store information regarding the movement of shipments
7 of security-sensitive materials by commercial motor vehicles;

8 (iv) the appropriate range of contact intervals between the
9 tracking technology and a commercial motor vehicle trans-
10 porting security-sensitive materials;

11 (v) technology that allows the installation by a motor car-
12 rier of concealed electronic devices on commercial motor vehi-
13 cles that can be activated by law enforcement authorities to
14 disable the vehicle or alert emergency response resources to
15 locate and recover security-sensitive materials in the event of
16 loss or theft of the materials;

17 (vi) whether installation of the technology described in
18 clause (v) should be incorporated into the program under
19 paragraph (1);

20 (vii) the costs, benefits, and practicality of the technology
21 described in clause (v) in the context of the overall benefit to
22 national security, including commerce in transportation; and

23 (viii) other systems and information that the Secretary de-
24 termines appropriate.

25 (b) LIMITATION.—The Secretary may not mandate the installation or uti-
26 lization of a technology described under this section without additional con-
27 gressional authority provided after August 3, 2007.

28 **§ 40784. Use of transportation security card in hazmat li-**
29 **censing**

30 (a) BACKGROUND CHECK.—An individual who has a valid transportation
31 employee identification card issued by the Secretary under section 70105 of
32 title 46 is deemed to have met the background records check required under
33 section 5103a of title 49.

34 (b) STATE REVIEW.—Nothing in this section prevents or preempts a
35 State from conducting a criminal records check of an individual who has
36 applied for a license to operate a motor vehicle transporting in commerce
37 a hazardous material.

38 **§ 40785. Pipeline security inspections and enforcement**

39 (a) IN GENERAL.—Consistent with the Annex to the Memorandum of
40 Understanding executed on August 9, 2006, between the Department of
41 Transportation and the Department, the Secretary, in consultation with the

1 Secretary of Transportation, shall establish a program for reviewing pipeline
2 operator adoption of recommendations of the September 5, 2002, Depart-
3 ment of Transportation Research and Special Programs Administration's
4 Pipeline Security Information Circular, including the review of pipeline secu-
5 rity plans and critical facility inspections.

6 (b) REVIEW AND INSPECTION.—The Secretary and the Secretary of
7 Transportation shall develop and implement a plan for reviewing the pipe-
8 line security plans and for inspecting the critical facilities of the 100 most
9 critical pipeline operators covered by the September 5, 2002, circular, where
10 the facilities have not been inspected for security purposes since September
11 5, 2002, by either the Department or the Department of Transportation.

12 (c) COMPLIANCE REVIEW METHODOLOGY.—In reviewing pipeline oper-
13 ator compliance under subsections (a) and (b), the Secretary and the Sec-
14 retary of Transportation shall use risk assessment methodologies to
15 prioritize risks and to target inspection and enforcement actions to the high-
16 est risk pipeline assets.

17 (d) REGULATIONS.—The Secretary and the Secretary of Transportation
18 shall develop and transmit to pipeline operators security recommendations
19 for natural gas and hazardous liquid pipelines and pipeline facilities. If the
20 Secretary determines that regulations are appropriate, the Secretary shall
21 consult with the Secretary of Transportation on the extent of risk and ap-
22 propriate mitigation measures, and the Secretary or the Secretary of Trans-
23 portation, consistent with the Annex to the Memorandum of Understanding
24 executed on August 9, 2006, shall promulgate regulations and carry out
25 necessary inspection and enforcement actions. Regulations shall incorporate
26 the guidance provided to pipeline operators by the September 5, 2002, De-
27 partment of Transportation Research and Special Programs Administra-
28 tion's Pipeline Security Information Circular and contain additional require-
29 ments as necessary based upon the results of the inspections performed
30 under subsection (b). The regulations shall include the imposition of civil
31 penalties for noncompliance.

32 **§ 40786. Pipeline security and incident recovery plan**

33 (a) IN GENERAL.—The Secretary, in consultation with the Secretary of
34 Transportation and the Administrator of the Pipeline and Hazardous Mate-
35 rials Safety Administration, and in accordance with the Annex to the Memo-
36 randum of Understanding executed on August 9, 2006, the National Strat-
37 egy for Transportation Security, and Homeland Security Presidential Direc-
38 tive—7, shall develop a pipeline security and incident recovery protocols plan.
39 The plan shall include—

40 (1) a security plan for the Government to provide increased security
41 support to the most critical interstate and intrastate natural gas and

1 hazardous liquid transmission pipeline infrastructure and operations as
 2 determined under section 40785 of this title when—

3 (A) the pipeline infrastructure or operations are under severe
 4 security threat levels of alert; or

5 (B) specific security threat information relating to the pipeline
 6 infrastructure or operations exists; and

7 (2) an incident recovery protocol plan, developed in conjunction with
 8 interstate and intrastate transmission and distribution pipeline opera-
 9 tors and terminals and facilities operators connected to pipelines, to de-
 10 velop protocols to ensure the continued transportation of natural gas
 11 and hazardous liquids to essential markets and for essential public
 12 health or national defense uses in the event of an incident affecting the
 13 interstate and intrastate natural gas and hazardous liquid transmission
 14 and distribution pipeline system, including protocols for restoring es-
 15 sential services supporting pipelines and granting access to pipeline op-
 16 erators for pipeline infrastructure repair, replacement, or bypass fol-
 17 lowing an incident.

18 (b) EXISTING PRIVATE- AND PUBLIC-SECTOR EFFORTS.—The plan shall
 19 take into account actions taken or planned by both private and public enti-
 20 ties to address identified pipeline security issues and assess the effective in-
 21 tegration of the actions.

22 (c) CONSULTATION.—In developing the plan under subsection (a), the
 23 Secretary shall consult with the Secretary of Transportation, interstate and
 24 intrastate transmission and distribution pipeline operators, nonprofit em-
 25 ployee organizations representing pipeline employees, emergency responders,
 26 offerors, State pipeline safety agencies, public safety officials, and other rel-
 27 evant parties.

28 **Chapter 409—Air Transportation Security**

Sec.

Subchapter I—General

40901. Definitions.

Subchapter II—Requirements

40911. Screening passengers and property.

40912. Refusal to transport passengers and property.

40913. Air transportation security.

40914. Domestic air transportation system security.

40915. Information about threats to civil aviation.

40916. Foreign air carrier security programs.

40917. Security standards at foreign airports.

40918. Travel advisory and suspension of foreign assistance.

40919. Passenger manifests.

40920. Agreements on aircraft sabotage, aircraft hijacking, and airport security.

40921. Intelligence.

40922. Research and development.

40923. Explosive detection.

40924. Airport construction guidelines.

40925. Alaska exemptions.

40926. Assessments and evaluations.

- 40927. Federal air marshals and training of law enforcement personnel.
 - 40928. Crew training.
 - 40929. PreCheck Program.
 - 40930. PreCheck expedited screening.
 - 40931. Screening partnership program.
 - 40932. Federal flight deck officer program.
 - 40933. Deputization of State and local law enforcement officers.
 - 40934. Airport security improvement projects.
 - 40935. Repair station security.
 - 40936. Deployment and use of detection equipment at airport screening checkpoints.
 - 40937. Appeal and redress process for passengers wrongly delayed or prohibited from boarding a flight.
 - 40938. Expedited screening for severely injured or disabled members of the armed forces and severely injured or disabled veterans.
 - 40939. Honor Flight program.
 - 40940. Donation of screening equipment to protect the United States
- Subchapter III—Administration and Personnel**
- 40951. Authority to exempt from regulations.
 - 40952. Administrative.
 - 40953. Federal Security Directors.
 - 40954. Foreign Security Liaison Officers.
 - 40955. Employment standards and training.
 - 40956. Employment investigations and restrictions.
 - 40957. Prohibition on transferring duties and powers.
 - 40958. Reports.
 - 40959. Training to operate certain aircraft.
 - 40960. Security service fee.
 - 40961. Immunity for reporting suspicious activities.
 - 40962. Performance goals and objectives.
 - 40963. Aviation Security Advisory Committee.

Subchapter I—General

§ 40901. Definitions

(a) TITLE 49 DEFINITIONS.—Unless otherwise specifically provided, the definitions in section 40102 of title 49 apply to this chapter.

(b) ADMINISTRATOR.—In this chapter, the term “Administrator” means the Administrator of the Transportation Security Administration.

Subchapter II—Requirements

§ 40911. Screening passengers and property

(a) IN GENERAL.—The Administrator shall provide for the screening of all passengers and property, including United States mail, cargo, carry-on and checked baggage, and other articles, that will be carried aboard a passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation. In the case of flights and flight segments originating in the United States, the screening shall take place before boarding and shall be carried out by a Federal Government employee (as defined in section 2105 of title 5), except as otherwise provided in section 40931 of this title and except for identifying passengers and baggage for screening under the CAPPs and known shipper programs and conducting positive bag-match programs.

(b) SUPERVISION OF SCREENING.—All screening of passengers and property at airports in the United States where screening is required under this section shall be supervised by uniformed Federal personnel of the Transpor-

1 tation Security Administration, who shall have the power to order the dis-
2 missal of an individual performing screening.

3 (c) CHECKED BAGGAGE DEADLINE.—A system must be in operation to
4 screen all checked baggage at all airports in the United States as soon as
5 practicable.

6 (d) EXPLOSIVES DETECTION SYSTEMS.—

7 (1) IN GENERAL.—The Administrator shall take all necessary action
8 to ensure that—

9 (A) explosives detection systems are deployed as soon as pos-
10 sible to ensure that all United States airports described in section
11 40913(c) of this title have sufficient explosives detection systems
12 to screen all checked baggage and that as soon as the systems are
13 in place at an airport, all checked baggage at the airport is
14 screened by those systems;

15 (B) all systems deployed under subparagraph (A) are fully uti-
16 lized; and

17 (C) if explosives detection equipment at an airport is unavail-
18 able, all checked baggage is screened by an alternative means.

19 (2) PRECLEARANCE AIRPORTS.—

20 (A) DEFINITION OF AVIATION SECURITY PRECLEARANCE
21 AGREEMENT.—In this paragraph, the term “aviation security
22 preclearance agreement” means an agreement that delineates and
23 implements security standards and protocols that are determined
24 by the Administrator, in coordination with U.S. Customs and Bor-
25 der Protection, to be comparable to those of the United States and
26 therefore sufficiently effective to enable passengers to deplane into
27 sterile areas of airports in the United States.

28 (B) IN GENERAL.—For a flight or flight segment originating at
29 an airport outside the United States and traveling to the United
30 States with respect to which checked baggage has been screened
31 in accordance with an aviation security preclearance agreement be-
32 tween the United States and the country in which the airport is
33 located, the Administrator may, in coordination with U.S. Customs
34 and Border Protection, determine whether the baggage must be
35 re-screened in the United States by an explosives detection system
36 before the baggage continues on any additional flight or flight seg-
37 ment.

38 (C) RE-SCREENING REQUIREMENT.—If the Administrator deter-
39 mines that the government of a foreign country has not main-
40 tained security standards and protocols comparable to those of the
41 United States at airports at which preclearance operations have

1 been established in accordance with this paragraph, the Adminis-
2 trator shall ensure that Transportation Security Administration
3 personnel re-screen passengers arriving from those airports and
4 their property in the United States before the passengers are per-
5 mitted into sterile area of airports in the United States.

6 (D) REPORT.—The Administrator shall submit to the Com-
7 mittee on Homeland Security of the House of Representatives, the
8 Committee on Commerce, Science, and Transportation of the Sen-
9 ate, and the Committee on Homeland Security and Governmental
10 Affairs of the Senate an annual report on the re-screening of bag-
11 gage under this paragraph. Each report shall include the following
12 for the year covered by the report:

13 (i) A list of airports outside the United States from which
14 a flight or flight segment traveled to the United States for
15 which the Administrator determined, in accordance with the
16 authority under subparagraph (B), that checked baggage was
17 not required to be re-screened in the United States by an ex-
18 plosives detection system before the baggage continued on an
19 additional flight or flight segment.

20 (ii) The amount of Federal savings generated from the ex-
21 ercise of the authority.

22 (e) ONE-STOP PILOT PROGRAM

23 (1) DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEES.—In
24 this section, the term “appropriate congressional committees” means—

25 (A) the Committee on Homeland Security and Committee on
26 Foreign Affairs of the House of Representatives; and

27 (B) the Committee on Homeland Security and Governmental
28 Affairs, the Committee on Commerce, Science, and Transpor-
29 tation, and the Committee on Foreign Relations of the Senate.

30 (2) IMPLEMENTATION.—Notwithstanding subsection (a), the Admin-
31 istrator, in coordination with the Commissioner of U.S. Customs and
32 Border Protection and the Secretary of State, may implement a pilot
33 program at not more than 6 foreign last point of departure airports
34 to permit passengers and their accessible property arriving on direct
35 flights or flight segments originating at those participating foreign air-
36 ports to continue on additional flights or flight segments originating in
37 the United States without additional security re-screening if—

38 (A) the initial screening was conducted in accordance with an
39 aviation security screening agreement described in paragraph (5);

1 (B) passengers arriving from participating foreign airports are
2 unable to access their checked baggage until the arrival at their
3 final destination; and

4 (C) on arrival in the United States, passengers arriving from
5 participating foreign airports do not come into contact with other
6 arriving international passengers, those passengers' property, or
7 other individuals who have not been screened or subjected to other
8 appropriate security controls required for entry into the airport's
9 sterile area.

10 (3)REQUIREMENTS.—In carrying out this subsection, the Adminis-
11 trator shall ensure that there is no reduction in the level of security
12 or specific Transportation Security Administration aviation security
13 standards or requirements for screening passengers and their property
14 prior to boarding an international flight bound for the United States,
15 including specific aviation security standards and requirements regard-
16 ing the following:

17 (A) High risk passengers and their property.

18 (B) Weapons, explosives, and incendiaries.

19 (C) Screening passengers and property transferring at a foreign
20 last point of departure airport from another airport and bound for
21 the United States, and addressing any commingling of the pas-
22 sengers and property with passengers and property screened under
23 the pilot program described in paragraph (2).

24 (D) Insider risk at foreign last point of departure airports.

25 (4)RE-SCREENING OF CHECKED BAGGAGE.—Subject to paragraph
26 (6), the Administrator may determine whether checked baggage arriv-
27 ing from participating foreign airports referenced in paragraph (2) that
28 screen using an explosives detection system must be re-screened in the
29 United States by an explosives detection system before the baggage
30 continues on any additional flight or flight segment.

31 (5)AVIATION SECURITY SCREENING AGREEMENT.—

32 (A)IN GENERAL.—An aviation security screening agreement de-
33 scribed in this paragraph is a treaty, executive agreement, or non-
34 binding instrument entered into with a foreign country that delin-
35 eates and implements security standards and protocols utilized at
36 a foreign last point of departure airport that are determined by
37 the Administrator—

38 (i) to be comparable to those of the United States; and

39 (ii) sufficiently effective to enable passengers and their ac-
40 cessible property to deplane into sterile areas of airports in
41 the United States without the need for re-screening.

1 (B)NON-DELEGATION.—The authority to approve an aviation
2 security screening agreement may not be delegated below the level
3 of the Secretary of State, the Secretary, or the Administrator.

4 (6)RE-SCREENING REQUIREMENT.—

5 (A)IN GENERAL.—If the Administrator determines that a for-
6 eign country participating in the aviation security screening agree-
7 ment has not maintained and implemented security standards and
8 protocols comparable to those of the United States at foreign last
9 point of departure airports at which a pilot program has been es-
10 tablished in accordance with this subsection, the Administrator
11 shall ensure that passengers and their property arriving from
12 those airports are re-screened in the United States, including by
13 using explosives detection systems in accordance with subsection
14 (d) and implementing regulations and directives, before the pas-
15 sengers and their property are permitted into sterile areas of air-
16 ports in the United States.

17 (B)CONSULTATION.—If the Administrator has reasonable
18 grounds to believe the other party to an aviation security screening
19 agreement has not complied with the agreement, the Adminis-
20 trator shall request immediate consultation with the party.

21 (C)SUSPENSION OR TERMINATION OF AGREEMENT.—If a satis-
22 factory resolution between the Transportation Security Adminis-
23 tration and a foreign country is not reached within 45 days after
24 a consultation request under subparagraph (B) or in the case of
25 the foreign country's continued or egregious failure to maintain
26 the security standards and protocols described in subparagraph
27 (A), the President, or with the concurrence of the Secretary of
28 State, the Secretary, or the Administrator, as appropriate, shall
29 suspend or terminate the aviation security screening agreement
30 with the country, as determined appropriate by the President, the
31 Secretary, or the Administrator. The Administrator shall notify
32 the appropriate congressional committees of the consultation and
33 suspension or termination, not later than 7 days after the con-
34 sultation and suspension or termination.

35 (7)BRIEFINGS TO CONGRESS.—Not later than 45 days before an
36 aviation security screening agreement described in paragraph (5) enters
37 into force, the Administrator, in coordination with the Secretary of
38 State, shall submit to the appropriate congressional committees the fol-
39 lowing:

40 (A) An aviation security threat assessment for the country in
41 which the foreign last point of departure airport is located.

1 (B) Information regarding any corresponding mitigation efforts
2 to address any security issues identified in the threat assessment,
3 including any plans for joint covert testing.

4 (C) Information on potential security vulnerabilities associated
5 with commencing a pilot program at the foreign last point of de-
6 parture airport pursuant to paragraph (2) and mitigation plans to
7 address the potential security vulnerabilities.

8 (D) An assessment of the impacts the pilot program will have
9 on aviation security.

10 (E) An assessment of the screening performed at the foreign
11 last point of departure airport, including the feasibility of Trans-
12 portation Security Administration personnel monitoring screening,
13 security protocols, and standards.

14 (F) Information regarding identifying the entity responsible for
15 screening passengers and property at the foreign last point of de-
16 parture airport.

17 (G) The name of the entity or local authority and any con-
18 tractor or subcontractor.

19 (H) Information regarding the screening requirements relating
20 to the aviation security screening agreement.

21 (I) Details regarding information sharing mechanisms between
22 the Transportation Security Administration and the foreign last
23 point of departure airport, screening authority, or entity respon-
24 sible for screening provided for under the aviation security screen-
25 ing agreement.

26 (J) A copy of the aviation security screening agreement, which
27 shall identify the foreign last point of departure airports at which
28 a pilot program under this section is to be established.

29 (8) CERTIFICATIONS.—For each aviation security screening agree-
30 ment described in paragraph (5), the Administrator, in coordination
31 with the Secretary of State, shall submit to the appropriate congres-
32 sional committees the following:

33 (A)(i) A certification that the agreement satisfies all of the re-
34 quirements specified in paragraph (3); or

35 (ii) in the event that one or more of the requirements are not
36 so satisfied, a description of the unsatisfied requirements and in-
37 formation on what actions the Administrator will take to ensure
38 that the remaining requirements are satisfied before the agree-
39 ment enters into force.

40 (B) A certification that the Transportation Security Administra-
41 tion and U.S. Customs and Border Protection have ensured that

1 any necessary physical modifications or appropriate mitigations
2 exist in the domestic one-stop security pilot program airport prior
3 to receiving international passengers from a last point of depart-
4 ure airport under the aviation security screening agreement.

5 (C) A certification that a foreign last point of departure airport
6 covered by an aviation security screening agreement has an oper-
7 ation to screen all checked bags as required by law, regulation, or
8 international agreement, including the full utilization of explosives
9 detection systems to the extent applicable.

10 (D) A certification that the Administrator consulted with stake-
11 holders, including air carriers, aviation nonprofit labor organiza-
12 tions, airport operators, relevant interagency partners, and other
13 stakeholders that the Administrator determines appropriate.

14 (9)REPORT TO CONGRESS.—Not later than December 23, 2027, the
15 Secretary, in coordination with the Administrator, shall submit to the
16 appropriate congressional committees a report regarding the implemen-
17 tation of the pilot program authorized under this subsection, including
18 information relating to the following:

19 (A) The impact of the program on homeland security and inter-
20 national aviation security, including any benefits and challenges of
21 the program.

22 (B) The impact of the program on passengers, airports, and air
23 carriers, including any benefits and challenges of the program.

24 (C) The impact and feasibility of continuing the program or ex-
25 panding it into a more permanent program, including any benefits
26 and challenges of the continuation or expansion.

27 (10)RULE OF CONSTRUCTION.—Nothing in this subsection may be
28 construed as limiting the authority of U.S. Customs and Border Pro-
29 tection to inspect persons and baggage arriving in the United States
30 in accordance with applicable law.

31 (11)SUNSET.—The pilot program authorized under this subsection
32 shall terminate on December 23, 2028.

33 (f) CARGO DEADLINE.—A system must be in operation to screen, inspect,
34 or otherwise ensure the security of all cargo that is to be transported in
35 all-cargo aircraft in air transportation and intrastate air transportation as
36 soon as practicable.

37 (g) AIR CARGO ON PASSENGER AIRCRAFT.—

38 (1) DEFINITION OF SCREENING.—In this subsection, the term
39 “screening” means a physical examination or nonintrusive methods of
40 assessing whether cargo poses a threat to transportation security, in-
41 cluding x-ray systems, explosives detection systems, explosives trace de-

1 tection, explosives detection canine teams certified by the Transpor-
2 tation Security Administration, or a physical search together with
3 manifest verification.

4 (2) IN GENERAL.—The Secretary shall establish a system to screen
5 100 percent of cargo transported on passenger aircraft operated by an
6 air carrier or foreign air carrier in air transportation or intrastate air
7 transportation to ensure the security of all passenger aircraft carrying
8 cargo.

9 (3) MINIMUM STANDARDS.—The system referred to in paragraph (2)
10 shall require, at a minimum, that equipment, technology, procedures,
11 personnel, or other methods approved by the Administrator, are used
12 to screen cargo carried on passenger aircraft described in paragraph
13 (2) to provide a level of security commensurate with the level of secu-
14 rity for the screening of passenger checked baggage.

15 (4) ADDITIONAL CARGO SCREENING METHODS.—

16 (A) IN GENERAL.—The Administrator may approve additional
17 methods to ensure that the cargo does not pose a threat to trans-
18 portation security and to assist in meeting the requirements of
19 this subsection.

20 (B) MINIMUM REQUIREMENTS.—The additional cargo screening
21 methods shall not include solely performing a review of informa-
22 tion about the contents of cargo or verifying the identity of a ship-
23 per of the cargo that is not performed in conjunction with other
24 security methods authorized under this subsection, including
25 whether a known shipper is registered in the known shipper data-
26 base.

27 (C) CERTIFICATION PROGRAM.—The additional cargo screening
28 methods may include a program to certify the security methods
29 used by shippers under paragraphs (2) and (3) and alternative
30 screening methods pursuant to exemptions referred to in sub-
31 section (b) of section 1602 of the Implementing Recommendations
32 of the 9/11 Commission Act of 2007 (Public Law 110–53, 121
33 Stat. 479).

34 (5) REGULATIONS.—The Secretary shall issue a final rule as a per-
35 manent regulation to implement this subsection in accordance with
36 chapter 5 of title 5.

37 (h) DEPLOYMENT OF ARMED LAW ENFORCEMENT PERSONNEL.—

38 (1) IN GENERAL.—The Administrator shall order the deployment of
39 law enforcement personnel authorized to carry firearms at each airport
40 security screening location to ensure passenger safety and national se-
41 curity.

1 (2) MINIMUM REQUIREMENTS.—Except at airports required to enter
2 into agreements under subsection (c), the Administrator shall order the
3 deployment of at least one law enforcement officer at each airport secu-
4 rity screening location. At the 100 largest airports in the United
5 States, in terms of annual passenger enplanements for the most recent
6 calendar year for which data are available, the Secretary shall order
7 the deployment of additional law enforcement personnel at airport secu-
8 rity screening locations if the Administrator determines that the addi-
9 tional deployment is necessary to ensure passenger safety and national
10 security.

11 (i) EXEMPTIONS AND ADVISING CONGRESS ON REGULATIONS.—The Ad-
12 ministrator—

13 (1) may exempt from this section air transportation operations, ex-
14 cept scheduled passenger operations of an air carrier providing air
15 transportation under a certificate issued under section 41102 of title
16 49 or a permit issued under section 41302 of title 49; and

17 (2) shall advise Congress of a regulation to be prescribed under this
18 section at least 30 days before the effective date of the regulation, un-
19 less the Administrator decides an emergency exists requiring the regu-
20 lation to become effective in fewer than 30 days and notifies Congress
21 of that decision.

22 (j) BLAST-RESISTANT CARGO CONTAINERS.—

23 (1) IN GENERAL.—The Administrator shall—

24 (A) evaluate the results of the blast-resistant cargo container
25 pilot program that was initiated before August 3, 2007; and

26 (B) prepare and distribute through the Aviation Security Advi-
27 sory Committee to the appropriate committees of Congress and air
28 carriers a report on that evaluation, which may contain nonclassi-
29 fied and classified sections.

30 (2) ACQUISITION, MAINTENANCE, AND REPLACEMENT.—On comple-
31 tion and consistent with the results of the evaluation that paragraph
32 (1)(A) requires, the Administrator shall—

33 (A) develop and implement a program, as the Administrator de-
34 termines appropriate, to acquire, maintain, and replace blast-re-
35 sistant cargo containers;

36 (B) pay for the program; and

37 (C) make available blast-resistant cargo containers to air car-
38 riers under paragraph (3).

39 (3) DISTRIBUTION TO AIR CARRIERS.—The Administrator shall make
40 available blast-resistant cargo containers to air carriers for use on a
41 risk-managed basis as determined by the Secretary.

- 1 (k) GENERAL AVIATION AIRPORT SECURITY PROGRAM.—
- 2 (1) IN GENERAL.—The Administrator shall—
- 3 (A) develop a standardized threat and vulnerability assessment
- 4 program for general aviation airports; and
- 5 (B) implement a program to perform the assessments on a risk-
- 6 managed basis at general aviation airports.
- 7 (2) GRANT PROGRAM.—The Administrator shall complete a study of
- 8 the feasibility of a program, based on a risk-managed approach, to pro-
- 9 vide grants to operators of general aviation airports for projects to up-
- 10 grade security at the airports. If the Secretary determines that a pro-
- 11 gram is feasible, the Secretary shall establish a program.
- 12 (3) REQUIRED SUBMISSIONS BY GENERAL AVIATION AIRCRAFT.—The
- 13 Administrator shall develop a risk-based system under which—
- 14 (A) general aviation aircraft, as identified by the Administrator,
- 15 in coordination with the Administrator of the Federal Aviation Ad-
- 16 ministration, are required to submit passenger information and
- 17 advance notification requirements for U. S. Customs and Border
- 18 Protection before entering United States airspace; and
- 19 (B) the information is checked against appropriate databases.
- 20 (l) LIMITATIONS ON USE OF ADVANCED IMAGING TECHNOLOGY FOR
- 21 SCREENING PASSENGERS.—
- 22 (1) DEFINITIONS.—In this subsection:
- 23 (A) ADVANCED IMAGING TECHNOLOGY.—The term “advanced
- 24 imaging technology”—
- 25 (i) means a device used in the screening of passengers that
- 26 creates a visual image of an individual showing the surface
- 27 of the skin and revealing other objects on the body; and
- 28 (ii) may include devices using backscatter x-rays or milli-
- 29 meter waves and devices referred to as “whole-body imaging
- 30 technology” or “body scanning machines”.
- 31 (B) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term
- 32 “appropriate congressional committees” means—
- 33 (i) the Committee on Commerce, Science, and Transpor-
- 34 tation and the Committee on Homeland Security and Govern-
- 35 mental Affairs of the Senate; and
- 36 (ii) the Committee on Homeland Security of the House of
- 37 Representatives.
- 38 (C) AUTOMATIC TARGET RECOGNITION SOFTWARE.—The term
- 39 “automatic target recognition software” means software installed
- 40 on an advanced imaging technology that produces a generic image

1 of the individual being screened that is the same as the images
2 produced for all other screened individuals.

3 (2) USE OF ADVANCED IMAGING TECHNOLOGY.—The Administrator
4 shall ensure that an advanced imaging technology used for the screen-
5 ing of passengers under this section—

6 (A) is equipped with and employs automatic target recognition
7 software; and

8 (B) complies with other requirements the Administrator deter-
9 mines necessary to address privacy considerations.

10 **§ 40912. Refusal to transport passengers and property**

11 (a) MANDATORY REFUSAL.—The Administrator shall prescribe regula-
12 tions requiring an air carrier, intrastate air carrier, or foreign air carrier
13 to refuse to transport—

14 (1) a passenger who does not consent to a search under section
15 40911(a) of this title establishing whether the passenger is carrying
16 unlawfully a dangerous weapon, explosive, or other destructive sub-
17 stance; or

18 (2) property of a passenger who does not consent to a search of the
19 property establishing whether the property unlawfully contains a dan-
20 gerous weapon, explosive, or other destructive substance.

21 (b) PERMISSIVE REFUSAL.—Subject to regulations of the Administrator,
22 an air carrier, intrastate air carrier, or foreign air carrier may refuse to
23 transport a passenger or property the carrier decides is, or might be, inim-
24 ical to safety.

25 (c) AGREEING TO CONSENT TO SEARCH.—An agreement to carry pas-
26 sengers or property in air transportation or intrastate air transportation by
27 an air carrier, intrastate air carrier, or foreign air carrier is deemed to in-
28 clude an agreement that the passenger or property will not be carried if con-
29 sent to search the passenger or property for a purpose referred to in this
30 section is not given.

31 **§ 40913. Air transportation security**

32 (a) DEFINITION OF LAW ENFORCEMENT PERSONNEL.—In this section,
33 “law enforcement personnel” means individuals—

34 (1) authorized to carry and use firearms;

35 (2) vested with the degree of the police power of arrest the Adminis-
36 trator considers necessary to carry out this section; and

37 (3) identifiable by appropriate indicia of authority.

38 (b) PROTECTION AGAINST VIOLENCE AND PIRACY.—The Administrator
39 shall prescribe regulations to protect passengers and property on an aircraft
40 operating in air transportation or intrastate air transportation against an

1 act of criminal violence or aircraft piracy. When prescribing a regulation
2 under this subsection, the Administrator shall—

3 (1) consult with the Secretary of Transportation, the Attorney Gen-
4 eral, the heads of other departments, agencies, and instrumentalities of
5 the United States Government, and State and local authorities;

6 (2) consider whether a proposed regulation is consistent with—

7 (A) protecting passengers; and

8 (B) the public interest in promoting air transportation and
9 intrastate air transportation;

10 (3) to the maximum extent practicable, require a uniform procedure
11 for searching and detaining passengers and property to ensure—

12 (A) their safety; and

13 (B) courteous and efficient treatment by an air carrier, an
14 agent or employee of an air carrier, and Government, State, and
15 local law enforcement personnel carrying out this section; and

16 (4) consider the extent to which a proposed regulation will carry out
17 this section.

18 (c) SECURITY PROGRAMS.—

19 (1) IN GENERAL.—The Administrator shall prescribe regulations
20 under subsection (b) that require each operator of an airport regularly
21 serving an air carrier holding a certificate issued by the Secretary of
22 Transportation to establish an air transportation security program that
23 provides a law enforcement presence and capability at each of those
24 airports that is adequate to ensure the safety of passengers. The regu-
25 lations shall authorize the operator to use the services of qualified
26 State, local, and private law enforcement personnel. When the Adminis-
27 trator decides, after being notified by an operator in the form the Ad-
28 ministrator prescribes, that not enough qualified State, local, and pri-
29 vate law enforcement personnel are available to carry out subsection
30 (b), the Administrator may authorize the operator to use, on a reim-
31 bursable basis, personnel employed by the Administrator, or by another
32 department, agency, or instrumentality of the Government with the
33 consent of the head of the department, agency, or instrumentality, to
34 supplement State, local, and private law enforcement personnel. When
35 deciding whether additional personnel are needed, the Administrator
36 shall consider the number of passengers boarded at the airport, the ex-
37 tent of anticipated risk of criminal violence or aircraft piracy at the air-
38 port or to the air carrier aircraft operations at the airport, and the
39 availability of qualified State or local law enforcement personnel at the
40 airport.

41 (2) INCLUSION OF AIRPORT TENANT SECURITY PROGRAM.—

1 (A) IN GENERAL.—The Administrator may approve a security
2 program of an airport operator, or an amendment to an existing
3 program, that incorporates a security program of an airport ten-
4 ant (except an air carrier separately complying with part 108 or
5 129 of title 14, Code of Federal Regulations) having access to a
6 secured area of the airport, if the program or amendment incor-
7 porates—

8 (i) the measures the tenant will use, within the tenant's
9 leased areas or areas designated for the tenant's exclusive use
10 under an agreement with the airport operator, to carry out
11 the security requirements imposed by the Administrator on
12 the airport operator under the access control system require-
13 ments of section 107.14 of title 14, Code of Federal Regula-
14 tions, or under other requirements of part 107 of title 14;
15 and

16 (ii) the methods the airport operator will use to monitor
17 and audit the tenant's compliance with the security require-
18 ments and provides that the tenant will be required to pay
19 monetary penalties to the airport operator if the tenant fails
20 to carry out a security requirement under a contractual provi-
21 sion or requirement imposed by the airport operator.

22 (B) OPERATOR NOT IN VIOLATION.—If the Administrator ap-
23 proves a program or amendment described in subparagraph (A),
24 the airport operator may not be found to be in violation of a re-
25 quirement of this subsection or subsection (b) when the airport op-
26 erator demonstrates that the tenant or an employee, permittee, or
27 invitee of the tenant is responsible for the violation and that the
28 airport operator has complied with all measures in its security pro-
29 gram for securing compliance with its security program by the
30 tenant.

31 (C) MAXIMUM USE OF CHEMICAL AND BIOLOGICAL WEAPONS
32 DETECTION EQUIPMENT.—The Secretary of Transportation may
33 require airports to maximize the use of technology and equipment
34 that is designed to detect or neutralize potential chemical or bio-
35 logical weapons.

36 (3) PILOT PROGRAMS.—The Administrator shall establish pilot pro-
37 grams in no fewer than 20 airports to test and evaluate new and
38 emerging technology for providing access control and other security
39 protections for closed or secure areas of the airports. The technology
40 may include biometric or other technology that ensures only authorized
41 access to secure areas.

1 (d) AUTHORIZING INDIVIDUALS TO CARRY FIREARMS AND MAKE AR-
2 RESTS.—With the approval of the Attorney General and the Secretary of
3 State, the Administrator may authorize an individual who carries out air
4 transportation security duties—

5 (1) to carry firearms; and

6 (2) to make arrests without warrant for an offense against the
7 United States committed in the presence of the individual or for a fel-
8 ony under the laws of the United States, if the individual reasonably
9 believes the individual to be arrested has committed or is committing
10 a felony.

11 (e) EXCLUSIVE RESPONSIBILITY OVER PASSENGER SAFETY.—The Ad-
12 ministrator has the exclusive responsibility to direct law enforcement activity
13 related to the safety of passengers on an aircraft involved in an offense
14 under section 41062 of this title from the moment all external doors of the
15 aircraft are closed following boarding until those doors are opened to allow
16 passengers to leave the aircraft. When requested by the Administrator,
17 other departments, agencies, and instrumentalities of the Government shall
18 provide assistance necessary to carry out this subsection.

19 (f) GOVERNMENT AND INDUSTRY CONSORTIA.—The Administrator may
20 establish at airports consortia of government and aviation industry rep-
21 resentatives to provide advice on matters related to aviation security and
22 safety. The consortia shall not be considered Federal advisory committees
23 for purposes of chapter 10 of title 5.

24 (g) IMPROVEMENT OF SECURED-AREA ACCESS CONTROL.—

25 (1) EMPLOYEE SANCTIONS.—

26 (A) PUBLICATION.—The Administrator shall publish in the
27 Federal Register a list of sanctions for use as guidelines in the
28 discipline of employees for infractions of airport access control re-
29 quirements.

30 (B) DISCIPLINARY APPROACH.—The guidelines shall incorporate
31 a progressive disciplinary approach that relates proposed sanctions
32 to the severity or recurring nature of the infraction and shall in-
33 clude measures such as remedial training, suspension from secu-
34 rity-related duties, suspension from all duties without pay, and
35 termination of employment.

36 (C) USE.—Each airport operator, air carrier, and security
37 screening company shall include the list of sanctions published by
38 the Administrator in its security program. The security program
39 shall include a process for taking prompt disciplinary action
40 against an employee who commits an infraction of airport access
41 control requirements.

1 (2) ACTIONS TO IMPROVE ACCESS CONTROL.—The Administrator
2 shall—

3 (A) work with airport operators and air carriers to implement
4 and strengthen existing controls to eliminate airport access control
5 weaknesses;

6 (B) require airport operators and air carriers to develop and im-
7 plement comprehensive and recurring training programs that
8 teach employees their roles in airport security, the importance of
9 their participation, how their performance will be evaluated, and
10 what action will be taken if they fail to perform;

11 (C) require airport operators and air carriers to develop and im-
12 plement programs that foster and reward compliance with airport
13 access control requirements and discourage and penalize non-
14 compliance in accordance with guidelines issued by the Adminis-
15 trator to measure employee compliance;

16 (D) on an ongoing basis, assess and test for compliance with
17 access control requirements, report annually findings of the assess-
18 ments, and assess the effectiveness of penalties in ensuring compli-
19 ance with security procedures and take other appropriate enforce-
20 ment actions when noncompliance is found;

21 (E) improve and better administer the Administrator’s security
22 database to ensure its efficiency, reliability, and usefulness for
23 identification of systemic problems and allocation of resources;

24 (F) improve the execution of the Administrator’s quality control
25 program; and

26 (G) work with airport operators to strengthen access control
27 points in secured areas (including air traffic control operations
28 areas, maintenance areas, crew lounges, baggage handling areas,
29 concessions, and catering delivery areas) to ensure the security of
30 passengers and aircraft and consider the deployment of biometric
31 or similar technologies that identify individuals based on unique
32 personal characteristics.

33 (h) IMPROVED AIRPORT PERIMETER ACCESS SECURITY.—

34 (1) DEFINITIONS.—In this subsection:

35 (A) BIOMETRIC IDENTIFIER.—The term “biometric identifier”
36 means a technology that enables the automated identification, or
37 verification of the identity, of an individual based on biometric in-
38 formation.

39 (B) BIOMETRIC IDENTIFIER INFORMATION.—The term “biomet-
40 ric identifier information” means the distinct physical or behav-

1 ioral characteristics of an individual that are used for unique iden-
2 tification, or verification of the identity, of an individual.

3 (C) FAILURE TO ENROLL.—The term “failure to enroll” means
4 the inability of an individual to enroll in a biometric identifier sys-
5 tem due to an insufficiently distinctive biometric sample, the lack
6 of a body part necessary to provide the biometric sample, a system
7 design that makes it difficult to provide consistent biometric iden-
8 tifier information, or other factors.

9 (D) FALSE MATCH.—The term “false match” means the incor-
10 rect matching of one individual’s biometric identifier information
11 to another individual’s biometric identifier information by a bio-
12 metric identifier system.

13 (E) FALSE NON-MATCH.—The term “false non-match” means
14 the rejection of a valid identity by a biometric identifier system.

15 (F) SECURE AREA OF AN AIRPORT.—The term “secure area of
16 an airport” means the sterile area and the Security Identification
17 Display Area of an airport (as the terms are defined in section
18 1540.5 of title 49, Code of Federal Regulations, or a successor
19 regulation to that section).

20 (2) IN GENERAL.—The Administrator, in consultation with the air-
21 port operator and law enforcement authorities, may order the deploy-
22 ment of necessary personnel at a secure area of the airport to counter
23 the risk of criminal violence, the risk of aircraft piracy at the airport,
24 or the risk to air carrier aircraft operations at the airport, or to meet
25 national security concerns.

26 (3) CONSIDERATION OF SECURITY OF AIRCRAFT AND GROUND AC-
27 CESS TO SECURE AREAS.—In determining where to deploy the per-
28 sonnel, the Administrator shall consider the physical security needs of
29 air traffic control facilities, parked aircraft, aircraft servicing equip-
30 ment, aircraft supplies (including fuel), automobile parking facilities
31 within airport perimeters or adjacent to secured facilities, and access
32 and transition areas at airports served by other means of ground or
33 water transportation.

34 (4) DEPLOYMENT OF FEDERAL LAW ENFORCEMENT PERSONNEL.—
35 The Secretary may enter into a memorandum of understanding or
36 other agreement with the Attorney General or the head of another ap-
37 propriate Federal law enforcement agency to deploy Federal law en-
38 forcement personnel at an airport in order to meet aviation safety and
39 security concerns.

40 (5) AIRPORT PERIMETER SCREENING.—The Administrator shall—

1 (A) require screening or inspection of all individuals, goods,
2 property, vehicles, and other equipment before entry into a secured
3 area of an airport in the United States described in subsection (e);

4 (B) prescribe specific requirements for the screening and inspec-
5 tion that will ensure at least the same level of protection as will
6 result from screening of passengers and their baggage;

7 (C) establish procedures to ensure the safety and integrity of—

8 (i) all persons providing services with respect to aircraft
9 providing passenger air transportation or intrastate air trans-
10 portation and facilities of those persons at an airport in the
11 United States described in subsection (e);

12 (ii) all supplies, including catering and passenger ameni-
13 ties, placed aboard the aircraft, including the sealing of sup-
14 plies to ensure easy visual detection of tampering; and

15 (iii) all persons providing the supplies and facilities of those
16 persons;

17 (D) require vendors having direct access to the airfield and air-
18 craft to develop security programs; and

19 (E) issue guidance for the use of biometric or other technology
20 that positively verifies the identity of each employee and law en-
21 forcement officer who enters a secure area of an airport.

22 (6) USE OF BIOMETRIC TECHNOLOGY IN AIRPORT ACCESS CONTROL
23 SYSTEMS.—In issuing guidance under paragraph (5)(E), the Adminis-
24 trator in consultation with representatives of the aviation industry, the
25 biometric identifier industry, and the National Institute of Standards
26 and Technology, shall establish, at a minimum—

27 (A) comprehensive technical and operational system require-
28 ments and performance standards for the use of biometric identi-
29 fier technology in airport access control systems (including airport
30 perimeter access control systems) to ensure that the biometric
31 identifier systems are effective, reliable, and secure;

32 (B) a list of products and vendors that meet the requirements
33 and standards set forth in subparagraph (A);

34 (C) procedures for implementing biometric identifier systems—

35 (i) to ensure that individuals do not use an assumed iden-
36 tity to enroll in a biometric identifier system; and

37 (ii) to resolve failures to enroll, false matches, and false
38 nonmatches; and

39 (D) best practices for incorporating biometric identifier tech-
40 nology into airport access control systems in the most effective
41 manner, including a process to best utilize existing airport access

1 control systems, facilities, and equipment, and existing data net-
2 works connecting airports.

3 (7) USE OF BIOMETRIC TECHNOLOGY FOR ARMED LAW ENFORCE-
4 MENT TRAVEL.—

5 (A) IN GENERAL.—The Secretary, in consultation with the At-
6 torney General, shall—

7 (i) implement this paragraph by publication in the Federal
8 Register; and

9 (ii) establish a national registered armed law enforcement
10 program, that shall be federally managed, for law enforce-
11 ment officers needing to be armed when traveling by commer-
12 cial aircraft.

13 (B) PROGRAM REQUIREMENTS.—The program shall—

14 (i) establish a credential or a system that incorporates bio-
15 metric technology and other applicable technologies;

16 (ii) establish a system for law enforcement officers who
17 need to be armed when traveling by commercial aircraft on
18 a regular basis and for those who need to be armed during
19 temporary travel assignments;

20 (iii) comply with other uniform credentialing initiatives, in-
21 cluding the Homeland Security Presidential Directive–12;

22 (iv) apply to all Federal, State, local, tribal, and territorial
23 government law enforcement agencies; and

24 (v) establish a process by which the travel credential or sys-
25 tem may be used to verify the identity, using biometric tech-
26 nology, of a Federal, State, local, tribal, or territorial law en-
27 forcement officer seeking to carry a weapon on board a com-
28 mercial aircraft, without unnecessarily disclosing to the public
29 that the individual is a law enforcement officer.

30 (C) PROCEDURES.—In establishing the program, the Secretary
31 shall develop procedures—

32 (i) to ensure that a law enforcement officer of a Federal,
33 State, local, tribal, or territorial government flying armed has
34 a specific reason for flying armed and the reason is within
35 the scope of the duties of the officer;

36 (ii) to preserve the anonymity of the armed law enforce-
37 ment officer;

38 (iii) to resolve failures to enroll, false matches, and false
39 nonmatches relating to the use of the law enforcement travel
40 credential or system;

1 (iv) to determine the method of issuance of the biometric
2 credential to law enforcement officers needing to be armed
3 when traveling by commercial aircraft;

4 (v) to invalidate a law enforcement travel credential or sys-
5 tem that is lost, stolen, or no longer authorized for use;

6 (vi) to coordinate the program with the Federal Air Mar-
7 shal Service, including the force multiplier program of the
8 Service; and

9 (vii) to implement a phased approach to launching the pro-
10 gram, addressing the immediate needs of the relevant Federal
11 agent population before expanding the program to other law
12 enforcement populations.

13 (i) AUTHORITY TO ARM FLIGHT DECK CREW WITH LESS-THAN-LETHAL
14 WEAPONS.—

15 (1) IN GENERAL.—If the Administrator, after receiving the rec-
16 ommendations of the National Institute of Justice, determines, with the
17 approval of the Attorney General and the Secretary of State, that it
18 is appropriate and necessary and would effectively serve the public in-
19 terest in avoiding air piracy, the Administrator may authorize members
20 of the flight deck crew on an aircraft providing air transportation or
21 intrastate air transportation to carry a less-than-lethal weapon while
22 the aircraft is engaged in providing the transportation.

23 (2) USAGE.—If the Administrator grants authority under paragraph
24 (1) for flight deck crew members to carry a less-than-lethal weapon
25 while engaged in providing air transportation or intrastate air trans-
26 portation, the Administrator shall—

27 (A) prescribe rules requiring that the crew member be trained
28 in the proper use of the weapon; and

29 (B) prescribe guidelines setting forth the circumstances under
30 which weapons may be used.

31 (3) REQUEST OF AIR CARRIERS TO USE LESS-THAN-LETHAL WEAP-
32 ONS.—If the Administrator receives a request from an air carrier for
33 authorization to allow pilots of the air carrier to carry less-than-lethal
34 weapons, the Administrator shall respond to that request within 90
35 days.

36 (j) SHORT-TERM ASSESSMENT AND DEPLOYMENT OF EMERGING SECU-
37 RITY TECHNOLOGIES AND PROCEDURES.—

38 (1) DEFINITION OF SECURE AREA OF AN AIRPORT.—In this sub-
39 section, the term “secure area of an airport” means the sterile area
40 and the Security Identification Display Area of an airport (as the

1 terms are defined in section 1540.5 of title 49, Code of Federal Regu-
2 lations, or a successor regulation to that section).

3 (2) IN GENERAL.—The Administrator shall periodically recommend
4 to airport operators commercially available measures or procedures to
5 prevent access to secure airport areas by unauthorized persons.

6 (3) SECURE FLIGHT PROGRAM.—

7 (A) IN GENERAL.—The Administrator shall ensure that the Se-
8 cure Flight Program, or a successor program—

9 (i) is used to evaluate all passengers before they board an
10 aircraft; and

11 (ii) includes procedures to ensure that individuals selected
12 by the program and their carry-on and checked baggage are
13 adequately screened.

14 (B) MODIFICATIONS.—The Administrator may modify a re-
15 quirement under the Secure Flight Program for flights that origi-
16 nate and terminate in the same State, if the Administrator deter-
17 mines that—

18 (i) the State has extraordinary air transportation needs or
19 concerns due to its isolation and dependence on air transpor-
20 tation; and

21 (ii) the routine characteristics of passengers, given the na-
22 ture of the market, regularly triggers primary selectee status.

23 (C) ADVANCED AIRLINE PASSENGER PRESCREENING.—

24 (i) TESTING.—The Administrator shall commence testing
25 of an advanced passenger prescreening system that will allow
26 the Department to assume the performance of comparing
27 passenger information, as defined by the Administrator, to
28 the automatic selectee and no fly lists, utilizing all appro-
29 priate records in the consolidated and integrated terrorist
30 watchlist maintained by the Federal Government.

31 (ii) ASSUMPTION OF PERFORMANCE.—After completion of
32 testing under clause (i), the Administrator, or the designee of
33 the Administrator, shall begin to assume the performance of
34 the passenger prescreening function of comparing passenger
35 information to the automatic selectee and no fly lists and uti-
36 lize all appropriate records in the consolidated and integrated
37 terrorist watchlist maintained by the Federal Government in
38 performing that function.

39 (iii) DUTIES IN ASSUMING PERFORMANCE.—In assuming
40 performance of the function under clause (ii), the Adminis-
41 trator shall—

1 (I) establish a procedure to enable airline passengers,
2 who are delayed or prohibited from boarding a flight be-
3 cause the advanced passenger prescreening system deter-
4 mined that they might pose a security threat, to appeal
5 a determination and correct information contained in the
6 system;

7 (II) ensure that Federal Government databases that
8 will be used to establish the identity of a passenger
9 under the system will not produce a large number of
10 false positives;

11 (III) establish an internal oversight board to oversee
12 and monitor the manner in which the system is being
13 implemented;

14 (IV) establish sufficient operational safeguards to re-
15 duce the opportunities for abuse;

16 (V) implement substantial security measures to pro-
17 tect the system from unauthorized access;

18 (VI) adopt policies establishing effective oversight of
19 the use and operation of the system; and

20 (VII) ensure that there are no specific privacy con-
21 cerns with the technological architecture of the system.

22 (iv) REQUIREMENT TO PROVIDE PASSENGER INFORMA-
23 TION.—After the completion of the testing of the advanced
24 passenger prescreening system, the Administrator, by order
25 or interim final rule—

26 (I) shall require air carriers to supply to the Adminis-
27 trator the passenger information needed to begin imple-
28 menting the advanced passenger prescreening system;
29 and

30 (II) shall require entities that provide systems and
31 services to air carriers in the operation of air carrier res-
32 ervations systems to provide to air carriers passenger in-
33 formation in possession of the entities, but only to the
34 extent necessary to comply with subclause (I).

35 (v) INCLUSION OF DETAINEE ON NO FLY LIST.—

36 (I) DEFINITION OF DETAINEE.—For purposes of this
37 clause, the term “detainee” means an individual in the
38 custody or under the physical control of the United
39 States as a result of armed conflict.

40 (II) IN GENERAL.—The Administrator, in coordination
41 with the Terrorist Screening Center, shall include on the

1 No Fly List an individual who was a detainee held at the
2 Naval Station, Guantanamo Bay, Cuba, unless the Presi-
3 dent certifies in writing to Congress that the detainee
4 poses no threat to the United States, its citizens, or its
5 allies.

6 (D) SCREENING OF EMPLOYEES AGAINST WATCHLIST.—The
7 Administrator, in coordination with the Secretary of Transpor-
8 tation and the Administrator of the Federal Aviation Administra-
9 tion, shall ensure that individuals are screened against all appro-
10 priate records in the consolidated and integrated terrorist
11 watchlist maintained by the Federal Government before—

12 (i) being certificated by the Federal Aviation Administra-
13 tion;

14 (ii) being granted unescorted access to the secure area of
15 an airport; or

16 (iii) being granted unescorted access to the air operations
17 area (as defined in section 1540.5 of title 49, Code of Federal
18 Regulations, or a successor regulation to that section) of an
19 airport.

20 (E) AIRCRAFT CHARTER CUSTOMER AND LESSEE
21 PRESCREENING.—

22 (i) ESTABLISHMENT.—The Administrator shall establish a
23 process by which operators of aircraft to be used in charter
24 air transportation with a maximum takeoff weight greater
25 than 12,500 pounds and lessors of aircraft with a maximum
26 takeoff weight greater than 12,500 pounds may—

27 (I) request the Department to use the advanced pas-
28 senger prescreening system to compare information
29 about an individual seeking to charter an aircraft with
30 a maximum takeoff weight greater than 12,500 pounds,
31 a passenger proposed to be transported aboard the air-
32 craft, and an individual seeking to lease an aircraft with
33 a maximum takeoff weight greater than 12,500 pounds,
34 to the automatic selectee and no fly lists, utilizing all ap-
35 propriate records in the consolidated and integrated ter-
36 rorist watchlist maintained by the Federal Government;
37 and

38 (II) refuse to charter or lease an aircraft with a max-
39 imum takeoff weight greater than 12,500 pounds to, or
40 transport aboard the aircraft, individuals identified on
41 the watch list.

1 (ii) APPLICABILITY.—The requirements of subparagraph
2 (C)(iii) apply to this subparagraph.

3 (iii) DESIGN AND REVIEW OF GUIDELINES, POLICIES, AND
4 OPERATING PROCEDURES.—The Secretary, in consultation
5 with the Terrorist Screening Center, shall design and review,
6 as necessary, guidelines, policies, and operating procedures
7 for the collection, removal, and updating of data maintained,
8 or to be maintained, in the no fly and automatic selectee lists.

9 (F) APPLICABILITY.—Section 607 of the Vision 100—Century
10 of Aviation Reauthorization Act (Public Law 108–176, 117 Stat.
11 2568) does not apply to the advanced passenger prescreening sys-
12 tem established under subparagraph (C).

13 (G) APPEAL PROCEDURES.—

14 (i) ESTABLISHMENT.—The Administrator shall establish a
15 timely and fair process for individuals identified as a threat
16 under one or more of subparagraphs (C), (D), and (E) to ap-
17 peal to the Transportation Security Administration the deter-
18 mination and correct erroneous information.

19 (ii) MAINTENANCE OF RECORD OF MISIDENTIFIED INDIVID-
20 UALS.—The process shall include the establishment of a
21 method by which the Administrator will be able to maintain
22 a record of air passengers and other individuals who have
23 been misidentified and have corrected erroneous information.
24 To prevent repeated delays of misidentified passengers and
25 other individuals, the Transportation Security Administration
26 record shall contain information determined by the Adminis-
27 trator to authenticate the identity of such a passenger or in-
28 dividual.

29 (k) LIMITATION ON LIABILITY FOR ACTS TO THWART CRIMINAL VIO-
30 LENCE OR AIRCRAFT PIRACY.—An individual is not liable for damages in
31 an action brought in a Federal or State court arising out of the acts of the
32 individual in attempting to thwart an act of criminal violence or piracy on
33 an aircraft if that individual reasonably believed that an act of criminal vio-
34 lence or piracy was occurring or was about to occur.

35 (l) AIR CHARTER PROGRAM.—

36 (1) IN GENERAL.—The Administrator shall implement an aviation
37 security program for charter air carriers with a maximum certificated
38 takeoff weight of more than 12,500 pounds.

39 (2) EXEMPTION FOR ARMED FORCES CHARTERS.—

1 (A) DEFINITION OF ARMED FORCES.—In this paragraph, the
2 term “armed forces” has the meaning given the term in section
3 101(a)(4) of title 10.

4 (B) IN GENERAL.—Paragraph (1) and the other requirements
5 of this chapter do not apply to passengers and property carried
6 by aircraft when employed to provide charter transportation to
7 members of the armed forces.

8 (C) SECURITY PROCEDURES.—The Secretary of Defense, in
9 consultation with the Secretary and the Secretary of Transpor-
10 tation, shall establish security procedures relating to the operation
11 of aircraft when employed to provide charter transportation to
12 members of the armed forces to or from an airport described in
13 subsection (c).

14 (m) SECURITY SCREENING FOR MEMBERS OF THE ARMED FORCES.—

15 (1) IN GENERAL.—The Administrator, in consultation with the De-
16 partment of Defense, shall develop and implement a plan to provide ex-
17 pedited security screening services for a member of the armed forces,
18 and, to the extent possible, an accompanying family member, if the
19 member of the armed forces, while in uniform, presents documentation
20 indicating official orders for air transportation departing from a pri-
21 mary airport (as defined in section 47102 of title 49).

22 (2) PROTOCOLS.—In developing the plan, the Administrator shall
23 consider—

24 (A) leveraging existing security screening models used to reduce
25 passenger wait times;

26 (B) establishing standard guidelines for the screening of mili-
27 tary uniform items, including combat boots; and

28 (C) incorporating new screening protocols into an existing trust-
29 ed passenger program, as established under section 109(a)(3) of
30 the Aviation and Transportation Security Act (Public Law 107–
31 71, 115 Stat. 613), or into the development of a new credential
32 or system that incorporates biometric technology and other appli-
33 cable technologies to verify the identity of individuals traveling in
34 air transportation.

35 (3) RULE OF CONSTRUCTION.—Nothing in this subsection shall af-
36 fect the authority of the Administrator to require additional screening
37 of a member of the armed forces if intelligence or law enforcement in-
38 formation indicates that additional screening is necessary.

39 (4) REPORT.—The Administrator shall submit to the appropriate
40 committees of Congress a report on the implementation of the plan.

41 (n) PASSENGER EXIT POINTS FROM STERILE AREA.—

1 (1) DEFINITION OF STERILE AREA.—In this subsection, the term
2 “sterile area” has the meaning given the term in section 1540.5 of title
3 49, Code of Federal Regulations, or any corresponding similar regula-
4 tion or ruling.

5 (2) IN GENERAL.—The Secretary shall ensure that the Transpor-
6 tation Security Administration is responsible for monitoring passenger
7 exit points from the sterile area of airports at which the Transportation
8 Security Administration provided the monitoring as of December 1,
9 2013.

10 **§ 40914. Domestic air transportation system security**

11 (a) ASSESSING THREATS.—The Administrator and the Director of the
12 Federal Bureau of Investigation jointly shall assess current and potential
13 threats to the domestic air transportation system. The assessment shall in-
14 clude consideration of the extent to which there are individuals with the ca-
15 pability and intent to carry out terrorist or related unlawful acts against
16 that system and the ways in which those individuals might carry out those
17 acts. The Administrator and the Director jointly shall decide on and carry
18 out the most effective method for continuous analysis and monitoring of se-
19 curity threats to that system.

20 (b) ASSESSING SECURITY.—In coordination with the Director of the Fed-
21 eral Bureau of Investigation, the Administrator shall carry out periodic
22 threat and vulnerability assessments on security at each airport that is part
23 of the domestic air transportation system. Each assessment shall include
24 consideration of—

25 (1) the adequacy of security procedures related to the handling and
26 transportation of checked baggage and cargo;

27 (2) space requirements for security personnel and equipment;

28 (3) separation of screened and unscreened passengers, baggage, and
29 cargo;

30 (4) separation of the controlled and uncontrolled areas of airport fa-
31 cilities; and

32 (5) coordination of the activities of security personnel of the Trans-
33 portation Security Administration, U.S. Customs and Border Protec-
34 tion, U.S. Immigration and Customs Enforcement, and air carriers,
35 and of other law enforcement personnel.

36 (c) MODAL SECURITY PLAN FOR AVIATION.—In addition to the require-
37 ments set forth in paragraphs (2) through (6) of section 11514(c) of this
38 title, the modal security plan for aviation prepared under section 11514 of
39 this title shall—

40 (1) establish a damage mitigation and recovery plan for the aviation
41 system in the event of a terrorist attack; and

1 (2) include a threat matrix document that outlines each threat to the
2 United States civil aviation system and the corresponding layers of se-
3 curity in place to address the threat.

4 (d) OPERATIONAL CRITERIA.—The Administrator shall issue operational
5 criteria to protect airport infrastructure and operations against the threats
6 identified in the plans prepared under section 11514(a) of this title and
7 shall approve best practices guidelines for airport assets.

8 (e) IMPROVING SECURITY.—The Administrator shall take necessary ac-
9 tions to improve domestic air transportation security by correcting defi-
10 ciencies in that security discovered in the assessments, analyses, and moni-
11 toring carried out under this section.

12 **§ 40915. Information about threats to civil aviation**

13 (a) PROVIDING INFORMATION.—Under guidelines the Administrator pre-
14 scribes, an air carrier, airport operator, ticket agent, or individual employed
15 by an air carrier, airport operator, or ticket agent, receiving information
16 (except a communication directed by the United States Government) about
17 a threat to civil aviation shall provide the information promptly to the Ad-
18 ministrator.

19 (b) FLIGHT CANCELLATION.—If a decision is made that a particular
20 threat cannot be addressed in a way adequate to ensure, to the extent fea-
21 sible, the safety of passengers and crew of a particular flight or series of
22 flights, the Administrator shall cancel the flight or series of flights.

23 (c) GUIDELINES ON PUBLIC NOTICE.—

24 (1) IN GENERAL.—The President shall develop guidelines for ensur-
25 ing that public notice is provided in appropriate cases about threats to
26 civil aviation. The guidelines shall identify officials responsible for—

27 (A) deciding, on a case-by-case basis, if public notice of a threat
28 is in the best interest of the United States and the traveling pub-
29 lic;

30 (B) ensuring that public notice is provided in a timely and effec-
31 tive way, including the use of a toll-free telephone number; and

32 (C) canceling the departure of a flight or series of flights under
33 subsection (b).

34 (2) CONTENTS.—The guidelines shall provide for consideration of—

35 (A) the specificity of the threat;

36 (B) the credibility of intelligence information related to the
37 threat;

38 (C) the ability to counter the threat effectively;

39 (D) the protection of intelligence information sources and meth-
40 ods;

1 (E) cancellation, by an air carrier or the Administrator, of a
2 flight or series of flights instead of public notice;

3 (F) the ability of passengers and crew to take steps to reduce
4 the risk to their safety after receiving public notice of a threat;
5 and

6 (G) other factors the Administrator considers appropriate.

7 (d) GUIDELINES ON NOTICE TO CREWS.—The Administrator shall de-
8 velop guidelines for ensuring that notice in appropriate cases of threats to
9 the security of an air carrier flight is provided to the flight crew and cabin
10 crew of that flight.

11 (e) LIMITATION ON NOTICE TO SELECTIVE TRAVELERS.—Notice of a
12 threat to civil aviation may be provided to selective potential travelers only
13 if the threat applies only to those travelers.

14 (f) RESTRICTING ACCESS TO INFORMATION.—In cooperation with the de-
15 partments, agencies, and instrumentalities of the Government that collect,
16 receive, and analyze intelligence information related to aviation security, the
17 Administrator shall develop procedures to minimize the number of individ-
18 uals who have access to information about threats. However, a restriction
19 on access to that information may be imposed only if the restriction does
20 not diminish the ability of the Government to carry out its duties and pow-
21 ers related to aviation security effectively, including providing notice to the
22 public and flight and cabin crews under this section.

23 (g) DISTRIBUTION OF GUIDELINES.—The guidelines developed under this
24 section shall be distributed for use by appropriate officials of the Depart-
25 ment of Transportation, the Department of State, the Department of Jus-
26 tice, and air carriers.

27 **§ 40916. Foreign air carrier security programs**

28 The Administrator shall continue in effect the requirement of section
29 129.25 of title 14, Code of Federal Regulations, that a foreign air carrier
30 must adopt and use a security program approved by the Administrator. The
31 Administrator shall not approve a security program of a foreign air carrier
32 under section 129.25 of title 14, Code of Federal Regulations, or a suc-
33 cessor regulation, unless the security program requires the foreign air car-
34 rier in its operations to and from airports in the United States to adhere
35 to the identical security measures that the Administrator requires air car-
36 riers serving the same airports to adhere to. The foregoing requirement
37 shall not be interpreted to limit the ability of the Administrator to impose
38 additional security measures on a foreign air carrier or an air carrier when
39 the Administrator determines that a specific threat warrants additional
40 measures. The Administrator shall prescribe regulations to carry out this
41 section.

1 **§ 40917. Security standards at foreign airports**

2 (a) ASSESSMENT.—

3 (1) IN GENERAL.—At intervals the Secretary of Transportation con-
4 siders necessary, the Secretary of Transportation shall assess the effec-
5 tiveness of the security measures maintained at—

6 (A) a foreign airport—

7 (i) served by an air carrier;

8 (ii) from which a foreign air carrier serves the United
9 States; or

10 (iii) that poses a high risk of introducing danger to inter-
11 national air travel; and

12 (B) other foreign airports the Secretary of Transportation con-
13 siders appropriate.

14 (2) MEANS OF ASSESSMENT.—The Secretary of Transportation shall
15 conduct an assessment under paragraph (1)—

16 (A) in consultation with appropriate aeronautic authorities of
17 the government of a foreign country concerned and each air car-
18 rier serving the foreign airport for which the Secretary of Trans-
19 portation is conducting the assessment;

20 (B) to establish the extent to which a foreign airport effectively
21 maintains and carries out security measures, including the screen-
22 ing and vetting of airport workers; and

23 (C) by using a standard that will result in an analysis of the
24 security measures at the airport based at least on the standards
25 and appropriate recommended practices contained in Annex 17 to
26 the Convention on International Civil Aviation in effect on the
27 date of the assessment.

28 (3) REPORT.—Each report to Congress required under section
29 40958(b) of this title shall contain a summary of the assessments con-
30 ducted under this subsection.

31 (b) CONSULTATION.—In carrying out subsection (a), the Secretary of
32 Transportation shall consult with the Secretary of State—

33 (1) on the terrorist threat that exists in each country; and

34 (2) to establish which foreign airports are not under the de facto
35 control of the government of the foreign country in which they are lo-
36 cated and pose a high risk of introducing danger to international air
37 travel.

38 (c) NOTIFYING FOREIGN AUTHORITIES.—When the Secretary of Trans-
39 portation, after conducting an assessment under subsection (a), decides that
40 an airport does not maintain and carry out effective security measures, the
41 Secretary of Transportation, after advising the Secretary of State, shall no-

1 tify the appropriate authorities of the government of the foreign country of
2 the decision and recommend the steps necessary to bring the security meas-
3 ures in use at the airport up to the standard used by the Secretary of
4 Transportation in making the assessment.

5 (d) ACTIONS WHEN AIRPORTS NOT MAINTAINING AND CARRYING OUT
6 EFFECTIVE SECURITY MEASURES.—

7 (1) IDENTIFICATION OF AIRPORT.—When the Secretary of Transpor-
8 tation decides under this section that an airport does not maintain and
9 carry out effective security measures—

10 (A) the Secretary of Transportation shall—

11 (i) publish the identity of the airport in the Federal Reg-
12 ister;

13 (ii) have the identity of the airport posted and displayed
14 prominently at all United States airports at which scheduled
15 air carrier operations are provided regularly; and

16 (iii) notify the news media of the identity of the airport;

17 (B) each air carrier and foreign air carrier providing transpor-
18 tation between the United States and the airport shall provide
19 written notice of the decision, on or with the ticket, to each pas-
20 senger buying a ticket for transportation between the United
21 States and the airport;

22 (C) notwithstanding section 40105(b) of title 49, the Secretary
23 of Transportation, after consulting with the appropriate aeronautic
24 authorities of the foreign country concerned and each air carrier
25 serving the airport and with the approval of the Secretary of
26 State, may withhold, revoke, or prescribe conditions on the oper-
27 ating authority of an air carrier or foreign air carrier that uses
28 that airport to provide foreign air transportation; and

29 (D) the President may prohibit an air carrier or foreign air car-
30 rier from providing transportation between the United States and
31 any other foreign airport that is served by aircraft flying to or
32 from the airport with respect to which a decision is made under
33 this section.

34 (2) EFFECTIVENESS.—

35 (A) IN GENERAL.—Paragraph (1) becomes effective—

36 (i) 90 days after the government of a foreign country is no-
37 tified under subsection (c) if the Secretary of Transportation
38 finds that the government has not brought the security meas-
39 ures at the airport up to the standard the Secretary of Trans-
40 portation used in making an assessment under subsection (a);
41 or

1 (ii) immediately on the decision of the Secretary of Trans-
2 portation under subsection (e) if the Secretary of Transpor-
3 tation decides, after consulting with the Secretary of State,
4 that a condition exists that threatens the safety or security
5 of passengers, aircraft, or crew traveling to or from the air-
6 port.

7 (B) STATE DEPARTMENT NOTICE.—The Secretary of Transpor-
8 tation immediately shall notify the Secretary of State of a decision
9 under subparagraph (A)(ii) so that the Secretary of State may
10 issue a travel advisory required under section 40918(a) of this
11 title.

12 (3) REPORT TO CONGRESS.—The Secretary of Transportation
13 promptly shall submit to Congress a report (and classified annex if nec-
14 essary) on action taken under paragraph (1) or (2), including informa-
15 tion on attempts made to obtain the cooperation of the government of
16 a foreign country in meeting the standard the Secretary of Transpor-
17 tation used in assessing the airport under subsection (a).

18 (4) TERMINATION OF ACTION.—An action required under paragraph
19 (1)(A) and (B) is no longer required only if the Secretary of Transpor-
20 tation, in consultation with the Secretary of State, decides that effec-
21 tive security measures are maintained and carried out at the airport.
22 The Secretary of Transportation shall notify Congress when the action
23 is no longer required to be taken.

24 (e) SUSPENSIONS.—Notwithstanding sections 40105(b) and 40106(b) of
25 title 49, the Secretary of Transportation, with the approval of the Secretary
26 of State and without notice or a hearing, shall suspend the right of an air
27 carrier or foreign air carrier to provide foreign air transportation, and the
28 right of a person to operate aircraft in foreign air commerce, to or from
29 a foreign airport when the Secretary of Transportation decides that—

30 (1) a condition exists that threatens the safety or security of pas-
31 sengers, aircraft, or crew traveling to or from that airport; and

32 (2) the public interest requires an immediate suspension of transpor-
33 tation between the United States and that airport.

34 (f) CONDITION OF CARRIER AUTHORITY.—This section is a condition of
35 authority the Secretary of Transportation grants under part A of subtitle
36 VII of title 49 to an air carrier or foreign air carrier.

37 **§ 40918. Travel advisory and suspension of foreign assist-**
38 **ance**

39 (a) TRAVEL ADVISORIES.—On being notified by the Administrator that
40 the Administrator has decided under section 40917(d)(2)(A)(ii) of this title
41 that a condition exists that threatens the safety or security of passengers,

1 aircraft, or crew traveling to or from a foreign airport that the Adminis-
2 trator has decided under section 40917 of this title does not maintain and
3 carry out effective security measures, the Secretary of State—

4 (1) immediately shall issue a travel advisory for that airport; and

5 (2) shall publicize the advisory widely.

6 (b) **SUSPENDING ASSISTANCE.**—The President shall suspend assistance
7 provided under the Foreign Assistance Act of 1961 (22 U.S.C. 2151 et seq.)
8 or the Arms Export Control Act (22 U.S.C. 2751 et seq.) to a country in
9 which is located an airport with respect to which section 40917(d)(1) of this
10 title becomes effective if the Secretary of State decides the country is a high
11 terrorist threat country. The President may waive this subsection if the
12 President decides, and reports to Congress, that the waiver is required be-
13 cause of national security interests or a humanitarian emergency.

14 (c) **ACTIONS NO LONGER REQUIRED.**—An action required under this sec-
15 tion is no longer required only if the Administrator has made a decision as
16 provided under section 40917(d)(4) of this title. The Administrator shall no-
17 tify Congress when the action is no longer required to be taken.

18 **§ 40919. Passenger manifests**

19 (a) **AIR CARRIER REQUIREMENTS.**—

20 (1) **IN GENERAL.**—The Secretary of Transportation shall require
21 each air carrier to provide a passenger manifest for a flight to an ap-
22 propriate representative of the Secretary of State—

23 (A) not later than 1 hour after that carrier is notified of an
24 aviation disaster outside the United States involving that flight; or

25 (B) if it is not technologically feasible or reasonable to comply
26 with subparagraph (A), then as expeditiously as possible, but not
27 later than 3 hours after the carrier is so notified.

28 (2) **CONTENTS.**—The passenger manifest should include the fol-
29 lowing information:

30 (A) The full name of each passenger.

31 (B) The passport number of each passenger, if required for
32 travel.

33 (C) The name and telephone number of a contact for each pas-
34 senger.

35 (3) **CONSIDERATION OF REQUIREMENT TO COLLECT INFORMA-**
36 **TION.**—In carrying out this subsection, the Secretary of Transportation
37 shall consider the necessity and feasibility of requiring air carriers to
38 collect passenger manifest information as a condition for passengers
39 boarding a flight of the carrier.

1 (b) FOREIGN AIR CARRIER REQUIREMENTS.—The Secretary of Transportation
2 shall consider imposing a requirement on foreign air carriers com-
3 parable to that imposed on air carriers under subsection (a)(1) and (2).

4 (c) FLIGHTS IN FOREIGN AIR TRANSPORTATION TO THE UNITED
5 STATES.—

6 (1) IN GENERAL.—Each air carrier and foreign air carrier operating
7 a passenger flight in foreign air transportation to the United States
8 shall provide to the Commissioner of U.S. Customs and Border Protec-
9 tion by electronic transmission a passenger and crew manifest con-
10 taining the information specified in paragraph (2). Carriers may use
11 the advanced passenger information system to provide the information.

12 (2) CONTENTS.—A passenger and crew manifest for a flight required
13 under paragraph (1) shall contain the following information:

14 (A) The full name of each passenger and crew member.

15 (B) The date of birth and citizenship of each passenger and
16 crew member.

17 (C) The sex of each passenger and crew member.

18 (D) The passport number and country of issuance of each pas-
19 senger and crew member if required for travel.

20 (E) The United States visa number or resident alien card num-
21 ber of each passenger and crew member, as applicable.

22 (F) Other information the Administrator, in consultation with
23 the Commissioner of U.S. Customs and Border Protection, deter-
24 mines is reasonably necessary to ensure aviation safety.

25 (3) PASSENGER NAME RECORDS.—The carriers shall make passenger
26 name record information available to U. S. Customs and Border Pro-
27 tection on request.

28 (4) TRANSMISSION OF MANIFEST.—Subject to paragraphs (5) and
29 (6), a passenger and crew manifest required for a flight under para-
30 graph (1) shall be transmitted to U. S. Customs and Border Protection
31 in advance of the aircraft's landing in the United States in the manner,
32 time, and form U.S. Customs and Border Protection prescribes.

33 (5) TRANSMISSION OF MANIFESTS TO OTHER FEDERAL AGENCIES.—
34 On request, information provided to the Administrator or U. S. Cus-
35 toms and Border Protection under this subsection may be shared with
36 other Federal agencies for the purpose of protecting national security.

37 (6) PRESCREENING INTERNATIONAL PASSENGERS.—

38 (A) IN GENERAL.—The Secretary, or the designee of the Sec-
39 retary, shall issue a notice of proposed rulemaking that will allow
40 the Department to compare passenger information for an inter-
41 national flight to or from the United States against the consoli-

1 dated and integrated terrorist watchlist maintained by the Federal
2 Government before departure of the flight.

3 (B) APPEAL PROCEDURES.—

4 (i) ESTABLISHMENT.—The Secretary shall establish a
5 timely and fair process for individuals identified as a threat
6 under subparagraph (A) to appeal to the Department the de-
7 termination and correct erroneous information.

8 (ii) RECORD OF MISIDENTIFIED INDIVIDUALS.—The proc-
9 ess shall include the establishment of a method by which the
10 Secretary will be able to maintain a record of air passengers
11 and other individuals who have been misidentified and have
12 corrected erroneous information. To prevent repeated delays
13 of misidentified passengers and other individuals, the Depart-
14 ment record shall contain information determined by the Sec-
15 retary to authenticate the identity of such a passenger or in-
16 dividual.

17 **§ 40920. Agreements on aircraft sabotage, aircraft hijacking,**
18 **and airport security**

19 The Secretary of State shall seek multilateral and bilateral agreement on
20 strengthening enforcement measures and standards for compliance related
21 to aircraft sabotage, aircraft hijacking, and airport security.

22 **§ 40921. Intelligence**

23 (a) DEFINITION OF INTELLIGENCE COMMUNITY.—In this section, “intel-
24 ligence community” means the intelligence and intelligence-related activities
25 of the following units of the United States Government:

- 26 (1) Department of State.
- 27 (2) Department of Defense.
- 28 (3) Department of the Treasury.
- 29 (4) Department of Energy.
- 30 (5) Departments of the Army, Navy, and Air Force.
- 31 (6) Central Intelligence Agency.
- 32 (7) National Security Agency.
- 33 (8) Defense Intelligence Agency.
- 34 (9) Federal Bureau of Investigation.
- 35 (10) Drug Enforcement Administration.

36 (b) POLICIES AND PROCEDURES ON REPORT AVAILABILITY.—The head
37 of each unit in the intelligence community shall prescribe policies and proce-
38 dures to ensure that intelligence reports about terrorism are made available,
39 as appropriate, to the heads of other units in the intelligence community,
40 the Secretary of Transportation, and the Administrator.

1 (c) UNIT FOR STRATEGIC PLANNING ON TERRORISM.—The heads of the
2 units in the intelligence community shall place greater emphasis on strategic
3 intelligence efforts by establishing a unit for strategic planning on terrorism.

4 (d) DESIGNATION OF INTELLIGENCE OFFICER.—At the request of the
5 Secretary, the Director of Central Intelligence shall designate at least one
6 intelligence officer of the Central Intelligence Agency to serve in a senior
7 position in the Office of the Secretary.

8 (e) WRITTEN WORKING AGREEMENTS.—The heads of units in the intel-
9 ligence community, the Secretary, and the Administrator shall review and,
10 as appropriate, revise written working agreements between the intelligence
11 community and the Administrator.

12 § 40922. Research and development

13 (a) PROGRAM REQUIREMENT.—

14 (1) IN GENERAL.—The Administrator shall establish and carry out
15 a program to accelerate and expand the research, development, and im-
16 plementation of technologies and procedures to counteract terrorist acts
17 against civil aviation. The program shall provide for developing and
18 having in place new equipment and procedures necessary to meet the
19 technological challenges presented by terrorism. The program shall in-
20 clude research on, and development of, technological improvements and
21 ways to enhance human performance.

22 (2) REQUIRED ACTIONS.—In designing and carrying out the pro-
23 gram established under this subsection, the Administrator shall—

24 (A) consult and coordinate activities with other departments,
25 agencies, and instrumentalities of the United States Government
26 doing similar research;

27 (B) identify departments, agencies, and instrumentalities that
28 would benefit from that research; and

29 (C) seek cost-sharing agreements with those departments, agen-
30 cies, and instrumentalities.

31 (3) ANNUAL REPORTS.—In carrying out the program established
32 under this subsection, the Administrator shall review and consider the
33 annual reports the Secretary submits to Congress on transportation se-
34 curity and intelligence.

35 (4) DESIGNATION OF RESPONSIBLE INDIVIDUAL.—

36 (A) IN GENERAL.—In carrying out the program established
37 under this subsection, the Administrator shall designate an indi-
38 vidual to be responsible for engineering, research, and development
39 with respect to security technology under the program.

40 (B) DECISION-MAKING.—The individual designated under sub-
41 paragraph (A) shall use appropriate systems engineering and risk

1 management models in making decisions regarding the allocation
2 of funds for engineering, research, and development with respect
3 to security technology under the program.

4 (C) ANNUAL REPORT.—The individual designated under sub-
5 paragraph (A) shall, on an annual basis, submit to the Adminis-
6 trator a report on activities under this paragraph during the pre-
7 ceding year. Each report shall include, for the year covered by the
8 report, information on—

9 (i) progress made in engineering, research, and develop-
10 ment with respect to security technology;

11 (ii) the allocation of funds for engineering, research, and
12 development with respect to security technology; and

13 (iii) engineering, research, and development with respect to
14 technologies drawn from other agencies, including the ration-
15 ale for engineering, research, and development with respect to
16 the technologies.

17 (5) GRANTS.—The Administrator may—

18 (A) make grants to institutions of higher learning and other ap-
19 propriate research facilities with demonstrated ability to carry out
20 research described in paragraph (1), and fix the amounts and
21 terms of the grants; and

22 (B) make cooperative agreements with governmental authorities
23 the Administrator decides are appropriate.

24 (b) REVIEW OF THREATS.—

25 (1) IN GENERAL.—The Administrator periodically shall review
26 threats to civil aviation, with particular focus on—

27 (A) a comprehensive systems analysis (employing vulnerability
28 analysis, threat attribute definition, and technology roadmaps) of
29 the civil aviation system, including—

30 (i) the destruction, commandeering, or diversion of civil air-
31 craft or the use of civil aircraft as a weapon; and

32 (ii) the disruption of civil aviation service, including by
33 cyberattack;

34 (B) explosive material that presents the most significant threat
35 to civil aircraft;

36 (C) the minimum amounts, configurations, and types of explo-
37 sive material that can cause, or would reasonably be expected to
38 cause, catastrophic damage to aircraft in air transportation;

39 (D) the amounts, configurations, and types of explosive material
40 that can be detected reliably by existing, or reasonably anticipated,
41 near-term explosive detection technologies;

1 (E) the potential release of chemical, biological, or similar weap-
2 ons or devices either within an aircraft or within an airport;

3 (F) the feasibility of using various ways to minimize damage
4 caused by explosive material that cannot be detected reliably by
5 existing, or reasonably anticipated, near-term explosive detection
6 technologies;

7 (G) the ability to screen passengers, carry-on baggage, checked
8 baggage, and cargo; and

9 (H) the technologies that might be used in the future to at-
10 tempt to destroy or otherwise threaten commercial aircraft and the
11 ways in which those technologies can be countered effectively.

12 (2) PROGRAM FOCUS AND PRIORITIES.—The Administrator shall use
13 the results of the review under this subsection to develop the focus and
14 priorities of the program established under subsection (a).

15 (c) SCIENTIFIC ADVISORY PANEL.—

16 (1) ESTABLISHMENT.—The Administrator shall establish a scientific
17 advisory panel to review, comment on, advise on the progress of, and
18 recommend modifications in, the program established under subsection
19 (a), including the need for long-range research programs to detect and
20 prevent catastrophic damage to commercial aircraft, commercial avia-
21 tion facilities, commercial aviation personnel and passengers, and other
22 components of the commercial aviation system by the next generation
23 of terrorist weapons.

24 (2) PANEL MEMBERS.—

25 (A) QUALIFICATIONS.—The advisory panel shall consist of indi-
26 viduals who have scientific and technical expertise in—

27 (i) the development and testing of effective explosive detec-
28 tion systems;

29 (ii) aircraft structure and experimentation to decide on the
30 type and minimum weights of explosives that an effective ex-
31 plosive detection technology must be capable of detecting;

32 (iii) technologies involved in minimizing airframe damage
33 to aircraft from explosives; and

34 (iv) other scientific and technical areas the Administrator
35 considers appropriate.

36 (B) CONSIDERATIONS.—In appointing individuals to the advi-
37 sory panel, the Administrator should consider individuals from
38 academia and the national laboratories, as appropriate.

39 (3) ORGANIZATION AS TEAMS.—The Administrator shall organize the
40 advisory panel into teams capable of undertaking the review of policies
41 and technologies upon request.

1 (4) BIENNIAL REVIEW.—The Administrator shall review the com-
2 position of the advisory panel biennially to ensure that the expertise of
3 the individuals on the panel is suited to the current and anticipated
4 duties of the panel.

5 (d) SECURITY AND RESEARCH AND DEVELOPMENT ACTIVITIES.—

6 (1) IN GENERAL.—The Administrator shall conduct research (includ-
7 ing behavioral research) and development activities appropriate to de-
8 velop, modify, test, and evaluate a system, procedure, facility, or device
9 to protect passengers and property against acts of criminal violence,
10 aircraft piracy, and terrorism and to ensure security.

11 (2) DISCLOSURE.—

12 (A) IN GENERAL.—Notwithstanding section 552 of title 5, the
13 Administrator shall prescribe regulations prohibiting disclosure of
14 information obtained or developed in ensuring security under this
15 title if the Secretary decides disclosing the information would—

- 16 (i) be an unwarranted invasion of personal privacy;
17 (ii) reveal a trade secret or privileged or confidential com-
18 mercial or financial information; or
19 (iii) be detrimental to transportation safety.

20 (B) INFORMATION TO CONGRESS.—Subparagraph (A) does not
21 authorize information to be withheld from a committee of Con-
22 gress authorized to have the information.

23 (C) DESIGNATION OF INFORMATION AS SENSITIVE SECURITY IN-
24 FORMATION NOT AUTHORIZED.—Nothing in subparagraph (A)
25 shall be construed to authorize the designation of information as
26 sensitive security information (as defined in section 15.5 of title
27 49, Code of Federal Regulations)—

- 28 (i) to conceal a violation of law, inefficiency, or administra-
29 tive error;
30 (ii) to prevent embarrassment to a person, organization, or
31 agency;
32 (iii) to restrain competition; or
33 (iv) to prevent or delay the release of information that does
34 not require protection in the interest of transportation secu-
35 rity, including basic scientific research information not clearly
36 related to transportation security.

37 (D) NONAPPLICABILITY OF SECTION 552A OF TITLE 5.—Section
38 552a of title 5 shall not apply to disclosures that the Adminis-
39 trator may make from the systems of records of the Transpor-
40 tation Security Administration to a Federal law enforcement, in-
41 telligence, protective service, immigration, or national security offi-

1 cial to assist the official receiving the information in the perform-
2 ance of official duties.

3 (3) TRANSFERS OF DUTIES AND POWERS PROHIBITED.—Except as
4 otherwise provided by law, the Administrator may not transfer a duty
5 or power under this section to another department, agency, or instru-
6 mentality of the United States Government.

7 **§ 40923. Explosive detection**

8 (a) DEPLOYMENT AND PURCHASE OF EQUIPMENT.—

9 (1) IN GENERAL.—A deployment or purchase of explosive detection
10 equipment under section 108.7(b)(8) or 108.20 of title 14, Code of
11 Federal Regulations, or similar regulation is required only if the Ad-
12 ministrator certifies that the equipment alone, or as part of an inte-
13 grated system, can detect under realistic air carrier operating condi-
14 tions the amounts, configurations, and types of explosive material that
15 would likely be used to cause catastrophic damage to commercial air-
16 craft. The Administrator shall base the certification on the results of
17 tests conducted under protocols developed in consultation with expert
18 scientists outside of the Transportation Security Administration.

19 (2) FACILITATING DEPLOYMENT.—Until the Administrator deter-
20 mines that equipment certified under paragraph (1) is commercially
21 available and has successfully completed operational testing as provided
22 in paragraph (1), the Administrator shall facilitate the deployment of
23 approved commercially available explosive detection devices the Admin-
24 istrator determines will enhance aviation security significantly. The Ad-
25 ministrator shall require that equipment deployed under this paragraph
26 be replaced by equipment certified under paragraph (1) when equip-
27 ment certified under paragraph (1) becomes commercially available.
28 The Administrator, based on operational considerations at individual
29 airports, may waive the required installation of commercially available
30 equipment under paragraph (1) in the interests of aviation security.
31 The Administrator may permit the requirements of this paragraph to
32 be met at airports by the deployment of dogs or other appropriate ani-
33 mals to supplement equipment for screening passengers, baggage, mail,
34 or cargo for explosives or weapons.

35 (3) PURCHASES BY ADMINISTRATOR.—This subsection does not pro-
36 hibit the Administrator from purchasing or deploying explosive detec-
37 tion equipment described in paragraph (1).

38 (b) GRANTS.—The Administrator may provide grants to continue the Ex-
39 plosive Detection K-9 Team Training Program to detect explosives at air-
40 ports and on aircraft.

1 **§ 40924. Airport construction guidelines**

2 In consultation with the Department of Transportation, air carriers, air-
3 port authorities, and others the Administrator considers appropriate, the
4 Administrator shall develop guidelines for airport design and construction
5 to allow for maximum security enhancement. In developing the guidelines,
6 the Administrator shall consider the results of the assessment carried out
7 under section 40914(a) of this title.

8 **§ 40925. Alaska exemptions**

9 The Administrator may exempt from sections 40911, 40913(a) through
10 (c) and (e), 40916, 40955, and 40956 of this title airports in Alaska served
11 only by air carriers that—

- 12 (1) hold certificates issued under section 41102 of title 49;
- 13 (2) operate aircraft with certificates for a maximum gross takeoff
14 weight of less than 12,500 pounds; and
- 15 (3) board passengers, or load property intended to be carried in an
16 aircraft cabin, that will be screened under section 40911 of this title
17 at another airport in Alaska before the passengers board, or the prop-
18 erty is loaded on, an aircraft for a place outside Alaska.

19 **§ 40926. Assessments and evaluations**

20 (a) PERIODIC ASSESSMENTS.—The Administrator shall require each air
21 carrier and airport (including the airport owner or operator in cooperation
22 with the air carriers and vendors serving each airport) that provides for
23 intrastate, interstate, or foreign air transportation to conduct periodic vul-
24 nerability assessments of the security systems of that air carrier or airport,
25 respectively. The Transportation Security Administration shall perform peri-
26 odic audits of the assessments.

27 (b) INVESTIGATIONS.—The Administrator shall conduct periodic and un-
28 announced inspections of security systems of airports and air carriers to de-
29 termine the effectiveness and vulnerabilities of the systems. To the extent
30 allowable by law, the Administrator may provide for anonymous tests of
31 those security systems.

32 **§ 40927. Federal air marshals and training of law enforce-**
33 **ment personnel**

34 (a) IN GENERAL.—The Administrator under the authority provided by
35 section 40913(d) of this title—

- 36 (1) may provide for deployment of Federal air marshals on every
37 passenger flight of air carriers in air transportation or intrastate air
38 transportation;
- 39 (2) shall provide for deployment of Federal air marshals on every
40 flight determined by the Secretary to present high security risks;

1 (3) shall provide for appropriate training, supervision, and equip-
2 ment of Federal air marshals;

3 (4) shall require air carriers providing flights described in paragraph
4 (1) to provide seating for a Federal air marshal on the flight without
5 regard to the availability of seats on the flight and at no cost to the
6 United States Government or the marshal;

7 (5) may require air carriers to provide, on a space-available basis,
8 to an off-duty Federal air marshal a seat on a flight to the airport
9 nearest the marshal's home at no cost to the marshal or the United
10 States Government if the marshal is traveling to that airport after
11 completing his or her security duties;

12 (6) may enter into agreements with Federal, State, and local agen-
13 cies under which appropriately trained law enforcement personnel from
14 the agencies, when traveling on a flight of an air carrier, will carry a
15 firearm and be prepared to assist Federal air marshals;

16 (7) shall establish procedures to ensure that Federal air marshals
17 are made aware of armed or unarmed law enforcement personnel on
18 board an aircraft; and

19 (8) may appoint as a Federal air marshal, regardless of age (if the
20 individual otherwise meets the background and fitness qualifications re-
21 quired for Federal air marshals)—

22 (A) an individual who is a retired law enforcement officer;

23 (B) an individual who is a retired member of the armed forces;

24 or

25 (C) an individual who was furloughed from an air carrier crew
26 position in the 1-year period beginning on September 11, 2011;

27 (9) shall require the Federal Air Marshal Service to utilize a risk-
28 based strategy when allocating resources between international and do-
29 mestic flight coverage, including when initially setting its annual target
30 numbers of average daily international and domestic flights to cover;

31 (10) shall require the Federal Air Marshal Service to utilize a risk-
32 based strategy to support domestic allocation decisions;

33 (11) shall require the Federal Air Marshal Service to utilize a risk-
34 based strategy to support international allocation decisions; and

35 (12) shall ensure that the seating arrangements of Federal air mar-
36 shals on aircraft are determined in a manner that is risk-based and
37 that allows the air marshals to be most capable of responding to cur-
38 rent threats to aviation security.

39 (b) INTERIM MEASURES.—Until the Administrator completes implemen-
40 tation of subsection (a), the Administrator may use, after consultation with
41 and concurrence of the heads of other Federal agencies and departments,

1 personnel from those agencies and departments, on a nonreimbursable basis,
2 to provide air marshal service.

3 (c) CONTINUATION OF INITIATIVES TO PROTECT ANONYMITY OF FED-
4 ERAL AIR MARSHALS.—The Director of the Federal Air Marshal Service
5 shall continue operational initiatives to protect the anonymity of Federal air
6 marshals.

7 (d) TRAINING FOR FEDERAL AND LOCAL LAW ENFORCEMENT PER-
8 SONNEL.—

9 (1) AVAILABILITY OF INFORMATION.—The Administrator and the
10 Director of the Federal Air Marshal Service shall make available, as
11 practicable, appropriate information on in-flight counterterrorism and
12 weapons handling procedures and tactics training to Federal law en-
13 forcement officers who fly while in possession of a firearm.

14 (2) IDENTIFICATION OF FRAUDULENT DOCUMENTS.—The Adminis-
15 trator and the Director of the Federal Air Marshal Service shall ensure
16 that Transportation Security Administration screeners and Federal air
17 marshals receive training in identifying fraudulent identification docu-
18 ments, including fraudulent or expired visas and passports. The train-
19 ing also shall be made available to other Federal law enforcement agen-
20 cies and local law enforcement agencies located in a State that borders
21 Canada or Mexico.

22 (e) AGREEMENT ON FEDERAL AIR MARSHALS ON FLIGHTS TO AND
23 FROM THE UNITED STATES.—

24 (1) DEVELOPMENT.—Not later than 60 days after October 5, 2018,
25 the Administrator shall develop a standard written agreement that
26 shall be the basis of all negotiations and agreements that begin after
27 October 5, 2018, between the United States and foreign governments
28 or partners regarding the presence of Federal air marshals on flights
29 to and from the United States, including deployment, technical assist-
30 ance, and information sharing.

31 (2) SIGNED AGREEMENT.—Except as provided in paragraph (3), not
32 later than 180 days after October 5, 2018, all agreements between the
33 United States and foreign governments or partners regarding the pres-
34 ence of Federal air marshals on flights to and from the United States
35 shall be in writing and signed by the Administrator or other authorized
36 United States Government representative.

37 (3) EXCEPTION.—The Administrator may schedule Federal air mar-
38 shal service on flights operating to a foreign country with which no
39 written agreement is in effect if the Administrator determines that—

40 (A) the mission is necessary for aviation security; and

41 (B) the requirements of paragraph (4)(C) are met.

1 (4) NOTIFICATION TO CONGRESS.—

2 (A) DEFINITION OF APPROPRIATE COMMITTEES OF CON-
3 GRESS.—In this paragraph, the term “appropriate committees of
4 Congress” means—

5 (i) the Committee on Commerce, Science, and Transpor-
6 tation of the Senate;

7 (ii) the Committee on Homeland Security and Govern-
8 mental Affairs of the Senate; and

9 (iii) the Committee on Homeland Security of the House of
10 Representatives.

11 (B) WRITTEN AGREEMENTS.—Not later than 30 days after the
12 date that the Administrator enters into a written agreement under
13 this subsection, the Administrator shall transmit to the appro-
14 priate committees of Congress a copy of the agreement.

15 (C) NO WRITTEN AGREEMENT.—The Administrator shall sub-
16 mit to the appropriate committees of Congress—

17 (i) not later than 30 days after October 5, 2018, a list of
18 each foreign government or partner that does not have a writ-
19 ten agreement under this subsection, including an explanation
20 for why no written agreement exists and a justification for
21 the determination that a mission under paragraph (3)(A) is
22 necessary for aviation security; and

23 (ii) not later than 30 days after the date that the Adminis-
24 trator makes a determination to schedule Federal air marshal
25 service on flights operating to a foreign country with which
26 no written agreement is in effect under paragraph (3), the
27 name of the applicable foreign government or partner, an ex-
28 planation for why no written agreement exists, and a jus-
29 tification for the determination that the mission under para-
30 graph (3)(A) is necessary for aviation security.

31 (f) AUTOMATED MISSION SCHEDULING.—The Administrator shall en-
32 deavor to acquire automated capabilities or technologies for scheduling Fed-
33 eral air marshal service missions based on current risk modeling.

34 (g) IMPROVING FEDERAL AIR MARSHAL SERVICE DEPLOYMENTS.—

35 (1) AFTER-ACTION REPORTS.—The Administrator shall strengthen
36 internal controls to ensure that all after-action reports on Federal air
37 marshal service special mission coverage provided to stakeholders in-
38 clude documentation of supervisory review and approval, and manda-
39 tory narratives.

40 (2) STUDY.—The Administrator shall contract with an independent
41 entity to conduct a validation and verification study of the risk analysis

1 and risk-based determinations guiding Federal air marshal service de-
2 ployment, including the use of risk-based strategies under paragraphs
3 (9) through (12) of subsection (a).

4 (3) COST-BENEFIT ANALYSIS.—The Administrator shall conduct a
5 cost-benefit analysis regarding mitigation of aviation security threats
6 through Federal air marshal service deployment.

7 (4) PERFORMANCE MEASURES.—The Administrator shall improve
8 existing performance measures to better determine the effectiveness of
9 in-flight operations in addressing the highest risks to aviation transpor-
10 tation based on current intelligence.

11 (h) TRAINING FOR FOREIGN LAW ENFORCEMENT PERSONNEL.—

12 (1) IN GENERAL.—The Administrator, after consultation with the
13 Secretary of State, may direct the Federal Air Marshal Service to pro-
14 vide appropriate air marshal training to law enforcement personnel of
15 foreign countries.

16 (2) WATCHLIST SCREENING.—The Federal Air Marshal Service may
17 only provide appropriate air marshal training to law enforcement per-
18 sonnel of foreign countries after comparing the identifying information
19 and records of law enforcement personnel of foreign countries against
20 all appropriate records in the consolidated and integrated terrorist
21 watchlists maintained by the Federal Government.

22 (3) FEES.—The Administrator shall establish reasonable fees and
23 charges to pay expenses incurred in carrying out this subsection. Funds
24 collected under this subsection shall be credited to the account in the
25 Treasury from which the expenses were incurred and shall be available
26 to the Administrator for purposes for which amounts in the account
27 are available.

28 **§ 40928. Crew training**

29 (a) BASIC SECURITY TRAINING.—

30 (1) IN GENERAL.—Each air carrier providing scheduled passenger
31 air transportation shall carry out a training program for flight and
32 cabin crew members to prepare the crew members for potential threat
33 conditions.

34 (2) PROGRAM ELEMENTS.—An air carrier training program under
35 this subsection shall include, at a minimum, elements that address each
36 of the following:

37 (A) The recognition of suspicious activities and the determina-
38 tion of the seriousness of an occurrence.

39 (B) Crew communication and coordination.

40 (C) The proper commands to give passengers and attackers.

41 (D) The appropriate responses to defend oneself.

1 (E) The use of protective devices assigned to crew members (to
2 the extent devices are required by the Administrator and the Ad-
3 ministrator of the Federal Aviation Administration).

4 (F) The psychology of terrorists to cope with hijacker behavior
5 and passenger responses.

6 (G) Situational training exercises regarding various threat con-
7 ditions.

8 (H) Flight deck procedures or aircraft maneuvers to defend the
9 aircraft, and cabin crew responses to the procedures and maneu-
10 vers.

11 (I) The proper conduct of a cabin search, including explosive de-
12 vice recognition.

13 (J) Other subject matter considered appropriate by the Admin-
14 istrator.

15 (3) APPROVAL.—An air carrier training program under this sub-
16 section shall be subject to approval by the Administrator.

17 (4) MINIMUM STANDARDS.—The Administrator may establish min-
18 imum standards for the training provided under this subsection and for
19 recurrent training.

20 (5) PROGRAMS TO CONTINUE IN EFFECT.—Notwithstanding para-
21 graphs (3) and (4), a training program of an air carrier to prepare
22 flight and cabin crew members for potential threat conditions that was
23 approved by the Administrator of the Federal Aviation Administration
24 or the Administrator before December 12, 2003, may continue in effect
25 until disapproved or ordered modified by the Administrator.

26 (6) MONITORING.—The Administrator, in consultation with the Ad-
27 ministrator of the Federal Aviation Administration, shall monitor air
28 carrier training programs under this subsection and periodically shall
29 review an air carrier's training program to ensure that the program is
30 adequately preparing crew members for potential threat conditions. In
31 determining when an air carrier's training program should be reviewed
32 under this paragraph, the Administrator shall consider complaints from
33 crew members. The Administrator shall ensure that employees respon-
34 sible for monitoring the training programs have the necessary resources
35 and knowledge.

36 (7) UPDATES.—The Administrator, in consultation with the Admin-
37 istrator of the Federal Aviation Administration, shall order air carriers
38 to modify training programs under this subsection to reflect new or dif-
39 ferent security threats.

40 (b) ADVANCED SELF-DEFENSE TRAINING.—

1 (1) IN GENERAL.—The Administrator shall develop and provide a
2 voluntary training program for flight and cabin crew members of air
3 carriers providing scheduled passenger air transportation.

4 (2) PROGRAM ELEMENTS.—The training program under this sub-
5 section shall include both classroom and effective hands-on training in
6 the following elements of self-defense:

7 (A) The deterrence of a passenger who might present a threat.

8 (B) Advanced control, striking, and restraint techniques.

9 (C) Training to defend oneself against edged or contact weap-
10 ons.

11 (D) Methods to subdue and restrain an attacker.

12 (E) The use of available items aboard the aircraft for self-de-
13 fense.

14 (F) Appropriate and effective responses to defend oneself, in-
15 cluding the use of force against an attacker.

16 (G) Other elements of training that the Administrator considers
17 appropriate.

18 (3) PARTICIPATION NOT REQUIRED.—A crew member shall not be
19 required to participate in the training program under this subsection.

20 (4) COMPENSATION.—Neither the Federal Government nor an air
21 carrier shall be required to compensate a crew member for partici-
22 pating in the training program under this subsection.

23 (5) FEES.—A crew member is not required to pay a fee for the
24 training program under this subsection.

25 (6) CONSULTATION.—In developing the training program under this
26 subsection, the Administrator shall consult with law enforcement per-
27 sonnel and security experts who have expertise in self-defense training,
28 terrorism experts, representatives of air carriers, the director of self-
29 defense training in the Federal Air Marshal Service, flight attendants,
30 labor organizations representing flight attendants, and educational in-
31 stitutions offering law enforcement training programs.

32 (7) DESIGNATION OF TRANSPORTATION SECURITY ADMINISTRATION
33 OFFICIAL.—The Administrator shall designate an official in the Trans-
34 portation Security Administration to be responsible for implementing
35 the training program under this subsection. The official shall consult
36 with air carriers and labor organizations representing crew members
37 before implementing the program to ensure that it is appropriate for
38 situations that may arise on board an aircraft during a flight.

39 (e) LIMITATION.—Actions by crew members under this section shall be
40 subject to section 40913(k) of this title.

1 **§ 40929. PreCheck Program**

2 (a) IN GENERAL.—The Administrator shall continue to administer the
3 PreCheck Program in accordance with section 11521(a)(3) of this title

4 (b) EXPANSION.—Not later than 180 days after October 5, 2018, the Ad-
5 ministrator shall enter into an agreement, using other transaction authority
6 under section 11508 of this title, with at least 2 private-sector entities to
7 increase the methods and capabilities available for the public to enroll in
8 the PreCheck Program.

9 (c) MINIMUM CAPABILITY REQUIREMENTS.—At least 1 agreement under
10 subsection (b) shall include the following capabilities:

11 (1) Start-to-finish secure online or mobile enrollment capability.

12 (2) Vetting of an applicant by means other than biometrics, such as
13 a risk assessment, if—

14 (A) the means—

15 (i) are evaluated and certified by the Secretary;

16 (ii) meet the definition of a qualified anti-terrorism tech-
17 nology under section 10931 of this title; and

18 (iii) are determined by the Administrator to provide a risk
19 assessment that is as effective as a fingerprint-based criminal
20 history records check conducted through the Federal Bureau
21 of Investigation with respect to identifying individuals who
22 are not qualified to participate in the PreCheck Program due
23 to disqualifying criminal history; and

24 (B) with regard to private-sector risk assessments, the Sec-
25 retary has certified that reasonable procedures are in place with
26 regard to the accuracy, relevancy, and proper utilization of infor-
27 mation employed in the risk assessments.

28 (d) ADDITIONAL CAPABILITY REQUIREMENTS.—At least 1 agreement
29 under subsection (b) shall include the following capabilities:

30 (1) Start-to-finish secure online or mobile enrollment capability.

31 (2) Vetting of an applicant by means of biometrics if the collection—

32 (A) is comparable with the appropriate and applicable standards
33 developed by the National Institute of Standards and Technology;

34 (B) protects privacy and data security, including that any per-
35 sonally identifiable information is collected, retained, used, and
36 shared in a manner consistent with section 552a of title 5 and
37 with agency regulations;

38 (C) is evaluated and certified by the Secretary; and

39 (D) is determined by the Administrator to provide a risk assess-
40 ment that is as effective as a fingerprint-based criminal history
41 records check conducted through the Federal Bureau of Investiga-

1 tion with respect to identifying individuals who are not qualified
2 to participate in the PreCheck Program due to disqualifying criminal
3 history.

4 (e) TARGET ENROLLMENT.—Subject to subsections (b), (c), and (d), the
5 Administrator shall take actions to expand the total number of individuals
6 enrolled in the PreCheck Program as follows:

7 (1) 7,000,000 passengers before October 1, 2019.

8 (2) 10,000,000 passengers before October 1, 2020.

9 (3) 15,000,000 passengers before October 1, 2021.

10 (f) MARKETING OF PRECHECK PROGRAM.—Not later than 90 days after
11 October 5, 2018, the Administrator shall—

12 (1) enter into at least 2 agreements, using other transaction author-
13 ity under section 11508 of this title, to market the PreCheck Program;
14 and

15 (2) implement a long-term strategy for partnering with the private
16 sector to encourage enrollment in the PreCheck Program.

17 (g) IDENTITY VERIFICATION ENHANCEMENT.—The Administrator
18 shall—

19 (1) coordinate with the heads of appropriate components of the De-
20 partment to leverage Department-held data and technologies to verify
21 the identity and citizenship of individuals enrolling in the PreCheck
22 Program;

23 (2) partner with the private sector to use biometrics and authentica-
24 tion standards, such as relevant standards developed by the National
25 Institute of Standards and Technology, to facilitate enrollment in the
26 Precheck Program; and

27 (3) consider leveraging the existing resources and abilities of airports
28 to collect fingerprints for use in background checks to expedite identity
29 verification.

30 (h) PRECHECK PROGRAM LANES OPERATION.—The Administrator
31 shall—

32 (1) ensure that PreCheck Program screening lanes are open and
33 available during peak and high-volume travel times at appropriate air-
34 ports to individuals enrolled in the PreCheck Program; and

35 (2) make every practicable effort to provide expedited screening at
36 standard screening lanes to maintain operational efficiency during
37 times when PreCheck Program screening lanes are closed to individuals
38 enrolled in the program.

39 (i) ELIGIBILITY OF MEMBERS OF THE ARMED FORCES FOR EXPEDITED
40 SECURITY SCREENING.—

1 (1) IN GENERAL.—Subject to paragraph (3), an individual specified
2 in paragraph (2) is eligible for expedited security screening under the
3 PreCheck Program.

4 (2) INDIVIDUALS SPECIFIED.—An individual specified in this sub-
5 section is any of the following:

6 (A) A member of the Armed Forces, including a member of a
7 reserve component or the National Guard.

8 (B) A cadet or midshipman of the United States Military Acad-
9 emy, the United States Naval Academy, the United States Air
10 Force Academy, or the United States Coast Guard Academy.

11 (C) A family member of an individual specified in subparagraph
12 (A) or (B) who is younger than 12 years old and accompanying
13 the individual.

14 (3) IMPLEMENTATION.—The eligibility of an individual specified in
15 paragraph (2) for expedited security screening under the PreCheck
16 Program is subject to such policies and procedures as the Adminis-
17 trator may prescribe to carry out this subsection, in consultation with
18 the Secretary of Defense and, with respect to the Coast Guard, the
19 Commandant of the Coast Guard.

20 (j) IDENTIFYING VULNERABILITIES IN VETTING PROCESS FOR
21 PRECHECK PROGRAM PARTICIPANTS.—The Administrator shall initiate an
22 assessment to identify security vulnerabilities in the vetting process for the
23 PreCheck Program, including determining whether subjecting PreCheck
24 Program participants to recurrent fingerprint-based criminal history records
25 checks, in addition to recurrent checks against the terrorist watchlist, could
26 be done in a cost-effective manner to strengthen the security of the
27 PreCheck Program.

28 (k) ASSURANCE OF SEPARATE PROGRAM.—In carrying out this section,
29 the Administrator shall ensure that the additional private-sector application
30 capabilities under subsections (b), (c), and (d) are undertaken in addition
31 to any other related Transportation Security Administration program, ini-
32 tiative, or procurement, including the Universal Enrollment Services pro-
33 gram.

34 (l) EXPENDITURE OF FUNDS.—Federal funds expended by the Adminis-
35 trator to expand PreCheck Program enrollment shall be expended in a man-
36 ner that includes the requirements of this section.

37 **§ 40930. PreCheck expedited screening**

38 (a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this
39 section, the term “appropriate committees of Congress” means—

40 (1) the Committee on Commerce, Science, and Transportation of the
41 Senate;

1 (2) the Committee on Homeland Security and Governmental Affairs
2 of the Senate; and

3 (3) the Committee on Homeland Security of the House of Represent-
4 atives.

5 (b) IN GENERAL.—The Administrator shall ensure that only a traveler
6 who is a member of a trusted traveler program specified in subsection (c)
7 is permitted to use a PreCheck security screening lane at a passenger
8 screening checkpoint.

9 (c) TRUSTED TRAVELER PROGRAMS SPECIFIED.—A trusted traveler pro-
10 gram specified in this subsection is any of the following:

11 (1) The PreCheck Program under section 40929 of this title.

12 (2) Any other program implemented by the Transportation Security
13 Administration under section 11521(a)(3) of this title

14 (3) Any other United States Government program that issues a
15 unique identifier, such as a known traveler number, that the Transpor-
16 tation Security Administration accepts as validating that the individual
17 holding the identifier is a member of a known low-risk population.

18 (d) EXEMPTIONS.—Nothing in this section shall affect—

19 (1) the authority of the Administrator, under section 40938 of this
20 title, to carry out expedited screening for members of the Armed
21 Forces with disabilities or severe injuries or veterans with disabilities
22 or severe injuries; or

23 (2) the Honor Flight program under section 40939 of this title.

24 (e) LOW-RISK TRAVELERS.—A traveler who is determined by the Admin-
25 istrator to be low risk based on the traveler’s age and who is not a member
26 of a trusted traveler program specified in subsection (c) shall be permitted
27 to utilize PreCheck security screening lanes at Transportation Security Ad-
28 ministration checkpoints when traveling on the same reservation as a mem-
29 ber of the program.

30 (f) RISK-MODIFIED SCREENING.—

31 (1) DEFINITION OF LOW-RISK PASSENGER.—In this subsection, the
32 term “low-risk passenger” means a passenger who—

33 (A) meets a risk-based, intelligence-driven criterion prescribed
34 by the Administrator; or

35 (B) undergoes a canine enhanced screening on arrival at the
36 passenger screening checkpoint.

37 (2) PILOT PROGRAM.—Not later than 60 days after October 5, 2018,
38 and subject to paragraph (3), the Administrator shall commence a pilot
39 program regarding a risk-modified screening protocol for lanes other
40 than designated PreCheck security screening lanes at passenger screen-

1 ing checkpoints, in airports of varying categories, to further segment
2 passengers based on risk.

3 (3) ELIGIBILITY.—Only a low-risk passenger shall be eligible to par-
4 ticipate in the risk-modified screening pilot program under paragraph
5 (2).

6 (4) TERMINATION.—The pilot program shall terminate on the date
7 that is 120 days after the date it commences under paragraph (2).

8 (5) BRIEFING.—Not later than 30 days after the termination date
9 under paragraph (4), the Administrator shall brief the appropriate
10 committees of Congress on the findings of the pilot program, includ-
11 ing—

12 (A) information relating to the security effectiveness and pas-
13 senger facilitation effectiveness of the risk-modified screening pro-
14 tocol;

15 (B) a determination regarding whether the risk-modified screen-
16 ing protocol was effective; and

17 (C) if the Administrator determined that the protocol was effec-
18 tive, a plan for the deployment of the protocol at as many Trans-
19 portation Security Administration passenger screening checkpoints
20 as practicable.

21 (6) IMPLEMENTATION.—In determining whether deployment of the
22 protocol at a Transportation Security Administration passenger screen-
23 ing checkpoint at an airport is practicable, the Administrator shall con-
24 sider—

25 (A) the level of risk at the airport;

26 (B) the available space at the airport;

27 (C) passenger throughput levels at the airport;

28 (D) the checkpoint configuration at the airport; and

29 (E) adequate resources to appropriately serve passengers in
30 PreCheck security screening lanes at the passenger screening
31 checkpoint.

32 (g) WORKING GROUP.—

33 (1) IN GENERAL.—In carrying out subsection (f), the Administrator
34 shall establish a working group to advise the Administrator on the de-
35 velopment of plans for the deployment of the protocol at Transpor-
36 tation Security Administration passenger screening checkpoints, other
37 than designated PreCheck security screening lanes, in the most effec-
38 tive and efficient manner practicable.

39 (2) MEMBERS.—The working group shall be comprised of represent-
40 atives of Category X, I, II, III, and IV airports and air carriers (as
41 the term is defined in section 40102 of title 49).

1 (3) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—CHAPTER 10
2 OF TITLE 5 SHALL NOT APPLY TO THE WORKING GROUP ESTABLISHED
3 UNDER THIS SUBSECTION.

4 (h) BRIEFINGS.—

5 (1) IN GENERAL.—The Administrator shall brief, on a biannual
6 basis, the appropriate committees of Congress on the implementation
7 of subsection (b) until the Administrator certifies that only travelers
8 who are members of trusted traveler programs specified in subsection
9 (c) are permitted to use PreCheck security screening lanes at passenger
10 screening checkpoints.

11 (2) CERTIFICATION.—On a determination by the Administrator that
12 only travelers who are members of a trusted traveler program specified
13 in subsection (c) are permitted to use PreCheck security screening
14 lanes at checkpoints in accordance with subsection (b), the Adminis-
15 trator shall submit to the appropriate committees of Congress a written
16 certification relating to the determination.

17 (i) INSPECTOR GENERAL ASSESSMENTS.—The Inspector General of the
18 Department shall assess and transmit to the appropriate committees of
19 Congress the Administrator's implementation under subsection (b).

20 (j) EXPANSION OF PRECHECK PROGRAM ENROLLMENT.—

21 (1) LONG-TERM STRATEGY.—The Administrator shall develop and
22 begin the implementation of a long-term strategy to increase enrollment
23 in the PreCheck Program.

24 (2) CONSIDERATIONS.—In developing the strategy under paragraph
25 (1), the Administrator shall consider the following:

26 (A) Partnering with air carriers (as the term is defined in sec-
27 tion 40102 of title 49) to incorporate PreCheck Program pro-
28 motion opportunities in the reservation process described in sec-
29 tion 1560.101 of title 49, Code of Federal Regulations;

30 (B) Including in the PreCheck Program an individual who—

31 (i) holds a Secret, Top Secret, or Top Secret/Sensitive
32 Compartmented Information clearance, unless the individual's
33 clearance has been revoked or the individual did not pass a
34 periodic reinvestigation; or

35 (ii) is a current, full-time Federal law enforcement officer.

36 (C) Providing PreCheck Program enrollment flexibility by offer-
37 ing secure mobile enrollment platforms that facilitate in-person
38 identity verification and application data collection, such as
39 through biometrics.

40 (D) Reducing travel time to PreCheck Program enrollment cen-
41 ters for applicants, including—

1 (i) by adjusting the locations and schedules of existing
2 PreCheck Program enrollment centers to accommodate de-
3 mand;

4 (ii) by seeking to colocate the enrollment centers with exist-
5 ing facilities that support the issuance of—

6 (I) United States passports; and

7 (II) Security Identification Display Area credentials
8 (as the term is defined in section 1540.5 of title 49,
9 Code of Federal Regulations) located in public, non-se-
10 cure areas of airports if no systems of an airport oper-
11 ator are used in support of enrollment activities for the
12 credentials; and

13 (iii) by increasing the availability of PreCheck Program en-
14 rollment platforms, such as kiosks, tablets, or staffed laptop
15 stations.

16 (E) Assessing the feasibility of providing financial assistance or
17 other incentives for PreCheck Program enrollment for—

18 (i) children who are at least 12 years old but less than 18
19 years old;

20 (ii) families consisting of 5 or more immediate family mem-
21 bers;

22 (iii) private-sector entities, including small businesses, to
23 establish PreCheck Program enrollment centers in their re-
24 spective facilities; and

25 (iv) private-sector entities, including small business con-
26 cerns (as the term is described in section 3 of the Small Busi-
27 ness Act (15 U.S.C. 632)), to reimburse an employee for the
28 cost of the PreCheck Program application.

29 (k) EXTENDED ENROLLMENT FOR ERRONEOUS REVOCATION.—Notwith-
30 standing any other provision of law, the Secretary shall, with respect to an
31 individual whose enrollment in a trusted traveler program was revoked in
32 error, extend by an amount of time equal to the period of revocation the
33 period of active enrollment in the program on reenrollment in the program
34 by the individual.

35 **§ 40931. Screening partnership program**

36 (a) IN GENERAL.—An airport operator may submit to the Administrator
37 an application to carry out the screening of passengers and property at the
38 airport under section 40911 of this title by personnel of a qualified private
39 screening company pursuant to a contract entered into with the Transpor-
40 tation Security Administration.

41 (b) APPROVAL OF APPLICATIONS.—

1 (1) IN GENERAL.—Not later than 60 days after the date of receipt
2 of an application submitted by an airport operator under subsection
3 (a), the Administrator shall approve or deny the application.

4 (2) STANDARDS.—The Administrator shall approve an application
5 submitted by an airport operator under subsection (a) if the Adminis-
6 trator determines that the approval would not compromise security or
7 detrimentally affect the cost-efficiency or the effectiveness of the
8 screening of passengers or property at the airport.

9 (3) REPORTS ON DENIALS OF APPLICATIONS.—

10 (A) IN GENERAL.—If the Administrator denies an application
11 submitted by an airport operator under subsection (a), the Admin-
12 istrator shall provide to the airport operator, not later than 60
13 days following the date of the denial, a written report that sets
14 forth—

15 (i) the findings that served as the basis for the denial;

16 (ii) the results of a cost or security analysis conducted in
17 considering the application; and

18 (iii) recommendations on how the airport operator can ad-
19 dress the reasons for the denial.

20 (B) SUBMISSION TO CONGRESS.—The Administrator shall sub-
21 mit to the Committee on Commerce, Science, and Transportation
22 of the Senate and the Committee on Homeland Security of the
23 House of Representatives a copy of a report provided to an airport
24 operator under subparagraph (A).

25 (c) QUALIFIED PRIVATE SCREENING COMPANY.—A private screening
26 company is qualified to provide screening services at an airport under this
27 section if the company will only employ individuals to provide the services
28 who meet all the requirements of this chapter applicable to Federal Govern-
29 ment personnel who perform screening services at airports under this chap-
30 ter and will provide compensation and other benefits to the individuals that
31 are not less than the level of compensation and other benefits provided to
32 the Federal Government personnel in accordance with this chapter.

33 (d) SELECTION OF CONTRACTS AND STANDARDS FOR PRIVATE SCREEN-
34 ING COMPANIES.—

35 (1) IN GENERAL.—The Administrator shall, on approval of the appli-
36 cation, provide the airport operator with a list of qualified private
37 screening companies.

38 (2) CONTRACTS.—The Administrator shall, to the extent practicable,
39 enter into a contract with a private screening company from the list
40 provided under paragraph (1) for the provision of screening at the air-

1 port not later than 120 days after the date of approval of an applica-
2 tion submitted by the airport operator under subsection (a) if—

3 (A) the level of screening services and protection provided at the
4 airport under the contract will be equal to or greater than the level
5 that would be provided at the airport by Federal Government per-
6 sonnel under this chapter;

7 (B) the private screening company is owned and controlled by
8 a citizen of the United States, to the extent that the Administrator
9 determines that there are private screening companies owned and
10 controlled by citizens of the United States; and

11 (C) the selected qualified private screening company offered con-
12 tract price is equal to or less than the cost to the Federal Govern-
13 ment to provide screening services at the airport.

14 (3) WAIVERS.—The Administrator may waive the requirement of
15 paragraph (2)(B) for a company that is a United States subsidiary
16 with a parent company that has implemented a foreign ownership, con-
17 trol, or influence mitigation plan that has been approved by the De-
18 fense Security Service of the Department of Defense prior to the sub-
19 mission of the application. The Administrator has complete discretion
20 to reject any application from a private screening company that re-
21 quires a waiver under this paragraph to provide screening services at
22 an airport.

23 (e) SUPERVISION OF SCREENING PERSONNEL.—The Administrator
24 shall—

25 (1) provide Federal Government supervisors to oversee all screening
26 at each airport at which screening services are provided under this sec-
27 tion and provide Federal Government law enforcement officers at the
28 airport pursuant to this chapter; and

29 (2) undertake covert testing and remedial training support for em-
30 ployees of private screening companies providing screening at airports.

31 (f) SUSPENSION OF TERMINATION OF CONTRACTS.—The Administrator
32 may suspend or terminate, as appropriate, a contract entered into with a
33 private screening company to provide screening services at an airport under
34 this section if the Administrator finds that the company has failed repeat-
35 edly to comply with a standard, regulation, directive, order, law, or contract
36 applicable to the hiring or training of personnel to provide services or to
37 the provision of screening at the airport.

38 (g) OPERATOR NOT LIABLE.—Notwithstanding another law, an operator
39 of an airport is not liable for a claim for damages filed in State or Federal
40 court (including a claim for compensatory, punitive, contributory, or indem-
41 nity damages) relating to—

- 1 (1) the airport operator's decision—
2 (A) to submit an application to the Administrator under sub-
3 section (a); or
4 (B) not to submit an application; and
5 (2) an act of negligence, gross negligence, or intentional wrongdoing
6 by—
7 (A) a qualified private screening company or its employees in
8 a case in which the qualified private screening company is acting
9 under a contract entered into with the Secretary or the Secretary's
10 designee; or
11 (B) employees of the Federal Government providing passenger
12 and property security screening services at the airport.

13 (h) EVALUATION OF SCREENING COMPANY PROPOSALS FOR AWARD.—

14 (1) IN GENERAL.—Except as provided in paragraph (2), notwith-
15 standing another law, including title 48 of the Code of Federal Regula-
16 tions and the Federal Advisory Committee Act (5 U.S.C. App.), an air-
17 port operator that has applied and been approved to have security
18 screening services carried out by a qualified private screening company
19 under contract with the Administrator may nominate to the head of the
20 contracting activity an individual to participate in the evaluation of
21 proposals for the award of the contract.

22 (2) PARTICIPATION ON A PROPOSAL EVALUATION COMMITTEE.—Par-
23 ticipation on a proposal evaluation committee under paragraph (1)
24 shall be conducted in accordance with chapter 21 of title 41.

25 (i) INNOVATIVE SCREENING APPROACHES AND TECHNOLOGIES.—The
26 Administrator shall encourage an airport operator to whom screening serv-
27 ices are provided under this section to recommend to the Administrator in-
28 novative screening approaches and technologies. On receipt of any rec-
29 ommendations, the Administrator shall review and, if appropriate, test, con-
30 duct a pilot project, and, if appropriate, deploy the approaches and tech-
31 nologies.

32 (j) OPERATOR LIABILITY.—Nothing in this section shall relieve an airport
33 operator from liability for its own acts or omissions related to its security
34 responsibilities. Except as may be provided by subchapter II of chapter 109
35 of this title, nothing in this section shall relieve a qualified private screening
36 company or its employees from liability related to its own acts of negligence,
37 gross negligence, or intentional wrongdoing.

38 **§ 40932. Federal flight deck officer program**

39 (a) DEFINITIONS.—In this section:

40 (1) AIR TRANSPORTATION.—The term “air transportation” includes
41 all-cargo air transportation.

1 (2) FIREARMS TRAINING FACILITY.—The term “firearms training fa-
2 cility” means a private or government-owned gun range approved by
3 the Administrator to provide recurrent or requalification training, as
4 applicable for the program, using a Transportation Security Adminis-
5 tration-approved contractor and a curriculum developed and approved
6 by the Transportation Security Administration.

7 (3) PILOT.—The term “pilot” means an individual who has final au-
8 thority and responsibility for the operation and safety of a flight or an-
9 other flight deck crew member.

10 (b) NONAPPLICABILITY.—This section does not apply to air carriers oper-
11 ating under part 135 of title 14, Code of Federal Regulations, and to pilots
12 employed by the carriers to the extent that the carriers and pilots are cov-
13 ered by section 135.119 of title 14, Code of Federal Regulations, or a suc-
14 cessor to that section.

15 (c) ESTABLISHMENT.—The Administrator shall establish a program to
16 deputize volunteer pilots of air carriers providing air transportation or intra-
17 state air transportation as Federal law enforcement officers to defend the
18 flight decks of aircraft of air carriers against acts of criminal violence or
19 air piracy. The officers shall be known as “Federal flight deck officers”.

20 (d) PROCEDURAL REQUIREMENTS.—

21 (1) IN GENERAL.—The Administrator shall establish procedural re-
22 quirements to carry out the program under this section.

23 (2) COMMENCEMENT OF PROGRAM.—The Administrator shall train
24 and deputize pilots who are qualified to be Federal flight deck officers
25 as Federal flight deck officers under the program.

26 (3) ISSUES TO BE ADDRESSED.—The procedural requirements estab-
27 lished under paragraph (1) shall address the following issues:

28 (A) The type of firearm to be used by a Federal flight deck offi-
29 cer.

30 (B) The type of ammunition to be used by a Federal flight deck
31 officer.

32 (C) The standards and training needed to qualify and requalify
33 as a Federal flight deck officer.

34 (D) The placement of the firearm of a Federal flight deck offi-
35 cer on board the aircraft to ensure both its security and its ease
36 of retrieval in an emergency.

37 (E) An analysis of the risk of catastrophic failure of an aircraft
38 as a result of the discharge (including an accidental discharge) of
39 a firearm to be used in the program into the avionics, electrical
40 systems, or other sensitive areas of the aircraft.

1 (F) The division of responsibility between pilots in the event of
2 an act of criminal violence or air piracy if only one pilot is a Fed-
3 eral flight deck officer and if both pilots are Federal flight deck
4 officers.

5 (G) Procedures for ensuring that the firearm of a Federal flight
6 deck officer does not leave the cockpit if there is a disturbance in
7 the passenger cabin of the aircraft or if the pilot leaves the cockpit
8 for personal reasons.

9 (H) Interaction between a Federal flight deck officer and a Fed-
10 eral air marshal on board the aircraft.

11 (I) The process for selection of pilots to participate in the pro-
12 gram based on their fitness to participate in the program, includ-
13 ing whether an additional background check should be required be-
14 yond that required by section 40956(a)(1) of this title.

15 (J) Storage and transportation of firearms between flights, in-
16 cluding international flights, to ensure the security of the firearms,
17 focusing particularly on whether security would be enhanced by re-
18 quiring storage of the firearm at the airport when the pilot leaves
19 the airport to remain overnight away from the pilot's base airport.

20 (K) Methods for ensuring that security personnel will be able
21 to identify whether a pilot may carry a firearm under the pro-
22 gram.

23 (L) Methods for ensuring that pilots (including Federal flight
24 deck officers) will be able to identify whether a passenger is a law
25 enforcement officer who may carry a firearm aboard the aircraft.

26 (M) Other issues that the Administrator considers necessary.

27 (4) PREFERENCE.—In selecting pilots to participate in the program,
28 the Administrator shall give preference to pilots who are former mili-
29 tary or law enforcement personnel.

30 (5) CLASSIFIED INFORMATION.—Notwithstanding section 552 of title
31 5, information developed under paragraph (3)(E) shall not be disclosed.

32 (6) NOTICE TO CONGRESS.—The Administrator shall provide notice
33 to the Committee on Transportation and Infrastructure of the House
34 of Representatives and the Committee on Commerce, Science, and
35 Transportation of the Senate after completing the analysis required by
36 paragraph (3)(E).

37 (7) MINIMIZATION OF RISK.—If the Administrator determines as a
38 result of the analysis under paragraph (3)(E) that there is a significant
39 risk of the catastrophic failure of an aircraft as a result of the dis-
40 charge of a firearm, the Administrator shall take necessary actions to
41 minimize that risk.

1 (8) REVIEW STANDARD.—The Administrator’s decisions regarding
2 the methods for implementing each of the procedural requirements
3 specified in paragraph (3) shall be subject to review only for abuse of
4 discretion.

5 (e) TRAINING, SUPERVISION, AND EQUIPMENT.—

6 (1) IN GENERAL.—The Administrator shall only be obligated to pro-
7 vide the training, supervision, and equipment necessary for a pilot to
8 be a Federal flight deck officer under this section at no expense to the
9 pilot or the air carrier employing the pilot.

10 (2) TRAINING.—

11 (A) IN GENERAL.—The Administrator shall base the require-
12 ments for the training of Federal flight deck officers under sub-
13 section (d) on the training standards applicable to Federal air
14 marshals, except that the Administrator shall take into account
15 the differing roles and responsibilities of Federal flight deck offi-
16 cers and Federal air marshals.

17 (B) ELEMENTS.—The training of a Federal flight deck officer
18 shall include, at a minimum—

19 (i) training to ensure that the officer achieves the level of
20 proficiency with a firearm required under subparagraph
21 (C)(i);

22 (ii) training to ensure that the officer maintains exclusive
23 control over the officer’s firearm at all times, including train-
24 ing in defensive maneuvers; and

25 (iii) training to assist the officer in determining when it is
26 appropriate to use the officer’s firearm and when it is appro-
27 priate to use less than lethal force.

28 (C) TRAINING IN USE OF FIREARMS.—

29 (i) LEVEL OF PROFICIENCY.—To be deputized as a Federal
30 flight deck officer, a pilot must achieve a level of proficiency
31 with a firearm that is required by the Administrator. The
32 level shall be comparable to the level of proficiency required
33 of Federal air marshals.

34 (ii) TRAINING BY ADMINISTRATOR OR FIREARMS TRAINING
35 FACILITY.—

36 (I) IN GENERAL.—The training of a Federal flight
37 deck officer in the use of a firearm may be conducted
38 by the Administrator or by a firearms training facility.

39 (II) ACCESS TO TRAINING FACILITIES.—The Adminis-
40 trator shall designate additional firearms training facili-
41 ties located in various regions of the United States for

1 Federal flight deck officers for recurrent and requali-
2 fying training relative to the number of the facilities
3 available on the day before October 5, 2018.

4 (iii) REQUALIFICATION.—

5 (I) IN GENERAL.—The Administrator shall require a
6 Federal flight deck officer to requalify to carry a firearm
7 under the program. The requalification shall occur at an
8 interval required by the Administrator.

9 (II) USE OF FACILITIES FOR REQUALIFICATION.—The
10 Administrator shall allow a Federal flight deck officer to
11 requalify to carry a firearm under the program through
12 training at a Transportation Security Administration-ap-
13 proved firearms training facility utilizing a Transpor-
14 tation Security Administration-approved contractor and
15 a curriculum developed and approved by the Transpor-
16 tation Security Administration.

17 (iv) PERIODIC REVIEW.—The Administrator shall periodi-
18 cally review requalification training intervals and assess
19 whether it is appropriate and sufficient to adjust the time be-
20 tween each requalification training to facilitate continued par-
21 ticipation in the program under this section while still main-
22 taining effectiveness of the training, and update the training
23 requirements as appropriate.

24 (D) TRAINING REVIEW.—Not later than 2 years after October
25 5, 2018, and biennially thereafter, the Administrator shall review
26 training facilities and training requirements for initial and recur-
27 rent training for Federal flight deck officers and evaluate how
28 training requirements, including the length of training, could be
29 streamlined while maintaining the effectiveness of the training,
30 and update the training requirements as appropriate.

31 (f) DEPUTIZATION.—

32 (1) IN GENERAL.—The Administrator may deputize, as a Federal
33 flight deck officer under this section, a pilot who submits to the Admin-
34 istrator a request to be such an officer and who the Administrator de-
35 termines is qualified to be such an officer.

36 (2) QUALIFICATION.—

37 (A) IN GENERAL.—A pilot is qualified to be a Federal flight
38 deck officer under this section if—

39 (i) the pilot is employed by an air carrier;

1 (ii) the Administrator determines that the pilot meets the
2 standards established by the Administrator for being a Fed-
3 eral flight deck officer; and

4 (iii) the Administrator determines that the pilot has com-
5 pleted the training required by the Administrator.

6 (B) CONSISTENCY WITH REQUIREMENTS FOR CERTAIN MEDICAL
7 CERTIFICATES.—In establishing standards under subparagraph
8 (A)(ii), the Administrator may not establish medical or physical
9 standards for a pilot to become a Federal flight deck officer that
10 are inconsistent with or more stringent than the requirements of
11 the Federal Aviation Administration for the issuance of the re-
12 quired airman medical certificate under part 67 of title 14, Code
13 of Federal Regulations (or any corresponding similar regulation or
14 ruling).

15 (3) DEPUTIZATION BY OTHER FEDERAL AGENCIES.—The Adminis-
16 trator may request another Federal agency to deputize, as Federal
17 flight deck officers under this section, pilots that the Administrator de-
18 termines are qualified to be Federal flight deck officers.

19 (4) REVOCATION.—The Administrator may revoke the deputization
20 of a pilot as a Federal flight deck officer if the Administrator finds
21 that the pilot is no longer qualified to be a Federal flight deck officer.

22 (5) TRANSFER FROM INACTIVE TO ACTIVE STATUS.—In accordance
23 with any applicable Transportation Security Administration appeals
24 processes, a pilot deputized as a Federal flight deck officer who moves
25 to inactive status may return to active status on successful completion
26 of a recurrent training program administered within program guide-
27 lines.

28 (g) COMPENSATION.—

29 (1) IN GENERAL.—Pilots participating in the program under this
30 section shall not be eligible for compensation from the Federal Govern-
31 ment for services provided as a Federal flight deck officer. The Federal
32 Government and air carriers shall not be obligated to compensate a
33 pilot for participating in the program or for the pilot's training or qual-
34 ification and requalification to carry firearms under the program.

35 (2) FACILITATION OF TRAINING.—An air carrier shall permit a pilot
36 seeking to be deputized as a Federal flight deck officer or a Federal
37 flight deck officer to take a reasonable amount of leave to participate
38 in initial, recurrent, or requalification training, as applicable, for the
39 program. Leave required under this paragraph may be provided with-
40 out compensation.

41 (h) AUTHORITY TO CARRY FIREARMS.—

1 (1) IN GENERAL.—The Administrator shall authorize a Federal
2 flight deck officer to carry a firearm while engaged in providing air
3 transportation or intrastate air transportation. Notwithstanding sub-
4 section (e)(1), the officer may purchase a firearm and carry that fire-
5 arm aboard an aircraft of which the officer is the pilot under this sec-
6 tion if the firearm is of a type that may be used under the program.

7 (2) PREEMPTION.—Notwithstanding another Federal or State law, a
8 Federal flight deck officer, whenever necessary to participate in the
9 program, may carry a firearm in a State and from one State to another
10 State.

11 (3) CARRYING FIREARMS OUTSIDE UNITED STATES.—In consultation
12 with the Secretary of State, the Administrator may take necessary ac-
13 tion to ensure that a Federal flight deck officer may carry a firearm
14 in a foreign country whenever necessary to participate in the program.

15 (4) CONSISTENCY WITH FEDERAL AIR MARSHAL PROGRAM.—The
16 Administrator shall harmonize, to the extent practicable and in a man-
17 ner that does not jeopardize existing Federal air marshal agreements,
18 the policies relating to the carriage of firearms on international flights
19 by Federal flight deck officers with the policies of the Federal air mar-
20 shal program for carrying firearms on international flights and car-
21 rying out the duties of a Federal flight deck officer, notwithstanding
22 Annex 17 of the International Civil Aviation Organization.

23 (i) AUTHORITY TO USE FORCE.—Notwithstanding section 40913(d) of
24 this title, the Administrator shall prescribe the standards and circumstances
25 under which a Federal flight deck officer may use, while the program under
26 this section is in effect, force (including lethal force) against an individual
27 in the defense of the flight deck of an aircraft in air transportation or intra-
28 state air transportation.

29 (j) LIMITATION ON LIABILITY.—

30 (1) AIR CARRIERS.—An air carrier is not liable for damages in an
31 action brought in a Federal or State court arising out of a Federal
32 flight deck officer's use of or failure to use a firearm.

33 (2) FEDERAL FLIGHT DECK OFFICERS.—A Federal flight deck offi-
34 cer is not liable for damages in an action brought in a Federal or State
35 court arising out of the acts or omissions of the officer in defending
36 the flight deck of an aircraft against acts of criminal violence or air
37 piracy unless the officer is guilty of gross negligence or willful mis-
38 conduct.

39 (3) FEDERAL GOVERNMENT.—For purposes of an action against the
40 United States with respect to an act or omission of a Federal flight
41 deck officer in defending the flight deck of an aircraft, the officer shall

1 be treated as an employee of the Federal Government under chapter
2 171 of title 28, relating to tort claims procedure.

3 (k) PROCEDURES FOLLOWING ACCIDENTAL DISCHARGES.—If an acci-
4 dental discharge of a firearm under the pilot program results in the injury
5 or death of a passenger or crew member on an aircraft—

6 (1) the Administrator shall revoke the deputization of the Federal
7 flight deck officer responsible for that firearm if the Administrator de-
8 termines that the discharge was attributable to the negligence of the
9 officer; and

10 (2) if the Administrator determines that a shortcoming in standards,
11 training, or procedures was responsible for the accidental discharge, the
12 Administrator may temporarily suspend the program until the short-
13 coming is corrected.

14 (l) LIMITATION ON AUTHORITY OF AIR CARRIERS.—An air carrier may
15 not—

16 (1) prohibit a pilot employed by the air carrier from becoming a Fed-
17 eral flight deck officer under this section;

18 (2) threaten a retaliatory action against a pilot employed by the air
19 carrier for becoming a Federal flight deck officer under this section;

20 (3) prohibit a Federal flight deck officer from piloting an aircraft op-
21 erated by the air carrier; or

22 (4) terminate the employment of a Federal flight deck officer, solely
23 on the basis of his or her volunteering for or participating in the pro-
24 gram under this section.

25 (m) CLASSIFY INFORMATION AS SENSITIVE SECURITY INFORMATION.—
26 Not later than 180 days after October 5, 2018—

27 (1) the Secretary of Transportation shall revise section 15.5(b)(11)
28 of title 49, Code of Federal Regulations, to classify information about
29 pilots deputized as Federal flight deck officers under this section as
30 sensitive security information in a manner consistent with the classi-
31 fication of information about Federal air marshals; and

32 (2) the Administrator shall revise section 1520.5(b)(11) of title 49,
33 Code of Federal Regulations, to classify information about pilots depu-
34 tized as Federal flight deck officers under this section as sensitive secu-
35 rity information in a manner consistent with the classification of infor-
36 mation about Federal air marshals.

37 (n) REGULATIONS.—Not later than 180 days after October 5, 2018, the
38 Administrator shall prescribe such regulations as may be necessary to carry
39 out this section.

1 **§ 40933. Deputization of State and local law enforcement of-**
2 **ficers**

3 (a) DEPUTIZATION AUTHORITY.—The Administrator may deputize a
4 State or local law enforcement officer to carry out Federal airport security
5 duties under this chapter.

6 (b) FULFILLMENT OF REQUIREMENTS.—A State or local law enforcement
7 officer who is deputized under this section shall be treated as a Federal law
8 enforcement officer for purposes of meeting the requirements of this chapter
9 and other provisions of law to provide Federal law enforcement officers to
10 carry out Federal airport security duties.

11 (c) AGREEMENTS.—To deputize a State or local law enforcement officer
12 under this section, the Administrator shall enter into a voluntary agreement
13 with the appropriate State or local law enforcement agency that employs the
14 State or local law enforcement officer.

15 (d) REIMBURSEMENT.—The Administrator shall reimburse a State or
16 local law enforcement agency for all reasonable, allowable, and allocable
17 costs incurred by the State or local law enforcement agency with respect to
18 a law enforcement officer deputized under this section.

19 (e) FEDERAL TORT CLAIMS ACT.—A State or local law enforcement offi-
20 cer who is deputized under this section shall be treated as an “employee
21 of the Government” for purposes of sections 1346(b) and 2401(b) and chap-
22 ter 171 of title 28 while carrying out Federal airport security duties in the
23 course and scope of the officer’s employment, subject to Federal supervision
24 and control, and under the terms of the deputization.

25 (f) STATIONING OF OFFICERS.—The Administrator may allow law en-
26 forcement personnel to be stationed other than at the airport security
27 screening location if that would be preferable for law enforcement purposes
28 and if the personnel would still be able to provide a prompt response to
29 problems occurring at the screening location.

30 **§ 40934. Airport security improvement projects**

31 (a) DEFINITION OF SPONSOR.—In this section, the term “sponsor” has
32 the meaning given the term in section 47102 of title 49.

33 (b) GRANT AUTHORITY.—Subject to the requirements of this section, the
34 Administrator shall make grants to airport sponsors—

35 (1) for projects to replace baggage conveyer systems related to avia-
36 tion security;

37 (2) for projects to reconfigure terminal baggage areas as needed to
38 install explosive detection systems;

39 (3) for projects to enable the Administrator to deploy explosive detec-
40 tion systems behind the ticket counter, in the baggage sorting area, or
41 in line with the baggage handling system; and

1 (4) for other airport security capital improvement projects.

2 (c) APPLICATIONS.—A sponsor seeking a grant under this section shall
3 submit to the Administrator an application in the form, and containing the
4 information, the Administrator prescribes.

5 (d) APPROVAL.—The Administrator, after consultation with the Secretary
6 of Transportation, may approve an application of a sponsor for a grant
7 under this section only if the Administrator determines that the project will
8 improve security at an airport or improve the efficiency of the airport with-
9 out lessening security.

10 (e) LETTERS OF INTENT.—

11 (1) ISSUANCE.—The Administrator shall issue a letter of intent to
12 a sponsor committing to obligate from future budget authority an
13 amount, not more than the Federal Government's share of the project's
14 cost, for an airport security improvement project (including interest
15 costs and costs of formulating the project).

16 (2) SCHEDULE.—A letter of intent under this subsection shall estab-
17 lish a schedule under which the Administrator will reimburse the spon-
18 sor for the Government's share of the project's costs, as amounts be-
19 come available, if the sponsor, after the Administrator issues the letter,
20 carries out the project without receiving amounts under this section.

21 (3) NOTICE TO ADMINISTRATOR.—A sponsor that has been issued a
22 letter of intent under this subsection shall notify the Administrator of
23 the sponsor's intent to carry out a project before the project begins.

24 (4) NOTICE TO CONGRESS.—The Administrator shall transmit to the
25 Committee on Appropriations and the Committee on Transportation
26 and Infrastructure of the House of Representatives and the Committee
27 on Appropriations and the Committee on Commerce, Science, and
28 Transportation of the Senate a written notification at least 3 days be-
29 fore the issuance of a letter of intent under this section.

30 (5) LIMITATIONS.—A letter of intent issued under this subsection is
31 not an obligation of the Government under section 1501 of title 31,
32 and the letter is not deemed to be an administrative commitment for
33 financing. An obligation or administrative commitment may be made
34 only as amounts are provided in authorization and appropriations laws.

35 (6) STATUTORY CONSTRUCTION.—Nothing in this subsection shall be
36 construed to prohibit the obligation of amounts pursuant to a letter of
37 intent under this subsection in the same fiscal year as the letter of in-
38 tent is issued.

39 (f) FEDERAL SHARE.—The Government's share of the cost of a project
40 under this section shall be 90 percent for a project at a medium or large
41 hub airport and 95 percent for a project at any other airport.

1 (g) APPLICABILITY OF CERTAIN REQUIREMENTS.—The requirements
2 that apply to grants and letters of intent issued under chapter 471 of title
3 49 (other than section 47102(3)) shall apply to grants and letters of intent
4 issued under this section.

5 (h) AVIATION SECURITY CAPITAL FUND.—

6 (1) IN GENERAL.—There is established in the Department the Avia-
7 tion Security Capital Fund. The first \$250,000,000 from fees received
8 under section 40960(a) of this title in each of fiscal years 2004
9 through 2028 is available to be deposited in the Fund. The Adminis-
10 trator shall impose the fee authorized by section 40960(a) of this title
11 so as to collect at least \$250,000,000 in each of the fiscal years for
12 deposit into the Fund. Amounts in the Fund are available to the Ad-
13 ministrator to make grants under this section.

14 (2) ALLOCATION.—Of the amount made available under paragraph
15 (1) for a fiscal year, not less than \$200,000,000 shall be allocated to
16 fulfill letters of intent issued under subsection (e).

17 (3) DISCRETIONARY GRANTS.—Of the amount made available under
18 paragraph (1) for a fiscal year, up to \$50,000,000 shall be used to
19 make discretionary grants, including other transaction agreements for
20 airport security improvement projects, with priority given to small hub
21 airports and nonhub airports.

22 (i) LEVERAGED FUNDING.—For purposes of this section, a grant under
23 subsection (b) to an airport sponsor to service an obligation issued by or
24 on behalf of that sponsor to fund a project described in subsection (b) is
25 considered to be a grant for that project.

26 **§ 40935. Repair station security**

27 (a) SECURITY REVIEW AND AUDIT.—To ensure the security of mainte-
28 nance and repair work conducted on air carrier aircraft and components at
29 foreign repair stations, the Administrator, in consultation with the Adminis-
30 trator of the Federal Aviation Administration, shall complete a security re-
31 view and audit of foreign repair stations that are certified by the Adminis-
32 trator of the Federal Aviation Administration under part 145 of title 14,
33 Code of Federal Regulations, and that work on air carrier aircraft and com-
34 ponents. The review shall be completed no later than 6 months after the
35 date on which the Administrator issues regulations under subsection (f).

36 (b) ADDRESSING SECURITY CONCERNS.—The Administrator shall require
37 a foreign repair station to address the security issues and vulnerabilities
38 identified in a security audit conducted under subsection (a) within 90 days
39 of providing notice to the repair station of the security issues and
40 vulnerabilities so identified and shall notify the Administrator of the Federal

1 Aviation Administration that a deficiency was identified in the security
2 audit.

3 (c) SUSPENSIONS AND REVOCATIONS OF CERTIFICATES.—

4 (1) FAILURE TO CARRY OUT EFFECTIVE SECURITY MEASURES.—If,
5 after the 90th day on which a notice is provided to a foreign repair
6 station under subsection (b), the Administrator determines that the
7 foreign repair station does not maintain and carry out effective security
8 measures, the Administrator shall notify the Administrator of the Fed-
9 eral Aviation Administration of the determination. On receipt of the de-
10 termination, the Administrator of the Federal Aviation Administration
11 shall suspend the certification of the repair station until the Adminis-
12 trator determines that the repair station maintains and carries out ef-
13 fective security measures and transmits the determination to the Ad-
14 ministrator of the Federal Aviation Administration.

15 (2) IMMEDIATE SECURITY RISK.—If the Administrator determines
16 that a foreign repair station poses an immediate security risk, the Ad-
17 ministrator shall notify the Administrator of the Federal Aviation Ad-
18 ministration of the determination. On receipt of the determination, the
19 Administrator of the Federal Aviation Administration shall revoke the
20 certification of the repair station.

21 (3) PROCEDURES FOR APPEALS.—The Administrator, in consultation
22 with the Administrator of the Federal Aviation Administration, shall
23 establish procedures for appealing a revocation of a certificate under
24 this subsection.

25 (d) FAILURE TO MEET AUDIT DEADLINE.—If the security audits re-
26 quired by subsection (a) are not completed on or before the date that is
27 6 months after the date on which the Administrator issues regulations
28 under subsection (f), the Administrator of the Federal Aviation Administra-
29 tion shall be barred from certifying a foreign repair station (other than a
30 station that was previously certified, or is in the process of certification, by
31 the Administrator of the Federal Aviation Administration under part A of
32 subtitle VII of title 49) until the audits are completed for existing stations.

33 (e) PRIORITY FOR AUDITS.—In conducting the audits described in sub-
34 section (a), the Administrator and the Administrator of the Federal Avia-
35 tion Administration shall give priority to foreign repair stations located in
36 countries identified by the Government as posing the most significant secu-
37 rity risks.

38 (f) REGULATIONS.—The Administrator, in consultation with the Adminis-
39 trator of the Federal Aviation Administration, shall issue final regulations
40 to ensure the security of foreign and domestic aircraft repair stations.

1 **§ 40936. Deployment and use of detection equipment at air-**
2 **port screening checkpoints**

3 (a) WEAPONS AND EXPLOSIVES.—The Secretary shall give a high priority
4 to developing, testing, improving, and deploying, at airport screening check-
5 points, equipment that detects nonmetallic, chemical, biological, and radio-
6 logical weapons, and explosives, in all forms, on individuals and in their per-
7 sonal property. The Secretary shall ensure that the equipment alone, or as
8 part of an integrated system, can detect under realistic operating conditions
9 the types of weapons and explosives that terrorists would likely try to smug-
10 gle aboard an air carrier aircraft.

11 (b) STRATEGIC PLAN FOR DEPLOYMENT AND USE OF EXPLOSIVE DE-
12 TECTION EQUIPMENT AT AIRPORT SCREENING CHECKPOINTS.—

13 (1) IN GENERAL.—The Administrator shall submit to the appro-
14 priate congressional committees a strategic plan to promote the optimal
15 utilization and deployment of explosive detection equipment at airports
16 to screen individuals and their personal property. Such equipment in-
17 cludes walk-through explosive detection portals, document scanners,
18 shoe scanners, and backscatter x-ray scanners. The plan may be sub-
19 mitted in a classified format.

20 (2) CONTENT.—The strategic plan shall include, at minimum—

21 (A) a description of current efforts to detect explosives in all
22 forms on individuals and in their personal property;

23 (B) a description of the operational applications of explosive de-
24 tection equipment at airport screening checkpoints;

25 (C) a deployment schedule and a description of the quantities
26 of equipment needed to implement the plan;

27 (D) a description of funding needs to implement the plan, in-
28 cluding a financing plan that provides for leveraging of non-Fed-
29 eral funding;

30 (E) a description of the measures taken and anticipated to be
31 taken in carrying out subsection (d); and

32 (F) a description of any recommended legislative actions.

33 (c) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be ap-
34 propriated to the Secretary for the use of the Transportation Security Ad-
35 ministration \$250,000,000, in addition to amounts otherwise authorized by
36 law, for research, development, and installation of detection systems and
37 other devices for the detection of biological, chemical, radiological, and ex-
38 plosive materials.

39 (d) INTERIM ACTION.—Until measures are implemented that enable the
40 screening of all passengers for explosives, the Administrator shall provide,
41 by means the Administrator considers appropriate, explosives detection

1 screening for all passengers identified for additional screening and their personal
2 property that will be carried aboard a passenger aircraft operated by
3 an air carrier or foreign air carrier in air transportation or intrastate air
4 transportation.

5 **§ 40937. Appeal and redress process for passengers wrongly**
6 **delayed or prohibited from boarding a flight**

7 (a) IN GENERAL.—The Secretary shall establish a timely and fair process
8 for individuals who believe they have been delayed or prohibited from board-
9 ing a commercial aircraft because they were wrongly identified as a threat
10 under the regimes utilized by the Transportation Security Administration,
11 U.S. Customs and Border Protection, or another office or component of the
12 Department.

13 (b) OFFICE OF APPEALS AND REDRESS.—

14 (1) ESTABLISHMENT.—The Secretary shall establish in the Depart-
15 ment an Office of Appeals and Redress to implement, coordinate, and
16 execute the process established by the Secretary under subsection (a).
17 The Office shall include representatives from the Transportation Secu-
18 rity Administration, U.S. Customs and Border Protection, and other
19 offices and components of the Department that the Secretary deter-
20 mines appropriate.

21 (2) RECORDS.—The process established by the Secretary under sub-
22 section (a) shall include the establishment of a method by which the
23 Office, under the direction of the Secretary, will be able to maintain
24 a record of air carrier passengers and other individuals who have been
25 misidentified and have corrected erroneous information.

26 (3) INFORMATION.—To prevent repeated delays of a misidentified
27 passenger or other individual, the Office of Appeals and Redress
28 shall—

29 (A) ensure that the records maintained under this subsection
30 contain information determined by the Secretary to authenticate
31 the identity of the passenger or individual;

32 (B) furnish to the Transportation Security Administration, U.S.
33 Customs and Border Protection, or another appropriate office or
34 component of the Department, on request, information necessary
35 to allow the office or component to assist air carriers in improving
36 their administration of the advanced passenger prescreening sys-
37 tem and reduce the number of false positives; and

38 (C) require that air carriers and foreign air carriers take action
39 to identify passengers determined, under the process established
40 under subsection (a), to have been wrongly identified.

1 (4) HANDLING OF PERSONALLY IDENTIFIABLE INFORMATION.—The
2 Secretary, in conjunction with the Chief Privacy Officer of the Depart-
3 ment, shall—

4 (A) require that Federal employees of the Department handling
5 personally identifiable information of passengers (in this para-
6 graph referred to as “PII”) complete mandatory privacy and secu-
7 rity training prior to being authorized to handle PII;

8 (B) ensure that the records maintained under this subsection
9 are secured by encryption, one-way hashing, other data
10 anonymization techniques, or other, equivalent security technical
11 protections the Secretary determines necessary;

12 (C) limit the information collected from misidentified passengers
13 or other individuals to the minimum amount necessary to resolve
14 a redress request;

15 (D) require that the data generated under this subsection shall
16 be shared or transferred via a secure data network that has been
17 audited to ensure that the anti-hacking and other security related
18 software functions properly and is updated as necessary;

19 (E) ensure that an employee of the Department receiving the
20 data contained in the records handles the information under sec-
21 tion 552a of title 5 and the Federal Information Security Manage-
22 ment Act of 2002 (Public Law 107–296, 116 Stat. 2259);

23 (F) only retain the data for as long as needed to assist the indi-
24 vidual traveler in the redress process; and

25 (G) conduct and publish a privacy impact assessment of the
26 process described within this subsection and transmit the assess-
27 ment to the Committee on Homeland Security of the House of
28 Representatives, the Committee on Commerce, Science, and
29 Transportation of the Senate, and the Committee on Homeland
30 Security and Governmental Affairs of the Senate.

31 (5) INITIATION OF REDRESS PROCESS AT AIRPORTS.—The Office of
32 Appeals and Redress shall establish at each airport at which the De-
33 partment has a significant presence a process to provide information
34 to air carrier passengers to begin the redress process established under
35 subsection (a).

36 **§ 40938. Expedited screening for severely injured or dis-**
37 **abled members of the armed forces and severely**
38 **injured or disabled veterans**

39 (a) PASSENGER SCREENING.—The Administrator, in consultation with
40 the Secretary of Defense, the Secretary of Veterans Affairs, and organiza-
41 tions identified by the Secretaries of Defense and Veterans Affairs that ad-

1 vocate on behalf of severely injured or disabled members of the armed forces
2 and severely injured or disabled veterans, shall develop and implement a
3 process to support and facilitate the ease of travel and to the extent possible
4 provide expedited passenger screening services through passenger screening
5 for severely injured or disabled members of the armed forces and severely
6 injured or disabled veterans. The process shall be designed to offer the indi-
7 vidual private screening to the maximum extent practicable.

8 (b) OPERATIONS CENTER.—As part of the process under subsection (a),
9 the Administrator shall maintain an operations center to provide support
10 and facilitate the movement of severely injured or disabled members of the
11 armed forces and severely injured or disabled veterans through passenger
12 screening prior to boarding a passenger aircraft operated by an air carrier
13 or foreign air carrier in air transportation or intrastate air transportation.

14 (c) PROTOCOLS.—The Administrator shall—

15 (1) establish and publish protocols, in consultation with the Sec-
16 retary of Defense, the Secretary of Veterans Affairs, and the organiza-
17 tions identified under subsection (a), under which a severely injured or
18 disabled member of the armed forces or severely injured or disabled
19 veteran, or the family member or other representative of the member
20 or veteran, may contact the operations center maintained under sub-
21 section (b) and request the expedited passenger screening services de-
22 scribed in subsection (a) for that member or veteran; and

23 (2) on receipt of a request under paragraph (1), require the oper-
24 ations center to notify the appropriate Federal Security Director of the
25 request for expedited passenger screening services, as described in sub-
26 section (a), for that member or veteran.

27 (d) TRAINING.—The Administrator shall integrate training on the proto-
28 cols established under subsection (c) into the training provided to all em-
29 ployees who will regularly provide the passenger screening services described
30 in subsection (a).

31 (e) RULE OF CONSTRUCTION.—Nothing in this section shall affect the
32 authority of the Administrator to require additional screening of a severely
33 injured or disabled member of the armed forces, a severely injured or dis-
34 abled veteran, or their accompanying family members or nonmedical attend-
35 ants, if intelligence, law enforcement, or other information indicates that ad-
36 ditional screening is necessary.

37 (f) REPORT.—The Administrator each year shall submit to Congress a re-
38 port on the implementation of this section. Each report shall include the
39 following:

40 (1) Information on the training provided under subsection (d).

1 (2) Information on the consultations between the Administrator and
2 the organizations identified under subsection (a).

3 (3) The number of people who accessed the operations center during
4 the period covered by the report.

5 (4) Other information the Administrator determines is appropriate.

6 **§ 40939. Honor Flight program**

7 The Administrator shall establish, in collaboration with the Honor Flight
8 Network or other not-for-profit organization that honors veterans, a process
9 for providing expedited and dignified passenger screening services for vet-
10 erans traveling on an Honor Flight Network private charter, or another not-
11 for-profit organization that honors veterans, to visit war memorials built
12 and dedicated to honor the service of those veterans.

13 **§ 40940. Donation of screening equipment to protect the**
14 **United States**

15 (a) IN GENERAL.—Subject to subsection (b), the Administrator may do-
16 nate security screening equipment to a foreign last point of departure air-
17 port operator if the equipment can be reasonably expected to mitigate a spe-
18 cific vulnerability to the security of the United States or United States citi-
19 zens.

20 (b) CONDITIONS.—Before donating any security screening equipment to
21 a foreign last point of departure airport operator, the Administrator shall—

22 (1) ensure that the screening equipment has been restored to com-
23 mercially available settings;

24 (2) ensure that no Transportation Security Administration-specific
25 security standards or algorithms exist on the screening equipment; and

26 (3) verify that the appropriate officials have an adequate system—

27 (A) to properly maintain and operate the screening equipment;
28 and

29 (B) to document and track any removal or disposal of the
30 screening equipment to ensure the screening equipment does not
31 come into the possession of terrorists or otherwise pose a risk to
32 security.

33 (c) REPORTS.—Not later than 30 days before a donation of security
34 screening equipment under subsection (a), the Administrator shall provide
35 to the Committee on Commerce, Science, and Transportation and the Com-
36 mittee on Homeland Security and Governmental Affairs of the Senate and
37 the Committee on Homeland Security of the House of Representatives a de-
38 tailed written explanation of the following:

39 (1) The specific vulnerability to the United States or United States
40 citizens that will be mitigated by the donation.

1 (2) An explanation as to why the recipient of the donation is unable
2 or unwilling to purchase security screening equipment to mitigate the
3 vulnerability.

4 (3) An evacuation plan for sensitive technologies in case of emer-
5 gency or instability in the country to which the donation is being made.

6 (4) How the Administrator will ensure the security screening equip-
7 ment that is being donated is used and maintained over the course of
8 its life by the recipient.

9 (5) The total dollar value of the donation.

10 (6) How the appropriate officials will document and track removal
11 or disposal of the screening equipment by the recipient to ensure the
12 screening equipment does not come into the possession of terrorists or
13 otherwise pose a risk to security.

14 **Subchapter III—Administration and** 15 **Personnel**

16 **§ 40951. Authority to exempt from regulations**

17 The Secretary may grant an exemption from a regulation prescribed in
18 carrying out sections 40911, 40913, 40919(c), and 40955 through 40957
19 of this title when the Secretary decides the exemption is in the public inter-
20 est.

21 **§ 40952. Administrative**

22 (a) IN GENERAL.—The Secretary or the Administrator may take action
23 the Administrator considers necessary to carry out sections 11522 through
24 11524(a) of this title, subchapters I and II of this chapter, sections 40951
25 through 40961 of this title, subchapter V of this chapter, and chapter 465
26 of title 49, including conducting investigations, prescribing regulations,
27 standards, and procedures, and issuing orders.

28 (b) INDEMNIFICATION.—The Administrator may indemnify an officer or
29 employee of the Transportation Security Administration against a claim or
30 judgment arising out of an act that the Administrator decides was com-
31 mitted within the scope of the official duties of the officer or employee.

32 **§ 40953. Federal Security Directors**

33 (a) ESTABLISHMENT, DESIGNATION, AND STATIONING.—The Adminis-
34 trator shall establish the position of Federal Security Director at each air-
35 port in the United States described in section 40913(c) of this title. The
36 Administrator shall designate individuals as Federal Security Directors for,
37 and station those Federal Security Directors at, those airports.

38 (b) DUTIES AND POWERS.—The Federal Security Director at each air-
39 port shall—

40 (1) oversee the screening of passengers and property at the airport;
41 and

1 (2) carry out other duties prescribed by the Administrator.

2 (c) INFORMATION SHARING.—Not later than 1 year after October 5,
3 2018, the Administrator shall—

4 (1) require each Federal Security Director of an airport to meet at
5 least quarterly with the airport director, airport security coordinator,
6 and law enforcement agencies serving the airport to discuss incident
7 management protocols, including the resolution of screening anomalies
8 at passenger screening checkpoints; and

9 (2) require each Federal Security Director at an airport to inform,
10 consult, and coordinate, as appropriate, with the respective airport se-
11 curity coordinator in a timely manner on security matters impacting
12 airport operations and to establish and maintain operational protocols
13 with the airport operators to ensure coordinated responses to security
14 matters.

15 **§ 40954. Foreign Security Liaison Officers**

16 (a) ESTABLISHMENT, DESIGNATION, AND STATIONING.—The Adminis-
17 trator shall establish the position of Foreign Security Liaison Officer for
18 each airport outside the United States at which the Administrator decides
19 an Officer is necessary for air transportation security. In coordination with
20 the Secretary of State, the Administrator shall designate an Officer for each
21 of those airports. In coordination with the Secretary of State, the Adminis-
22 trator shall designate an Officer for each of those airports where extraor-
23 dinary security measures are in place. The Secretary of State shall give high
24 priority to stationing those Officers.

25 (b) DUTIES AND POWERS.—Each Federal Security Liaison Officer re-
26 ports directly to the Administrator. The Officer at each airport shall—

27 (1) serve as the liaison of the Administrator to foreign security au-
28 thorities (including governments of foreign countries and foreign air-
29 port authorities) in carrying out United States Government security re-
30 quirements at that airport; and

31 (2) to the extent practicable, carry out duties and powers referred
32 to in section 40953(b) of this title.

33 (c) COORDINATION OF ACTIVITIES.—The activities of each Foreign Secu-
34 rity Liaison Officer shall be coordinated with the chief of the diplomatic
35 mission of the United States to which the Officer is assigned. Activities of
36 an Officer under this section shall be consistent with the duties and powers
37 of the Secretary of State and the chief of mission to a foreign country under
38 section 103 of the Omnibus Diplomatic Security and Antiterrorism Act of
39 1986 (22 U.S.C. 4802) and section 207 of the Foreign Service Act of 1980
40 (22 U.S.C. 3927).

1 **§ 40955. Employment standards and training**

2 (a) EMPLOYMENT STANDARDS.—The Administrator shall prescribe stand-
3 ards for the employment and continued employment of, and contracting for,
4 air carrier personnel and, as appropriate, airport security personnel. The
5 standards shall include—

- 6 (1) minimum training requirements for new employees;
7 (2) retraining requirements;
8 (3) minimum staffing levels;
9 (4) minimum language skills; and
10 (5) minimum education levels for employees, when appropriate.

11 (b) REVIEW AND RECOMMENDATIONS.—In coordination with air carriers,
12 airport operators, and other interested persons, the Administrator shall re-
13 view issues related to human performance in the aviation security system
14 to maximize that performance. When the review is completed, the Adminis-
15 trator shall recommend guidelines and prescribe appropriate changes in ex-
16 isting procedures to improve that performance.

17 (c) SECURITY PROGRAM TRAINING, STANDARDS, AND QUALIFICA-
18 TIONS.—

19 (1) IN GENERAL.—The Administrator—

20 (A) may train individuals employed to carry out a security pro-
21 gram under section 40913(c) of this title; and

22 (B) shall prescribe uniform training standards and uniform
23 minimum qualifications for individuals eligible for that training.

24 (2) REIMBURSEMENTS.—The Administrator may authorize reim-
25 bursement for travel, transportation, and subsistence expenses for secu-
26 rity training of non-United States Government domestic and foreign in-
27 dividuals whose services will contribute significantly to carrying out
28 civil aviation security programs. To the extent practicable, air travel re-
29 imbursed under this paragraph shall be on air carriers.

30 (d) EDUCATION AND TRAINING STANDARDS FOR SECURITY COORDINA-
31 TORS, SUPERVISORY PERSONNEL, AND PILOTS.—

32 (1) IN GENERAL.—The Administrator shall prescribe standards for
33 educating and training—

34 (A) ground security coordinators;

35 (B) security supervisory personnel; and

36 (C) airline pilots as in-flight security coordinators.

37 (2) ELEMENTS.—The standards shall include initial training, re-
38 training, and continuing education requirements and methods. The re-
39 quirements and methods shall be used annually to measure the per-
40 formance of ground security coordinators and security supervisory per-
41 sonnel.

1 (e) SECURITY SCREENERS.—

2 (1) TRAINING PROGRAM.—The Administrator shall establish a pro-
3 gram for the hiring and training of security screening personnel.

4 (2) HIRING.—

5 (A) QUALIFICATIONS.—The Administrator shall establish quali-
6 fication standards for individuals to be hired by the United States
7 as security screening personnel. Notwithstanding another law, the
8 standards shall require, at a minimum, an individual—

9 (i) to have a satisfactory or better score on a Federal secu-
10 rity screening personnel selection examination;

11 (ii) to be a citizen of the United States or a national of
12 the United States, as defined in section 101(a) of the Immi-
13 gration and Nationality Act (8 U.S.C. 1101(a));

14 (iii) to meet, at a minimum, the requirements set forth in
15 subsection (f);

16 (iv) to meet other qualifications the Administrator may es-
17 tablish; and

18 (v) to have the ability to demonstrate daily a fitness for
19 duty without an impairment due to illegal drugs, sleep depri-
20 vation, medication, or alcohol.

21 (B) BACKGROUND CHECKS.—The Administrator shall require
22 that an individual to be hired as a security screener undergo an
23 employment investigation (including a criminal history record
24 check) under section 40956(a)(1) of this title.

25 (C) DISQUALIFICATION OF INDIVIDUALS WHO PRESENT NA-
26 TIONAL SECURITY RISKS.—The Administrator, in consultation
27 with the heads of other appropriate Federal agencies, shall estab-
28 lish procedures, in addition to any background check conducted
29 under section 40956 of this title, to ensure that an individual who
30 presents a threat to national security is not employed as a security
31 screener.

32 (3) EXAMINATION.—The Administrator shall develop a security
33 screening personnel examination for use in determining the qualifica-
34 tion of individuals seeking employment as security screening personnel.

35 (4) REVIEW OF STANDARDS, RULES, AND REGULATIONS.—The Ad-
36 ministrator shall review, and revise as necessary, a standard, rule, or
37 regulation governing the employment of individuals as security screen-
38 ing personnel.

39 (f) EMPLOYMENT STANDARDS FOR SCREENING PERSONNEL.—

1 (1) SCREENER REQUIREMENTS.—Notwithstanding another law, an
2 individual may not be deployed as a security screener unless that indi-
3 vidual meets the following requirements:

4 (A) EDUCATION OR EXPERIENCE.—The individual possesses a
5 high school diploma, a general equivalency diploma, or experience
6 that the Administrator has determined to be sufficient for the in-
7 dividual to perform the duties of the position.

8 (B) BASIC APTITUDES AND PHYSICAL ABILITIES.—The indi-
9 vidual possesses basic aptitudes and physical abilities, including
10 color perception, visual and aural acuity, physical coordination,
11 and motor skills, to the following standards:

12 (i) Screeners operating screening equipment are able to dis-
13 tinguish on the screening equipment monitor the appropriate
14 imaging standard specified by the Administrator.

15 (ii) Screeners operating screening equipment are able to
16 distinguish each color displayed on every type of screening
17 equipment and explain what each color signifies.

18 (iii) Screeners are able to hear and respond to the spoken
19 voice and to audible alarms generated by screening equipment
20 in an active checkpoint environment.

21 (iv) Screeners performing physical searches or other related
22 operations are able to efficiently and thoroughly manipulate
23 and handle the baggage, containers, and other objects subject
24 to security processing.

25 (v) Screeners performing pat-downs or hand-held metal de-
26 tector searches of individuals have sufficient dexterity and ca-
27 pability to thoroughly conduct those procedures over an indi-
28 vidual's entire body.

29 (C) READ, WRITE, AND SPEAK ENGLISH.—The individual is able
30 to read, speak, and write English well enough to—

31 (i) carry out written and oral instructions regarding the
32 proper performance of screening duties;

33 (ii) read English language identification media, credentials,
34 airline tickets, and labels on items normally encountered in
35 the screening process;

36 (iii) provide direction to and understand and answer ques-
37 tions from English-speaking individuals undergoing screening;
38 and

39 (iv) write incident reports and statements and log entries
40 into security records in the English language.

1 (D) TRAINING.—The individual has satisfactorily completed all
2 initial, recurrent, and appropriate specialized training required by
3 the security program, except as provided in paragraph (3).

4 (2) VETERANS PREFERENCE.—The Administrator shall provide a
5 preference for the hiring of an individual as a security screener if the
6 individual is a member or former member of the armed forces and if
7 the individual is entitled, under statute, to retired, retirement, or re-
8 tainer pay on account of service as a member of the armed forces.

9 (3) EXCEPTIONS.—An individual who has not completed the training
10 required by this section may be deployed during the on-the-job portion
11 of training to perform functions if that individual—

12 (A) is closely supervised; and

13 (B) does not make independent judgments as to whether indi-
14 viduals or property may enter a sterile area or aircraft without
15 further inspection.

16 (4) REMEDIAL TRAINING.—No individual employed as a security
17 screener may perform a screening function after that individual has
18 failed an operational test related to that function until that individual
19 has successfully completed the remedial training specified in the secu-
20 rity program.

21 (5) ANNUAL PROFICIENCY REVIEW.—The Administrator shall pro-
22 vide that an annual evaluation of each individual assigned screening
23 duties is conducted and documented. An individual employed as a secu-
24 rity screener may not continue to be employed in that capacity unless
25 the evaluation demonstrates that the individual—

26 (A) continues to meet all qualifications and standards required
27 to perform a screening function;

28 (B) has a satisfactory record of performance and attention to
29 duty based on the standards and requirements in the security pro-
30 gram; and

31 (C) demonstrates the current knowledge and skills necessary to
32 courteously, vigilantly, and effectively perform screening functions.

33 (6) OPERATIONAL TESTING.—In addition to the annual proficiency
34 review conducted under paragraph (5), the Administrator shall provide
35 for the operational testing of personnel.

36 (g) TRAINING.—

37 (1) USE OF OTHER AGENCIES.—The Administrator may enter into
38 a memorandum of understanding or other arrangement with another
39 Federal agency or department with appropriate law enforcement re-
40 sponsibilities, to provide personnel, resources, or other forms of assist-
41 ance in the training of security screening personnel.

1 (2) TRAINING PLAN.—The Administrator shall develop a plan for the
2 training of security screening personnel. The plan shall require, at a
3 minimum, that a security screener—

4 (A) has completed 40 hours of classroom instruction or success-
5 fully completed a program that the Administrator determines will
6 train individuals to a level of proficiency equivalent to the level
7 that would be achieved by the classroom instruction;

8 (B) has completed 60 hours of on-the-job instructions; and

9 (C) has successfully completed an on-the-job training examina-
10 tion prescribed by the Administrator.

11 (3) EQUIPMENT-SPECIFIC TRAINING.—An individual employed as a
12 security screener may not use a security screening device or equipment
13 in the scope of that individual's employment unless the individual has
14 been trained on that device or equipment and has successfully com-
15 pleted a test on the use of the device or equipment.

16 (h) TECHNOLOGICAL TRAINING.—

17 (1) DEFINITION OF DUAL-USE ITEM.—In this subsection, the term
18 “dual-use item” means an item that may seem harmless but that may
19 be used as a weapon.

20 (2) IN GENERAL.—The Administrator shall require training to en-
21 sure that screeners are proficient in using the most up-to-date new
22 technology and to ensure their proficiency in recognizing new threats
23 and weapons.

24 (3) PERIODIC ASSESSMENTS.—The Administrator shall make peri-
25 odic assessments to determine if there are dual-use items and inform
26 security screening personnel of the existence of the items.

27 (4) CURRENT LISTS OF DUAL-USE ITEMS.—Current lists of dual-use
28 items shall be part of the ongoing training for screeners.

29 (i) LIMITATION ON RIGHT TO STRIKE.—An individual who screens pas-
30 sengers or property, or both, at an airport under this section may not par-
31 ticipate in a strike, or assert the right to strike, against the person (includ-
32 ing a governmental entity) employing the individual to perform the screen-
33 ing.

34 (j) UNIFORMS.—The Administrator shall require an individual who
35 screens passengers and property under section 40911 of this title to be at-
36 tired while on duty in a uniform approved by the Administrator.

37 (k) ACCESSIBILITY OF COMPUTER-BASED TRAINING FACILITIES.—The
38 Administrator shall work with air carriers and airports to ensure that com-
39 puter-based training facilities intended for use by security screeners at an
40 airport regularly serving an air carrier holding a certificate issued by the

1 Secretary of Transportation are conveniently located for that airport and
2 easily accessible.

3 (l) INITIAL AND RECURRING TRAINING.—

4 (1) INITIAL TRAINING.—The Administrator shall establish a training
5 program for new security screening personnel located at the Transpor-
6 tation Security Administration Academy.

7 (2) RECURRING TRAINING.—

8 (A) IN GENERAL.—Not later than 180 days after October 5,
9 2018, the Administrator shall establish recurring training for se-
10 curity screening personnel regarding updates to screening proce-
11 dures and technologies, including, in response to weaknesses iden-
12 tified in covert tests at airports—

13 (i) methods to identify the verification of false or fraudu-
14 lent travel documents; and

15 (ii) training on emerging threats.

16 (B) CONTENTS.—The training under subparagraph (A) shall in-
17 clude—

18 (i) internal controls for monitoring and documenting com-
19 pliance of transportation security officers with the training
20 requirements; and

21 (ii) such other matters as are identified by the Adminis-
22 trator with regard to the training.

23 **§ 40956. Employment investigations and restrictions**

24 (a) EMPLOYMENT INVESTIGATION REQUIREMENT.—

25 (1) IN GENERAL.—

26 (A) EMPLOYEE COVERAGE.—The Administrator shall require by
27 regulation that an employment investigation, including a criminal
28 history record check and a review of available law enforcement
29 data bases and records of other governmental and international
30 agencies, to the extent determined practicable by the Adminis-
31 trator, shall be conducted of each individual employed in, or apply-
32 ing for, a position as a security screener under section 40955(e)
33 of this title or a position in which the individual has unescorted
34 access, or may permit other individuals to have unescorted access,
35 to—

36 (i) aircraft of an air carrier or foreign air carrier; or

37 (ii) a secured area of an airport in the United States the
38 Administrator designates that serves an air carrier or foreign
39 air carrier.

40 (B) FURTHER COVERAGE.—The Administrator shall require by
41 regulation that an employment investigation (including a criminal

1 history record check and a review of available law enforcement
2 data bases and records of other governmental and international
3 agencies, to the extent determined practicable by the Adminis-
4 trator) be conducted for—

5 (i) individuals who are responsible for screening passengers
6 or property under section 40911 of this title;

7 (ii) supervisors of the individuals described in clause (i);

8 (iii) individuals who regularly have escorted access to air-
9 craft of an air carrier or foreign air carrier or a secured area
10 of an airport in the United States the Administrator des-
11 ignates that serves an air carrier or foreign air carrier; and

12 (iv) other individuals who exercise security functions associ-
13 ated with baggage or cargo that the Administrator determines
14 is necessary to ensure air transportation security.

15 (C) EXEMPTION.—An employment investigation, including a
16 criminal history record check, is not required under this subsection
17 for an individual who is exempted under section 107.31(m)(1) or
18 (2) of title 14, Code of Federal Regulations, as in effect on No-
19 vember 22, 2000. The Administrator shall work with the Inter-
20 national Civil Aviation Organization and with appropriate authori-
21 ties of foreign countries to ensure that individuals exempted under
22 this subparagraph do not pose a threat to aviation or national se-
23 curity.

24 (2) EMPLOYER ROLE.—An air carrier, foreign air carrier, airport op-
25 erator, or government that employs, or authorizes or makes a contract
26 for the services of, an individual in a position described in paragraph
27 (1) shall ensure that the investigation the Administrator requires is
28 conducted.

29 (3) PERIODIC AUDITS.—The Administrator shall provide for the peri-
30 odic audit of the effectiveness of criminal history record checks con-
31 ducted under paragraph (1).

32 (b) PROHIBITED EMPLOYMENT.—

33 (1) IN GENERAL.—Except as provided in paragraph (3), an air car-
34 rier, foreign air carrier, airport operator, or government may not em-
35 ploy, or authorize or make a contract for the services of, an individual
36 in a position described in subsection (a)(1) if—

37 (A) the investigation of the individual required under this sec-
38 tion has not been conducted; or

39 (B) the results of that investigation establish that, in the 10-
40 year period ending on the date of the investigation, the individual
41 was convicted (or found not guilty by reason of insanity) of—

- 1 (i) a crime referred to in section 41044 of this title, section
2 32 of title 18, or section 46306, 46308, 46312, or 46315, or
3 chapter 465, of title 49;
- 4 (ii) murder;
- 5 (iii) assault with intent to murder;
- 6 (iv) espionage;
- 7 (v) sedition;
- 8 (vi) treason;
- 9 (vii) rape;
- 10 (viii) kidnapping;
- 11 (ix) unlawful possession, sale, distribution, or manufacture
12 of an explosive or weapon;
- 13 (x) extortion;
- 14 (xi) armed or felony unarmed robbery;
- 15 (xii) distribution of, or intent to distribute, a controlled
16 substance;
- 17 (xiii) a felony involving a threat;
- 18 (xiv) a felony involving—
- 19 (I) willful destruction of property;
- 20 (II) importation or manufacture of a controlled sub-
21 stance;
- 22 (III) burglary;
- 23 (IV) theft;
- 24 (V) dishonesty, fraud, or misrepresentation;
- 25 (VI) possession or distribution of stolen property;
- 26 (VII) aggravated assault;
- 27 (VIII) bribery; and
- 28 (IX) illegal possession of a controlled substance pun-
29 ishable by a maximum term of imprisonment of more
30 than 1 year, or another crime classified as a felony that
31 the Administrator determines indicates a propensity for
32 placing contraband aboard an aircraft in return for
33 money; or
- 34 (xv) conspiracy to commit any of the acts referred to in
35 clauses (i) through (xiv).
- 36 (2) OTHER FACTORS.—The Administrator may specify other factors
37 that are sufficient to prohibit the employment of an individual in a po-
38 sition described in subsection (a)(1).
- 39 (3) ALTERNATE SECURITY ARRANGEMENTS.—An air carrier, foreign
40 air carrier, airport operator, or government may employ, or authorize
41 or contract for the services of, an individual in a position described in

1 subsection (a)(1) without carrying out the investigation required under
2 this section, if the Administrator approves a plan to employ the indi-
3 vidual that provides alternate security arrangements.

4 (c) FINGERPRINTING AND RECORD CHECK INFORMATION.—

5 (1) IN GENERAL.—If the Administrator requires an identification
6 and criminal history record check, to be conducted by the Attorney
7 General, as part of an investigation under this section, the Adminis-
8 trator shall designate an individual to obtain fingerprints and submit
9 those fingerprints to the Attorney General. The Attorney General may
10 make the results of a check available to an individual the Administrator
11 designates. Before designating an individual to obtain and submit fin-
12 gerprints or receive results of a check, the Administrator shall consult
13 with the Attorney General. All Federal agencies shall cooperate with
14 the Administrator and the Administrator's designee in the process of
15 collecting and submitting fingerprints.

16 (2) REGULATIONS.—The Administrator shall prescribe regulations
17 on—

18 (A) procedures for taking fingerprints; and

19 (B) requirements for using information received from the Attor-
20 ney General under paragraph (1)—

21 (i) to limit the dissemination of the information; and

22 (ii) to ensure that the information is used only to carry out
23 this section.

24 (3) ACCESS TO INVESTIGATION.—If an identification and criminal
25 history record check is conducted as part of an investigation of an indi-
26 vidual under this section, the individual—

27 (A) shall receive a copy of a record received from the Attorney
28 General; and

29 (B) may complete and correct the information contained in the
30 check before a final employment decision is made based on the
31 check.

32 (d) FEES AND CHARGES.—The Administrator and the Attorney General
33 shall establish reasonable fees and charges to pay expenses incurred in car-
34 rying out this section. The employer of the individual being investigated
35 shall pay the costs of a record check of the individual. Money collected
36 under this section shall be credited to the account in the Treasury from
37 which the expenses were incurred and shall be available to the Adminis-
38 trator and the Attorney General for those expenses.

39 (e) WHEN INVESTIGATION OR RECORD CHECK NOT REQUIRED.—This
40 section does not require an investigation or record check when the investiga-
41 tion or record check is prohibited by a law of a foreign country.

1 **§ 40957. Prohibition on transferring duties and powers**

2 Except as specifically provided by law, the Administrator may not trans-
3 fer a duty or power under section 40913(a), (b), (c), or (e), 40916,
4 40922(a) through (c), 40955, 40956, or 40958(b)(2) of this title.

5 **§ 40958. Reports**

6 (a) TRANSPORTATION SECURITY.—Not later than March 31 of each year,
7 the Secretary shall submit to Congress a report on transportation security
8 with recommendations the Secretary considers appropriate. The report shall
9 be prepared in conjunction with the biennial report the Administrator sub-
10 mits under subsection (b) in each year the Administrator submits the bi-
11 ennial report, but may not duplicate the information submitted under sub-
12 section (b) or section 40917(a)(3) of this title. The Secretary may submit
13 the report in classified and unclassified parts. The report shall include—

14 (1) an assessment of trends and developments in terrorist activities,
15 methods, and other threats to transportation;

16 (2) an evaluation of deployment of explosive detection devices;

17 (3) recommendations for research, engineering, and development ac-
18 tivities related to transportation security, except research engineering
19 and development activities related to aviation security to the extent
20 those activities are covered by the national aviation research plan re-
21 quired under section 44501(c) of title 49;

22 (4) identification and evaluation of cooperative efforts with other de-
23 partments, agencies, and instrumentalities of the United States Gov-
24 ernment;

25 (5) an evaluation of cooperation with foreign transportation and se-
26 curity authorities;

27 (6) the status of the extent to which the recommendations of the
28 President's Commission on Aviation Security and Terrorism have been
29 carried out and the reasons for delay in carrying out those rec-
30 ommendations;

31 (7) an assessment of financial and staffing requirements, and the at-
32 tainment of existing staffing goals, for carrying out the duties and pow-
33 ers of the Administrator relating to security; and

34 (8) appropriate legislative and regulatory recommendations.

35 (b) SCREENING AND FOREIGN AIR CARRIER AND AIRPORT SECURITY.—
36 The Administrator shall submit biennially to Congress a report on the effec-
37 tiveness of procedures under section 40911 (except subsection (e)) of this
38 title that includes—

39 (1) a summary of the assessments conducted under section
40 40917(a)(1) and (2) of this title; and

1 (2) an assessment of the steps being taken, and the progress being
2 made, in ensuring compliance with section 40916 of this title for each
3 foreign air carrier security program at airports outside the United
4 States—

5 (A) at which the Administrator decides that Foreign Security
6 Liaison Officers are necessary for air transportation security; and

7 (B) for which extraordinary security measures are in place.

8 **§ 40959. Training to operate certain aircraft**

9 (a) WAITING PERIOD.—

10 (1) DEFINITION OF TRAINING.—In this subsection, the term “train-
11 ing”—

12 (A) means training received from an instructor in an aircraft
13 or aircraft simulator; but

14 (B) does not include recurrent training, ground training, or
15 demonstration flights for marketing purposes.

16 (2) REQUIREMENTS.—A person operating as a flight instructor, pilot
17 school, or aviation training center or subject to regulation under part
18 A of subtitle VII of title 49 may provide training in the operation of
19 an aircraft having a maximum certificated takeoff weight of more than
20 12,500 pounds to an alien (as defined in section 101(a) of the Immi-
21 gration and Nationality Act (8 U.S.C. 1101(a))) or to another indi-
22 vidual specified by the Secretary only if—

23 (A) that person has first notified the Secretary that the alien
24 or individual has requested training and submitted to the Sec-
25 retary, in the form the Secretary prescribes, the following informa-
26 tion about the alien or individual:

27 (i) Full name, including aliases used by the applicant or
28 variations in spelling of the applicant’s name.

29 (ii) Passport and visa information.

30 (iii) Country of citizenship.

31 (iv) Date of birth.

32 (v) Dates of training.

33 (vi) Fingerprints collected by, or under the supervision of,
34 a Federal, State, or local law enforcement agency or by an-
35 other entity approved by the Federal Bureau of Investigation
36 or the Secretary, including fingerprints taken by United
37 States Government personnel at a United States embassy or
38 consulate; and

39 (B) the Secretary has not directed, within 30 days after being
40 notified under subparagraph (A), that person not to provide the

1 requested training because the Secretary has determined that the
2 individual presents a risk to aviation or national security.

3 (b) INTERRUPTION OF TRAINING.—If the Secretary, more than 30 days
4 after receiving notification under subsection (a) from a person providing
5 training described in subsection (a), determines that the individual presents
6 a risk to aviation or national security, the Secretary shall immediately notify
7 the person providing the training of the determination, and that person
8 shall immediately terminate the training.

9 (c) NOTIFICATION.—A person operating as a flight instructor, pilot
10 school, or aviation training center or subject to regulation under part A of
11 subtitle VII of title 49 may provide training in the operation of an aircraft
12 having a maximum certificated takeoff weight of 12,500 pounds or less to
13 an alien (as defined in section 101(a) of the Immigration and Nationality
14 Act (8 U.S.C. 1101(a)) or to another individual specified by the Secretary
15 only if that person has notified the Secretary that the individual has re-
16 quested the training and furnished the Secretary with that individual's iden-
17 tification in the form the Secretary requires.

18 (d) EXPEDITED PROCESSING.—The Secretary shall establish a process to
19 ensure that the waiting period under subsection (a) shall not exceed 5 days
20 for an alien (as defined in section 101(a) of the Immigration and Nation-
21 ality Act (8 U.S.C. 1101(a))) who—

22 (1) holds an airman's certification of a foreign country that is recog-
23 nized by an agency of the United States, including a military agency,
24 that permits an individual to operate a multi-engine aircraft that has
25 a certificated takeoff weight of more than 12,500 pounds;

26 (2) is employed by a foreign air carrier that is certified under part
27 129 of title 14, Code of Federal Regulations, and that has a security
28 program approved under part 1546 of title 49, Code of Federal Regula-
29 tions;

30 (3) is an individual who has unescorted access to a secured area of
31 an airport designated under section 40956(a)(1)(A)(ii) of this title; or

32 (4) is an individual who is part of a class of individuals that the Sec-
33 retary has determined that providing aviation training to presents mini-
34 mal risk to aviation or national security because of the aviation train-
35 ing already possessed by the class of individuals.

36 (e) NONAPPLICABILITY TO CERTAIN FOREIGN MILITARY PILOTS.—The
37 procedures and processes required by subsections (a) through (d) do not
38 apply to a foreign military pilot endorsed by the Department of Defense for
39 flight training in the United States and seeking training described in sub-
40 section (a)(1) in the United States.

41 (f) FEE.—

1 (1) IN GENERAL.—The Secretary may assess a fee for an investiga-
2 tion under this section. The Secretary may adjust the maximum
3 amount of the fee to reflect the costs of an investigation.

4 (2) OFFSET.—Notwithstanding section 3302 of title 31, a fee col-
5 lected under this section—

6 (A) shall be credited to the account in the Treasury from which
7 the expenses were incurred and shall be available to the Secretary
8 for those expenses; and

9 (B) shall remain available until expended.

10 (g) INTERAGENCY COOPERATION.—The Attorney General, the Director of
11 National Intelligence, and the Administrator of the Federal Aviation Admin-
12 istration shall cooperate with the Secretary in implementing this section.

13 (h) SECURITY AWARENESS TRAINING FOR EMPLOYEES.—The Secretary
14 shall require flight schools to conduct a security awareness program for
15 flight school employees to increase their awareness of suspicious cir-
16 cumstances and activities of individuals enrolling in or attending flight
17 school.

18 **§ 40960. Security service fee**

19 (a) GENERAL AUTHORITY.—

20 (1) PASSENGER FEES.—The Administrator shall impose a uniform
21 fee, on passengers of air carriers and foreign air carriers in air trans-
22 portation and intrastate air transportation originating at airports in
23 the United States, to pay for the following costs of providing civil avia-
24 tion security services:

25 (A) Salary, benefits, overtime, retirement and other costs of
26 screening personnel, their supervisors and managers, Federal law
27 enforcement personnel, and State and local law enforcement offi-
28 cers deputized under section 40933 of this title, who are deployed
29 at airport security screening locations under section 40911 (except
30 subsection (e)) of this title.

31 (B) The costs of training personnel described in subparagraph
32 (A), and the acquisition, operation, and maintenance of equipment
33 used by the personnel.

34 (C) The costs of performing background investigations of per-
35 sonnel described in subparagraphs (A), (D), (F), and (G).

36 (D) The costs of the Federal air marshals program.

37 (E) The costs of performing civil aviation security research and
38 development under this title.

39 (F) The costs of Federal Security Directors under section
40 40913 of this title.

1 (G) The costs of deploying Federal law enforcement personnel
2 under section 40913(h) of this title.

3 (H) The costs of security-related capital improvements at air-
4 ports.

5 (I) The costs of training pilots and flight attendants under sec-
6 tions 40928 and 40932 of this title.

7 (2) DETERMINATION OF COSTS.—The amount of the costs listed in
8 paragraph (1) shall be determined by the Administrator and are not
9 subject to judicial review

10 (b) SCHEDULE OF FEES.—In imposing fees under subsection (a), the Ad-
11 ministrator shall ensure that the fees are reasonably related to the Trans-
12 portation Security Administration’s costs of providing services rendered.

13 (c) LIMITATION ON FEE.—

14 (1) DEFINITION OF ROUND TRIP.—In this subsection, “round trip”
15 means a trip on an air travel itinerary that terminates or has a stop-
16 over at the origin point (or co-terminal).

17 (2) LIMITATION.—The fee imposed under subsection (a) is \$5.60 per
18 one-way trip in air transportation or intrastate air transportation that
19 originates at an airport in the United States, except the fee imposed
20 per round trip shall not exceed \$11.20.

21 (3) OFFSETTING COLLECTIONS.—Beginning on October 21, 2027,
22 fees collected under subsection (a)(1) for a fiscal year shall be credited
23 as offsetting collections to appropriations made for aviation security
24 measures carried out by the Transportation Security Administration
25 and shall remain available until expended.

26 (d) IMPOSITION OF FEE.—

27 (1) IN GENERAL.—Notwithstanding section 9701 of title 31 and the
28 procedural requirements of section 553 of title 5, the Administrator
29 shall impose the fee under subsection (a) through the publication of no-
30 tice of the fee in the Federal Register and begin collection of the fee
31 as soon as possible.

32 (2) SPECIAL RULES FOR PASSENGER FEES.—A fee imposed under
33 subsection (a) through the procedures under paragraph (1) shall apply
34 only to tickets sold after the date on which the fee is imposed. If a
35 fee imposed under subsection (a) through the procedures under para-
36 graph (1) on transportation of a passenger of a carrier described in
37 subsection (a) is not collected from the passenger, the amount of the
38 fee shall be paid by the carrier.

39 (3) SUBSEQUENT MODIFICATION OF FEE.—After imposing a fee
40 under paragraph (1), the Administrator may modify, from time to time

1 through publication of notice in the Federal Register, the imposition
2 or collection of the fee, or both.

3 (4) LIMITATION ON COLLECTION.—A fee may be collected under this
4 section, other than subsection (i), only to the extent that the expendi-
5 ture of the fee to pay the costs of activities and services for which the
6 fee is imposed is provided for in advance in an appropriations Act or
7 in section 40934 of this title.

8 (e) ADMINISTRATION OF FEES.—

9 (1) FEES PAYABLE TO ADMINISTRATOR.—All fees imposed and
10 amounts collected under this section are payable to the Administrator.

11 (2) FEES COLLECTED BY AIR CARRIER.—A fee imposed under sub-
12 section (a)(1) shall be collected by the air carrier or foreign air carrier
13 that sells a ticket for transportation described in subsection (a).

14 (3) DUE DATE FOR REMITTANCE.—A fee collected under this section
15 shall be remitted on the last day of each calendar month by the carrier
16 collecting the fee. The amount to be remitted shall be for the calendar
17 month preceding the calendar month in which the remittance is made.

18 (4) INFORMATION.—The Administrator may require the provision of
19 information the Administrator decides is necessary to verify that fees
20 have been collected and remitted at the proper times and in the proper
21 amounts.

22 (5) FEE NOT SUBJECT TO TAX.—For purposes of section 4261 of
23 the Internal Revenue Code of 1986 (26 U.S.C. 4261), a fee imposed
24 under this section is not considered to be part of the amount paid for
25 taxable transportation.

26 (6) COST OF COLLECTING FEE.—No portion of the fee collected
27 under this section may be retained by the air carrier or foreign air car-
28 rier for the costs of collecting, handling, or remitting the fee, except
29 for interest accruing to the carrier after collection and before remit-
30 tance.

31 (f) RECEIPTS CREDITED AS OFFSETTING COLLECTIONS.—Notwith-
32 standing section 3302 of title 31, a fee collected under this section—

33 (1) shall be credited as offsetting collections to the account that fi-
34 nances the activities and services for which the fee is imposed;

35 (2) shall be available for expenditure only to pay the costs of activi-
36 ties and services for which the fee is imposed; and

37 (3) shall remain available until expended.

38 (g) REFUNDS.—The Administrator may refund a fee paid by mistake or
39 an amount paid in excess of that required.

40 (h) EXEMPTIONS.—The Administrator may exempt from the passenger
41 fee imposed under subsection (a) a passenger enplaning at an airport in the

1 United States that does not receive screening services under section 40911
2 of this title for that segment of the trip for which the passenger does not
3 receive screening.

4 (i) DEPOSIT OF RECEIPTS.—

5 (1) IN GENERAL.—Out of fees received in a fiscal year under sub-
6 section (a), after amounts are made available in the fiscal year under
7 section 40934(h) of this title, the next funds derived from the fees in
8 the fiscal year, in the amount specified for the fiscal year in paragraph
9 (4), shall be credited as offsetting receipts and deposited in the general
10 fund of the Treasury.

11 (2) FEE LEVELS.—The Secretary shall impose the fee authorized by
12 subsection (a) so as to collect in a fiscal year at least the amount speci-
13 fied in paragraph (4) for the fiscal year for making deposits under
14 paragraph (1).

15 (3) RELATIONSHIP TO OTHER PROVISIONS.—Subsections (b) and (f)
16 do not apply to amounts to be used for making deposits under this sub-
17 section.

18 (4) FISCAL YEAR AMOUNTS.—For purposes of paragraphs (1) and
19 (2), the fiscal year amounts are as follows:

20 (A) \$1,520,000,000 for fiscal year 2023.

21 (B) \$1,560,000,000 for fiscal year 2024.

22 (C) \$1,600,000,000 for fiscal year 2025.

23 (D) \$1,640,000,000 for fiscal year 2026.

24 (E) \$1,680,000,000 for fiscal year 2027.

25 **§ 40961. Immunity for reporting suspicious activities**

26 (a) IN GENERAL.—An air carrier or foreign air carrier or an employee
27 of an air carrier or foreign air carrier who makes a voluntary disclosure of
28 a suspicious transaction relevant to a possible violation of law or regulation,
29 relating to air piracy, a threat to aircraft or passenger safety, or terrorism,
30 as defined in section 3077 of title 18, to an employee or agent of the De-
31 partment, the Department of Transportation, the Department of Justice, a
32 Federal, State, or local law enforcement officer, or an airport or airline se-
33 curity officer shall not be civilly liable to any person under a law or regula-
34 tion of the United States, or a constitution, law, or regulation of a State
35 or political subdivision of a State, for the disclosure.

36 (b) APPLICATION.—Subsection (a) does not apply to—

37 (1) a disclosure made with actual knowledge that the disclosure was
38 false, inaccurate, or misleading; or

39 (2) a disclosure made with reckless disregard as to the truth or fal-
40 sity of that disclosure.

1 **§ 40962. Performance goals and objectives**

2 (a) SHORT-TERM TRANSITION.—

3 (1) IN GENERAL.—The Administrator, in consultation with other rel-
4 evant Federal agencies and Congress, may—

5 (A) establish acceptable levels of performance for aviation secu-
6 rity, including screening operations and access control; and

7 (B) provide Congress with an action plan, containing measur-
8 able goals and milestones, that outlines how those levels of per-
9 formance will be achieved.

10 (2) BASICS OF ACTION PLAN.—The action plan shall clarify the re-
11 sponsibilities of the Transportation Security Administration, the Fed-
12 eral Aviation Administration, and any other agency or organization
13 that may have a role in ensuring the safety and security of the civil
14 air transportation system.

15 (b) LONG-TERM RESULTS-BASED MANAGEMENT.—

16 (1) PERFORMANCE PLAN.—

17 (A) IN GENERAL.—Each year, consistent with the requirements
18 of the Government Performance and Results Act of 1993 (in this
19 section referred to as “GPRA”) (Public Law 103–62, 107 Stat.
20 285), the Secretary and the Administrator shall agree on a per-
21 formance plan for the succeeding 5 years that establishes measur-
22 able goals and objectives for aviation security. The plan shall iden-
23 tify action steps necessary to achieve the goals.

24 (B) CLARIFICATION OF RESPONSIBILITIES.—In addition to
25 meeting the requirements of GPRA, the performance plan should
26 clarify the responsibilities of the Secretary, the Administrator, and
27 any other agency or organization that may have a role in ensuring
28 the safety and security of the civil air transportation system.

29 (C) ANNUAL PERFORMANCE REPORT.—Each year, consistent
30 with the requirements of GPRA, the Administrator shall prepare
31 and submit to Congress an annual report, including an evaluation
32 of the extent to which goals and objectives were met. The report
33 shall include the results achieved during the year relative to the
34 goals established in the performance plan.

35 **§ 40963. Aviation Security Advisory Committee**

36 (a) DEFINITIONS.—In this section:

37 (1) ADVISORY COMMITTEE.—The term “Advisory Committee” means
38 the aviation security advisory committee established under subsection

39 (b).

40 (2) PERIMETER SECURITY.—The term “perimeter security”—

1 (A) means procedures or systems to monitor, secure, and pre-
2 vent unauthorized access to an airport, including its airfield and
3 terminal; and

4 (B) includes the fence area surrounding an airport, access
5 gates, and access controls.

6 (b) ESTABLISHMENT.—The Administrator shall establish in the Trans-
7 portation Security Administration an aviation security advisory committee.

8 (c) DUTIES.—

9 (1) IN GENERAL.—The Administrator shall consult the Advisory
10 Committee, as appropriate, on aviation security matters, including on
11 the development, refinement, and implementation of policies, programs,
12 rulemaking, and security directives pertaining to aviation security,
13 while adhering to sensitive security guidelines.

14 (2) RECOMMENDATIONS.—

15 (A) IN GENERAL.—At the request of the Administrator, the Ad-
16 visory Committee shall develop recommendations for improvements
17 to aviation security.

18 (B) RECOMMENDATIONS OF SUBCOMMITTEES.—Recommendations
19 agreed on by the subcommittees established under this section
20 shall be approved by the Advisory Committee before trans-
21 mission to the Administrator.

22 (3) PERIODIC REPORTS.—The Advisory Committee shall periodically
23 submit to the Administrator—

24 (A) reports on matters identified by the Administrator; and

25 (B) reports on other matters identified by a majority of the
26 members of the Advisory Committee.

27 (4) ANNUAL REPORT.—The Advisory Committee shall submit to the
28 Administrator an annual report providing information on the activities,
29 findings, and recommendations of the Advisory Committee, including
30 its subcommittees, for the preceding year. Not later than 6 months
31 after the date that the Administrator receives the annual report, the
32 Administrator shall publish a public version describing the Advisory
33 Committee's activities and such related matters as would be inform-
34 ative to the public consistent with the policy of section 552(b) of title
35 5.

36 (5) FEEDBACK.—Not later than 90 days after receiving recom-
37 mendations transmitted by the Advisory Committee under para-
38 graph (4), the Administrator shall respond in writing to the Advisory
39 Committee with feedback on each of the recommendations, an action
40 plan to implement any of the recommendations with which the Admin-

1 istrator concurs, and a justification for why any of the recommenda-
2 tions have been rejected.

3 (6) CONGRESSIONAL NOTIFICATION.—Not later than 30 days after
4 providing written feedback to the Advisory Committee under paragraph
5 (5), the Administrator shall notify the Committee on Commerce,
6 Science, and Transportation of the Senate and the Committee on
7 Homeland Security of the House of Representatives on the feedback,
8 and provide a briefing on request.

9 (7) REPORT TO CONGRESS.—Prior to briefing the Committee on
10 Commerce, Science, and Transportation of the Senate and the Com-
11 mittee on Homeland Security of the House of Representatives under
12 paragraph (6), the Administrator shall submit to the committees a re-
13 port containing information relating to the recommendations trans-
14 mitted by the Advisory Committee in accordance with paragraph (4).

15 (d) MEMBERSHIP.—

16 (1) IN GENERAL.—

17 (A) APPOINTMENT.—The Administrator shall appoint the mem-
18 bers of the Advisory Committee.

19 (B) COMPOSITION.—The Advisory Committee consists of indi-
20 viduals representing not more than 34 member organizations.
21 Each organization shall be represented by 1 individual (or the in-
22 dividual's designee).

23 (C) REPRESENTATION.—The membership of the Advisory Com-
24 mittee shall include representatives of—

25 (i) air carriers;

26 (ii) all-cargo air transportation;

27 (iii) indirect air carriers;

28 (iv) labor organizations representing air carrier employees;

29 (v) labor organizations representing transportation security
30 officers;

31 (vi) aircraft manufacturers;

32 (vii) airport operators;

33 (viii) airport construction and maintenance contractors;

34 (ix) labor organizations representing employees of airport
35 construction and maintenance contractors;

36 (x) general aviation;

37 (xi) privacy organizations;

38 (xii) the travel industry;

39 (xiii) airport-based businesses (including minority-owned
40 small businesses);

- 1 (xiv) businesses that conduct security screening operations
2 at airports;
3 (xv) aeronautical repair stations;
4 (xvi) passenger advocacy groups;
5 (xvii) the aviation security technology industry (including
6 screening technology and biometrics);
7 (xviii) victims of terrorist acts against aviation; and
8 (xix) law enforcement and security experts.

9 (2) TERM OF OFFICE.—

10 (A) IN GENERAL.—The term of each member of the Advisory
11 Committee shall be 2 years.

12 (B) REAPPOINTMENT.—A member of the Advisory Committee
13 may be reappointed.

14 (C) REMOVAL.—The Administrator may review the participation
15 of a member of the Advisory Committee and remove the member
16 for cause at any time.

17 (3) PROHIBITION ON COMPENSATION.—The members of the Advisory
18 Committee shall not receive pay, allowances, or benefits from the Gov-
19 ernment by reason of their service on the Advisory Committee.

20 (4) MEETINGS.—

21 (A) IN GENERAL.—The Administrator shall require the Advi-
22 sory Committee to meet at least semiannually and may convene
23 additional meetings as necessary.

24 (B) PUBLIC MEETINGS.—At least 1 of the meetings described
25 in subparagraph (A) shall be open to the public.

26 (C) ATTENDANCE.—The Advisory Committee shall maintain a
27 record of the individuals present at each meeting.

28 (5) MEMBER ACCESS TO SENSITIVE SECURITY INFORMATION.—Not
29 later than 60 days after the date of a member's appointment, the Ad-
30 ministrator shall determine if there is cause for the member to be re-
31 stricted from possessing sensitive security information. Without that
32 cause, and on the member's voluntarily signing a non-disclosure agree-
33 ment, the member may be granted access to sensitive security informa-
34 tion that is relevant to the member's advisory duties. The member shall
35 protect the sensitive security information in accordance with part 1520
36 of title 49, Code of Federal Regulations.

37 (6) CHAIR.—A stakeholder representative on the Advisory Com-
38 mittee who is elected by the appointed membership of the Advisory
39 Committee shall chair the Advisory Committee.

40 (e) SUBCOMMITTEES.—

1 (1) MEMBERSHIP.—The Advisory Committee chairperson, in coordi-
2 nation with the Administrator, may establish in the Advisory Com-
3 mittee any subcommittee that the Administrator and Advisory Com-
4 mittee determine to be necessary. The Administrator and the Advisory
5 Committee shall create subcommittees to address aviation security
6 issues, including the following:

7 (A) The implementation of the air cargo security programs es-
8 tablished by the Transportation Security Administration to screen
9 air cargo on passenger aircraft and all-cargo aircraft in accordance
10 with established cargo screening mandates.

11 (B) General aviation facilities, general aviation aircraft, and heli-
12 copter operations at general aviation and commercial service air-
13 ports.

14 (C) Recommendations on airport perimeter security, exit lane
15 security, and technology at commercial service airports, and access
16 control issues.

17 (D) Security technology standards and requirements, including
18 their harmonization internationally, technology to screen pas-
19 sengers, passenger baggage, carry-on baggage, and cargo, and bio-
20 metric technology.

21 (2) CONSIDERATION OF RISK-BASED SECURITY.—All subcommittees
22 established by the Advisory Committee chairperson in coordination with
23 the Administrator shall consider risk-based security approaches in the
24 performance of their functions that weigh the optimum balance of costs
25 and benefits in transportation security, including for passenger screen-
26 ing, baggage screening, air cargo security policies, and general aviation
27 security matters.

28 (3) MEETINGS AND REPORTING.—Each subcommittee shall meet at
29 least quarterly and submit to the Advisory Committee for inclusion in
30 the annual report required under subsection (c)(4) information, includ-
31 ing recommendations, regarding issues in the subcommittee.

32 (4) CO-CHAIRS.—Each subcommittee shall be co-chaired by a Gov-
33 ernment official and an industry official.

34 (5) SUBJECT MATTER EXPERTS.—Each subcommittee shall include
35 subject matter experts with relevant expertise who are appointed by its
36 co-chairs.

37 (f) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of title
38 5 shall not apply to the Advisory Committee and its subcommittees.

39 **SEC. 4. CONFORMING AMENDMENTS.**

40 (a) TITLE 6, UNITED STATES CODE.—Chapter 409 of title 6, United
41 States Code, as enacted by section 3, is amended as follows:

1 (1) By inserting after section 40963 the following:

2 **“§ 40964. General authority**

3 “The Administrator may take action the Administrator considers nec-
4 essary to carry out this chapter, including conducting investigations, pre-
5 scribing regulations, standards, and procedures, and issuing orders.

6 **“§ 40965. Withholding information**

7 “(a) OBJECTIONS TO DISCLOSURE.—A person may object to the public
8 disclosure of information in a record filed under this chapter. An objection
9 must be in writing and must state the reasons for the objection.

10 “(b) WITHHOLDING INFORMATION FROM CONGRESS.—This section does
11 not authorize information to be withheld from a committee of Congress au-
12 thorized to have the information.

13 **“Subchapter IV—Alcohol and Controlled**
14 **Substances Testing**

15 **“§ 40981. Definition of controlled substance**

16 “In this subchapter, the term “controlled substance” means a substance
17 under section 102 of the Controlled Substances Act (21 U.S.C. 802) speci-
18 fied by the Administrator.

19 **“§ 40982. Application**

20 “This subchapter applies to—

21 “(1) programs relating to testing of airport security screening per-
22 sonnel; and

23 “(2) employees of the Transportation Security Administration whose
24 duties include responsibility for security-sensitive functions.

25 **“§ 40983. Alcohol and controlled substances testing pro-**
26 **grams**

27 “(a) EMPLOYEES OF AIR CARRIERS AND FOREIGN AIR CARRIERS.—

28 “(1) IN GENERAL.—In the interest of aviation security, the Adminis-
29 trator shall prescribe regulations—

30 “(A) that establish a program requiring employers of airport se-
31 curity screening personnel to conduct preemployment, reasonable
32 suspicion, random, and post-accident testing of their personnel re-
33 sponsible for security-sensitive functions (as decided by the Ad-
34 ministrator) for the use of a controlled substance in violation of
35 law or a United States Government regulation; and

36 “(B) that—

37 “(i) establish a program requiring employers of airport se-
38 curity screening personnel to conduct reasonable suspicion,
39 random, and post-accident testing of their personnel respon-
40 sible for security-sensitive functions (as decided by the Ad-

1 administrator) for the use of alcohol in violation of law or a
2 United States Government regulation; and

3 “(ii) permit the employers to conduct preemployment test-
4 ing of airport security screening personnel responsible for
5 safety-sensitive functions (as decided by the Administrator)
6 for the use of alcohol.

7 “(2) RECURRING TESTING.—When the Administrator considers it
8 appropriate in the interest of security, the Administrator may prescribe
9 regulations for conducting periodic recurring testing of airport security
10 screening personnel responsible for security-sensitive functions for the
11 use of alcohol or a controlled substance in violation of law or a United
12 States Government regulation.

13 “(b) EMPLOYEES OF TRANSPORTATION SECURITY ADMINISTRATION.—

14 “(1) IN GENERAL.—The Administrator—

15 “(A) shall establish for employees of the Transportation Secu-
16 rity Administration whose duties include responsibility for secu-
17 rity-sensitive functions a program—

18 “(i) of preemployment, reasonable suspicion, random, and
19 post-accident testing for the use of a controlled substance in
20 violation of law or a United States Government regulation;
21 and

22 “(ii) of reasonable suspicion, random, and post-accident
23 testing for the use of alcohol in violation of law or a United
24 States Government regulation; and

25 “(B) may establish a program of preemployment testing for the
26 use of alcohol for employees of the Transportation Security Ad-
27 ministration whose duties include responsibility for security-sen-
28 sitive functions.

29 “(2) RECURRING TESTING.—When the Administrator considers it
30 appropriate in the interest of security, the Administrator may prescribe
31 regulations for conducting periodic recurring testing of employees of
32 the Transportation Security Administration responsible for security-
33 sensitive functions for the use of alcohol or a controlled substance in
34 violation of law or a United States Government regulation.

35 “(c) SANCTIONS.—In prescribing regulations under the programs re-
36 quired by this section, the Administrator shall require, as the Administrator
37 considers appropriate, the disqualification or dismissal of an individual
38 under this subchapter when a test conducted and confirmed under this sub-
39 chapter indicates the individual has used alcohol or a controlled substance
40 in violation of law or a United States Government regulation.

1 **“§ 40984. Prohibited service**

2 “(a) USE OF ALCOHOL OR A CONTROLLED SUBSTANCE.—An individual
3 may not use alcohol or a controlled substance after October 28, 1991, in
4 violation of law or a United States Government regulation and serve as an
5 air carrier employee responsible for security-sensitive functions (as decided
6 by the Administrator) or employee of the Transportation Security Adminis-
7 tration with responsibility for security-sensitive functions.

8 “(b) REHABILITATION REQUIRED TO RESUME SERVICE.—Notwith-
9 standing subsection (a), an individual found to have used alcohol or a con-
10 trolled substance after October 28, 1991, in violation of law or a United
11 States Government regulation may serve as an air carrier employee respon-
12 sible for security-sensitive functions (as decided by the Administrator), or
13 employee of the Transportation Security Administration with responsibility
14 for security-sensitive functions only if the individual completes a rehabilita-
15 tion program described in section 40986 of this title.

16 “(c) PERFORMANCE OF PRIOR DUTIES PROHIBITED.—An individual who
17 served as an air carrier employee responsible for security-sensitive functions
18 (as decided by the Administrator), or employee of the Transportation Secu-
19 rity Administration with responsibility for security-sensitive functions and
20 who was found by the Administrator to have used alcohol or a controlled
21 substance after October 28, 1991, in violation of law or a United States
22 Government regulation may not carry out the duties related to air transpor-
23 tation that the individual carried out before the finding of the Administrator
24 if the individual—

25 “(1) used the alcohol or controlled substance when on duty;

26 “(2) began or completed a rehabilitation program described in sec-
27 tion 40986 of this title before using the alcohol or controlled substance;
28 or

29 “(3) refuses to begin or complete a rehabilitation program described
30 in section 40986 of this title after a finding by the Administrator under
31 this section.

32 **“§ 40985. Testing and laboratory requirements**

33 “‘In carrying out section 40983 of this title, the Administrator shall de-
34 velop requirements that—

35 “(1) promote, to the maximum extent practicable, individual privacy
36 in the collection of specimens;

37 “(2) for laboratories and testing procedures for controlled sub-
38 stances, incorporate the Department of Health and Human Services
39 scientific and technical guidelines dated April 11, 1988, and any
40 amendments to those guidelines, including mandatory guidelines estab-
41 lishing—

1 “(A) comprehensive standards for every aspect of laboratory
2 controlled substances testing and laboratory procedures to be ap-
3 plied in carrying out this subchapter, including standards requir-
4 ing the use of the best available technology to ensure the complete
5 reliability and accuracy of controlled substances tests and strict
6 procedures governing the chain of custody of specimens collected
7 for controlled substances testing;

8 “(B) the minimum list of controlled substances for which indi-
9 viduals may be tested; and

10 “(C) appropriate standards and procedures for periodic review
11 of laboratories and criteria for certification and revocation of cer-
12 tification of laboratories to perform controlled substances testing
13 in carrying out this subchapter;

14 “(3) require that a laboratory involved in controlled substances test-
15 ing under this subchapter have the capability and facility, at the lab-
16 oratory, of performing screening and confirmation tests;

17 “(4) provide that all tests indicating the use of alcohol or a con-
18 trolled substance in violation of law or a United States Government
19 regulation be confirmed by a scientifically recognized method of testing
20 capable of providing quantitative information about alcohol or a con-
21 trolled substance;

22 “(5) provide that each specimen be subdivided, secured, and labeled
23 in the presence of the tested individual and that a part of the specimen
24 be retained in a secure manner to prevent the possibility of tampering,
25 so that if the individual’s confirmation test results are positive the indi-
26 vidual has an opportunity to have the retained part tested by a 2d con-
27 firmation test done independently at another certified laboratory if the
28 individual requests the 2d confirmation test not later than 3 days after
29 being advised of the results of the 1st confirmation test;

30 “(6) ensure appropriate safeguards for testing to detect and quantify
31 alcohol in breath and body fluid samples, including urine and blood,
32 through the development of regulations that may be necessary and in
33 consultation with the Secretary of Health and Human Services;

34 “(7) provide for the confidentiality of test results and medical infor-
35 mation (except information about alcohol or a controlled substance) of
36 employees, except that this paragraph does not prevent the use of test
37 results for the orderly imposition of appropriate sanctions under this
38 subchapter; and

39 “(8) ensure that employees are selected for tests by nondiscrim-
40 inatory and impartial methods, so that no employee is harassed by
41 being treated differently from other employees in similar circumstances.

1 **“§ 40986. Rehabilitation**

2 “(a) PROGRAM FOR EMPLOYEES OF AIR CARRIERS AND FOREIGN AIR
3 CARRIERS.—The Administrator shall prescribe regulations establishing re-
4 quirements for rehabilitation programs that at least provide for the identi-
5 fication and opportunity for treatment of employees of air carriers and fore-
6 eign air carriers referred to in section 40983(a)(1) of this title who need
7 assistance in resolving problems with the use of alcohol or a controlled sub-
8 stance in violation of law or a United States Government regulation. Each
9 air carrier and foreign air carrier is encouraged to make the program avail-
10 able to all its employees in addition to the employees referred to in section
11 40983(a)(1). The Administrator shall decide on the circumstances under
12 which employees shall be required to participate in a program. This sub-
13 section does not prevent an air carrier or foreign air carrier from estab-
14 lishing a program under this subsection in cooperation with another air car-
15 rier or foreign air carrier.

16 “(b) PROGRAM FOR EMPLOYEES OF THE TRANSPORTATION SECURITY
17 ADMINISTRATION.—The Administrator shall establish and maintain a reha-
18 bilitation program that at least provides for the identification and oppor-
19 tunity for treatment of employees of the Transportation Security Adminis-
20 tration whose duties include responsibility for security-sensitive functions
21 who need assistance in resolving problems with the use of alcohol or a con-
22 trolled substance.

23 **“§ 40987. Relationship to other laws, regulations, standards,**
24 **and orders**

25 “(a) EFFECT ON STATE AND LOCAL GOVERNMENT LAWS, REGULATIONS,
26 STANDARDS, OR ORDERS.—A State or local government may not prescribe,
27 issue, or continue in effect a law, regulation, standard, or order that is in-
28 consistent with regulations prescribed under this subchapter. However, a
29 regulation prescribed under this subchapter does not preempt a State crimi-
30 nal law that imposes sanctions for reckless conduct leading to loss of life,
31 injury, or damage to property.

32 “(b) INTERNATIONAL OBLIGATIONS AND FOREIGN LAWS.—

33 “(1) IN GENERAL.—In prescribing regulations under this sub-
34 chapter, the Administrator—

35 “(A) shall establish only requirements applicable to foreign air
36 carriers that are consistent with international obligations of the
37 United States; and

38 “(B) shall consider applicable laws and regulations of foreign
39 countries.

40 “(2) REQUEST TO STRENGTHEN AND ENFORCE EXISTING STAND-
41 ARDS.—The Secretary and the Secretary of State jointly shall request

1 the governments of foreign countries that are members of the Inter-
2 national Civil Aviation Organization to strengthen and enforce existing
3 standards to prohibit crewmembers in international civil aviation from
4 using alcohol or a controlled substance in violation of law or a United
5 States Government regulation.

6 “(c) OTHER REGULATIONS ALLOWED.—This section does not prevent the
7 Administrator from continuing in effect, amending, or further
8 supplementing a regulation prescribed before October 28, 1991, governing
9 the use of alcohol or a controlled substance by airport security screening
10 employees, air carrier employees responsible for security-sensitive functions
11 (as decided by the Administrator), or employees of the Transportation Secu-
12 rity Administration with responsibility for security-sensitive functions.

13 **“Subchapter V—Enforcement and** 14 **Penalties**

15 **“Part A—Enforcement**

16 **“§ 41001. Complaints and investigations**

17 “(a) IN GENERAL.—

18 “(1) FILING COMPLAINT.—A person may file a complaint in writing
19 with the Administrator about a person violating this chapter or a re-
20 quirement prescribed under this chapter. Except as provided in sub-
21 section (b), the Administrator shall investigate the complaint if a rea-
22 sonable ground appears to the Administrator for the investigation.

23 “(2) CONDUCTING INVESTIGATION.—On the initiative of the Admin-
24 istrator, the Administrator may conduct an investigation, if a reason-
25 able ground appears to the Administrator for the investigation, about—

26 “(A) a person violating this chapter or a requirement prescribed
27 under this chapter; or

28 “(B) a question that may arise under this chapter.

29 “(3) DISMISSAL OF COMPLAINT.—The Administrator may dismiss a
30 complaint without a hearing when the Administrator is of the opinion
31 that the complaint does not state facts that warrant an investigation
32 or action.

33 “(4) HEARINGS AND ORDERS.—After notice and an opportunity for
34 a hearing and subject to section 40105(b) of title 49, the Administrator
35 shall issue an order to compel compliance with this chapter if the Ad-
36 ministrator finds in an investigation under this subsection that a per-
37 son is violating this chapter.

38 “(b) COMPLAINTS AGAINST MEMBERS OF ARMED FORCES.—The Admin-
39 istrator shall refer a complaint against a member of the armed forces of
40 the United States performing official duties to the Secretary of the depart-
41 ment concerned for action. Not later than 90 days after receiving the com-

1 plaint, the Secretary of that department shall inform the Administrator of
2 the action taken on the complaint, including any corrective or disciplinary
3 action taken.

4 **“§ 41002. Proceedings**

5 “(a) CONDUCTING PROCEEDINGS.—Subject to subchapter II of chapter 5
6 of title 5, the Administrator may conduct proceedings in a way conducive
7 to justice and the proper dispatch of business.

8 “(b) APPEARANCE.—A person may appear and be heard before the Ad-
9 ministrator in person or by an attorney.

10 “(c) RECORDING AND PUBLIC ACCESS.—Official action taken by the Ad-
11 ministrator under this chapter shall be recorded. Proceedings before the Ad-
12 ministrator shall be open to the public on request of an interested party un-
13 less the Administrator decides that secrecy is required because of national
14 defense.

15 “(d) CONFLICTS OF INTEREST.—The Administrator or an officer or em-
16 ployee of the Transportation Security Administration may not participate in
17 a proceeding referred to in subsection (a) in which the individual has a pe-
18 cuniary interest.

19 **“§ 41003. Service of notice, process, and actions**

20 “(a) DESIGNATING AGENTS.—

21 “(1) IN GENERAL.—Each air carrier and foreign air carrier shall
22 designate an agent on whom service of notice and process in a pro-
23 ceeding before, and an action of, the Administrator, may be made.

24 “(2) FORM OF DESIGNATION; CHANGES.—The designation—

25 “(A) shall be in writing and filed with the Administrator; and

26 “(B) may be changed in the same way as originally made.

27 “(b) SERVICE.—

28 “(1) METHOD OF SERVICE.—Service may be made—

29 “(A) by personal service;

30 “(B) on a designated agent; or

31 “(C) by certified or registered mail to the person to be served
32 or the designated agent of the person.

33 “(2) DATE OF SERVICE.—The date of service made by certified or
34 registered mail is the date of mailing.

35 “(c) SERVING AGENTS.—Service on an agent designated under this sec-
36 tion shall be made at the office or usual place of residence of the agent.
37 If an air carrier or foreign air carrier does not have a designated agent,
38 service may be made by posting the notice, process, or action in the office
39 of the Administrator.

1 **“§ 41004. Evidence**

2 “(a) IN GENERAL.—In conducting a hearing or investigation under this
3 chapter, the Administrator may—

4 “(1) subpoena witnesses and records related to a matter involved in
5 the hearing or investigation from any place in the United States to the
6 designated place of the hearing or investigation;

7 “(2) administer oaths;

8 “(3) examine witnesses; and

9 “(4) receive evidence at a place in the United States the Adminis-
10 trator designates.

11 “(b) COMPLIANCE WITH SUBPOENAS.—If a person disobeys a subpoena,
12 the Administrator or a party to a proceeding before the Administrator may
13 petition a court of the United States to enforce the subpoena. A judicial
14 proceeding to enforce a subpoena under this section may be brought in the
15 jurisdiction in which the proceeding or investigation is conducted. The court
16 may punish a failure to obey an order of the court to comply with the sub-
17 poena as a contempt of court.

18 “(c) DEPOSITIONS.—

19 “(1) IN GENERAL.—In a proceeding or investigation, the Adminis-
20 trator may order an individual to give testimony by deposition and to
21 produce records. If an individual fails to be deposed or to produce
22 records, the order may be enforced in the same way a subpoena may
23 be enforced under subsection (b).

24 “(2) TAKING OF DEPOSITION.—A deposition may be taken before an
25 individual designated by the Administrator and having the power to ad-
26 minister oaths.

27 “(3) NOTICE REQUIREMENTS.—Before taking a deposition, the party
28 or the attorney of the party proposing to take the deposition must give
29 reasonable notice in writing to the opposing party or the attorney of
30 record of that party. The notice shall state the name of the witness
31 and the time and place of the taking of the deposition.

32 “(4) DEPOSITION PROCESS.—The testimony of an individual deposed
33 under this subsection shall be under oath. The individual taking the
34 deposition shall prepare, or cause to be prepared, a transcript of the
35 testimony taken. The transcript shall be subscribed by the deponent.
36 Each deposition shall be filed promptly with the Administrator.

37 “(5) DEPOSITIONS ABROAD.—If the laws of a foreign country allow,
38 the testimony of a witness in that country may be taken by deposi-
39 tion—

1 “(A) by a consular officer or an individual commissioned by the
2 Administrator or agreed on by the parties by written stipulation
3 filed with the Administrator; or

4 “(B) under letters rogatory issued by a court of competent ju-
5 risdiction at the request of the Administrator.

6 “(d) WITNESS FEES AND MILEAGE AND CERTAIN FOREIGN COUNTRY
7 EXPENSES.—A witness summoned before the Administrator or whose depo-
8 sition is taken under this section and the individual taking the deposition
9 are each entitled to the same fee and mileage that the witness and indi-
10 vidual would have been paid for those services in a court of the United
11 States. Under regulations of the Administrator, the Administrator shall pay
12 the necessary expenses incident to executing, in another country, a commis-
13 sion or letter rogatory issued at the initiative of the Administrator.

14 “(e) DESIGNATING EMPLOYEES TO CONDUCT HEARINGS.—When des-
15 ignated by the Administrator, an employee appointed under section 3105 of
16 title 5 may conduct a hearing, subpoena witnesses, administer oaths, exam-
17 ine witnesses, and receive evidence at a place in the United States the Ad-
18 ministrator designates. On request of a party, the Administrator shall hear
19 or receive argument.

20 **“§ 41005. Regulations and orders**

21 “(a) EFFECTIVENESS OF ORDERS.—Except as provided in this chapter,
22 a regulation prescribed or order issued by the Administrator takes effect
23 within a reasonable time prescribed by the Administrator. The regulation or
24 order remains in effect under its own terms or until superseded. Except as
25 provided in this chapter, the Administrator may amend, modify, or suspend
26 an order in the way, and by giving the notice, that the Administrator de-
27 cides.

28 “(b) CONTENTS AND SERVICE OF ORDERS.—An order of the Adminis-
29 trator shall include the findings of fact on which the order is based and
30 shall be served on the parties to the proceeding and the persons affected
31 by the order.

32 **“§ 41006. Enforcement by the Department**

33 “The Administrator may bring a civil action against a person in a district
34 court of the United States to enforce this chapter or a requirement or regu-
35 lation prescribed or order issued under this chapter. The action may be
36 brought in the judicial district in which the person does business or the vio-
37 lation occurred.

38 **“§ 41007. Enforcement by Attorney General**

39 “(a) IN GENERAL.—On request of the Administrator, the Attorney Gen-
40 eral may bring a civil action in an appropriate court—

1 “(1) to enforce this chapter or a requirement or regulation pre-
2 scribed or order issued under this chapter; and

3 “(2) to prosecute a person violating this chapter or a requirement
4 or regulation prescribed or order issued under this chapter.

5 “(b) COSTS AND EXPENSES PAID OUT OF APPROPRIATIONS FOR COURT
6 EXPENSES.—The costs and expenses of a civil action under this chapter
7 shall be paid out of the appropriations for the expenses of the courts of the
8 United States.

9 “(c) PARTICIPATION OF ADMINISTRATOR.—On request of the Attorney
10 General, the Administrator may participate in a civil action under this chap-
11 ter.

12 **“§ 41008. Joinder and intervention**

13 “A person interested in or affected by a matter under consideration in
14 a proceeding before the Administrator, a civil action to enforce this chapter,
15 or a requirement or regulation prescribed or order issued under this chapter
16 may be joined as a party or permitted to intervene in the proceeding or civil
17 action.

18 **“§ 41009. Judicial review**

19 “(a) FILING AND VENUE.—A person disclosing a substantial interest in
20 an order issued by the Administrator, in whole or in part under this chapter
21 or section 11507 or 11513 of this title, may apply for review of the order
22 by filing a petition for review in the United States Court of Appeals for the
23 District of Columbia Circuit or in the court of appeals of the United States
24 for the circuit in which the person resides or has its principal place of busi-
25 ness. The petition must be filed not later than 60 days after the order is
26 issued. The court may allow the petition to be filed after the 60th day only
27 if there are reasonable grounds for not filing by the 60th day.

28 “(b) JUDICIAL PROCEDURES.—When a petition is filed under subsection
29 (a), the clerk of the court immediately shall send a copy of the petition to
30 the Administrator. The Administrator shall file with the court a record of
31 any proceeding in which the order was issued, as provided in section 2112
32 of title 28.

33 “(c) AUTHORITY OF COURT.—When the petition is sent to the Adminis-
34 trator, the court has exclusive jurisdiction to affirm, amend, modify, or set
35 aside any part of the order and may order the Administrator to conduct
36 further proceedings. After reasonable notice to the Administrator, the court
37 may grant interim relief by staying the order or taking other appropriate
38 action when good cause for its action exists. Findings of fact by the Admin-
39 istrator, if supported by substantial evidence, are conclusive.

40 “(d) REQUIREMENT FOR PRIOR OBJECTION.—In reviewing an order
41 under this section, the court may consider an objection to an order of the

1 Administrator only if the objection was made in the proceeding conducted
2 by the Administrator or if there was a reasonable ground for not making
3 the objection in the proceeding.

4 “(e) SUPREME COURT REVIEW.—A decision by a court under this section
5 may be reviewed only by the Supreme Court under section 1254 of title 28.

6 **“Part B—Penalties**

7 **“Subpart 1—Civil Penalties**

8 **“§ 41021. General penalties**

9 “(a) DEFINITION OF SMALL BUSINESS CONCERN.—In this section, the
10 term “small business concern” has the meaning given the term in section
11 3 of the Small Business Act (15 U.S.C. 632).

12 “(b) IN GENERAL.—

13 “(1) CIVIL PENALTY.—Except as provided in paragraph (2), a person
14 is liable to the United States Government for a civil penalty of not
15 more than \$10,000, and not more \$25,000 in the case of a person op-
16 erating an aircraft for the transportation of passengers or property for
17 compensation (except an individual serving as an airman), for violating
18 this chapter.

19 “(2) PENALTIES APPLICABLE TO INDIVIDUALS AND SMALL BUSINESS
20 CONCERNS.—An individual (except an airman serving as an airman) or
21 small business concern is liable to the United States Government for
22 a civil penalty of not more than \$10,000 for violating—

23 “(A) this chapter (except sections 40912, 40913(d), 40914, and
24 40917 through 40919); or

25 “(B) a regulation prescribed or order issued under a provision
26 to which subparagraph (A) applies.

27 “(3) SEPARATE VIOLATIONS.—A separate violation occurs under this
28 subsection for each day the violation continues or, if applicable, for
29 each flight involving the violation.

30 “(4) FAILURE TO COLLECT AIRPORT SECURITY BADGES.—Notwith-
31 standing paragraph (1), an employer (other than a governmental entity
32 or airport operator) who employs an employee to whom an airport secu-
33 rity badge or other identifier used to obtain access to a secure area of
34 an airport is issued and who does not collect or make reasonable efforts
35 to collect the badge from the employee on the date that the employ-
36 ment of the employee is terminated and does not notify the operator
37 of the airport of the termination within 24 hours of the date of the
38 termination is liable to the Government for a civil penalty not to exceed
39 \$10,000.

40 “(c) ADMINISTRATIVE IMPOSITION OF PENALTIES.—

1 “(1) IN GENERAL.—The Secretary may impose a civil penalty for a
2 violation of this chapter (except sections 40912, 40913(d), 40917 (a)
3 through (d)(1)(A) and (1)(C) through (f), 40918, and 40919).

4 “(2) WRITTEN NOTICE.—The Secretary shall give written notice of
5 the finding of a violation and the penalty.

6 “(3) LIMIT ON REEXAMINATION.—In a civil action to collect a civil
7 penalty imposed by the Secretary under this subsection, the issues of
8 liability and the amount of the penalty may not be reexamined.

9 “(4) DISTRICT COURT JURISDICTION.—Notwithstanding paragraph
10 (1), the district courts of the United States have exclusive jurisdiction
11 of a civil action involving a penalty the Secretary initiates if—

12 “(A) the amount in controversy is more than—

13 “(i) \$50,000 if the violation was committed by a person be-
14 fore December 12, 2003;

15 “(ii) \$400,000 if the violation was committed by a person
16 other than an individual or small business concern on or after
17 that date; or

18 “(iii) \$50,000 if the violation was committed by an indi-
19 vidual or small business concern on or after that date;

20 “(B) the action is in rem or another action in rem based on the
21 same violation has been brought;

22 “(C) the action involves an aircraft subject to a lien that has
23 been seized by the Government; or

24 “(D) another action has been brought for an injunction based
25 on the same violation.

26 “(5) MAXIMUM PENALTY.—The maximum civil penalty the Adminis-
27 trator may impose under this subsection is—

28 “(A) \$50,000 if the violation was committed by a person before
29 December 12, 2003;

30 “(B) \$400,000 if the violation was committed by a person other
31 than an individual or small business concern on or after that date;
32 or

33 “(C) \$50,000 if the violation was committed by an individual or
34 small business concern on or after that date.

35 “(d) COMPROMISE AND SETOFF.—

36 “(1) COMPROMISE.—The Secretary may compromise the amount of
37 a civil penalty imposed for violating—

38 “(A) this chapter (except sections 40912, 40913(d), 40914,
39 40917(a) through (d)(1)(A) and (1)(C) through (f), 40918, and
40 40919); or

1 “(B) a regulation prescribed or order issued under a provision
2 to which subparagraph (A) applies.

3 “(2) SETOFF.—The United States Government may deduct the
4 amount of a civil penalty imposed or compromised under this sub-
5 section from amounts it owes the person liable for the penalty.

6 “(e) JUDICIAL REVIEW.—An order of the Secretary imposing a civil pen-
7 alty may be reviewed judicially only under section 41009 of this title.

8 “(f) NONAPPLICATION.—

9 “(1) IN GENERAL.—This section does not apply to the following
10 when performing official duties:

11 “(A) A member of the armed forces of the United States.

12 “(B) A civilian employee of the Department of Defense subject
13 to the Uniform Code of Military Justice.

14 “(2) REPORT ON ACTION TAKEN.—The appropriate military author-
15 ity is responsible for taking necessary disciplinary action and submit-
16 ting to the Administrator a timely report on any action taken.

17 **“§ 41022. False information**

18 “(a) CIVIL PENALTY.—A person that, knowing the information to be
19 false, gives, or causes to be given, under circumstances in which the infor-
20 mation reasonably may be believed, false information about an alleged at-
21 tempt being made or to be made to do an act that would violate section
22 41062(a), 41064, 41065, or 41066 of this title is liable to the United States
23 Government for a civil penalty of not more than \$10,000 for each violation.

24 “(b) COMPROMISE AND SETOFF.—

25 “(1) COMPROMISE.—The Secretary may compromise the amount of
26 a civil penalty imposed under subsection (a).

27 “(2) SETOFF.—The United States Government may deduct the
28 amount of a civil penalty imposed or compromised under this section
29 from amounts it owes the person liable for the penalty.

30 **“§ 41023. Carrying a weapon**

31 “(a) CIVIL PENALTY.—An individual who, when on, or attempting to
32 board, an aircraft in, or intended for operation in, air transportation or
33 intrastate air transportation, has on or about the individual or the property
34 of the individual a concealed dangerous weapon that is or would be acces-
35 sible to the individual in flight is liable to the United States Government
36 for a civil penalty of not more than \$10,000 for each violation.

37 “(b) COMPROMISE AND SETOFF.—

38 “(1) COMPROMISE.—The Secretary may compromise the amount of
39 a civil penalty imposed under subsection (a).

1 “(2) SETOFF.—The United States Government may deduct the
2 amount of a civil penalty imposed or compromised under this section
3 from amounts it owes the individual liable for the penalty.

4 “(c) NONAPPLICATION.—This section does not apply to—

5 “(1) a law enforcement officer of a State or political subdivision of
6 a State, or an officer or employee of the United States Government,
7 authorized to carry arms in an official capacity; or

8 “(2) another individual the Secretary by regulation authorizes to
9 carry arms in an official capacity.

10 **“§ 41024. Liens on aircraft**

11 “When an aircraft is involved in a violation of this chapter (except sec-
12 tions 40912, 40913(d), 40914, 40917(a) through (d)(1)(A) and (1)(C)
13 through (f), and 40918) and the violation is by the owner of, or individual
14 commanding, the aircraft, the aircraft is subject to a lien for the civil pen-
15 alty as provided in section 46304 of title 49.

16 **“§ 41025. Actions to recover civil penalties**

17 “A civil penalty under this subpart may be collected by bringing a civil
18 action against the person subject to the penalty, a civil action in rem
19 against an aircraft subject to a lien for a penalty, or both. The action shall
20 conform as nearly as practicable to a civil action in admiralty, regardless
21 of the place an aircraft in a civil action in rem is seized. However, a party
22 may demand a jury trial of an issue of fact in an action involving a civil
23 penalty under this chapter if the value of the matter in controversy is more
24 than \$20. Issues of fact tried by a jury may be reexamined only under com-
25 mon law rules.

26 **“Subpart 2—Criminal Penalties**

27 **“§ 41041. Reporting and recordkeeping violations.**

28 “An air carrier or an officer, agent, or employee of an air carrier shall
29 be fined under title 18 for intentionally—

30 “(1) failing to make a report or keep a record under this chapter;

31 “(2) falsifying, mutilating, or altering a report or record under this
32 chapter; or

33 “(3) filing a false report or record under this chapter.

34 **“§ 41042. Unlawful disclosure of information**

35 “(a) CRIMINAL PENALTY.—The Administrator, or an officer or employee
36 of the Transportation Security Administration, shall be fined under title 18,
37 imprisoned for not more than 2 years, or both, if the Administrator, officer,
38 or employee knowingly and willfully discloses information that—

39 “(1) the Administrator, officer, or employee acquires when inspecting
40 the records of an air carrier; or

1 “(2) is withheld from public disclosure under section 40963 of this
2 title.

3 “(b) NONAPPLICATION.—Subsection (a) does not apply if—

4 “(1) the officer or employee is directed by the Administrator to dis-
5 close information that the Administrator had ordered withheld; or

6 “(2) the Administrator, officer, or employee is directed by a court
7 of competent jurisdiction to disclose the information.

8 “(c) WITHHOLDING INFORMATION FROM CONGRESS.—This section does
9 not authorize the Administrator to withhold information from a committee
10 of Congress authorized to have the information.

11 **“§ 41043. Refusing to appear or produce records**

12 “A person not obeying a subpoena or requirement of the Administrator
13 to appear and testify or produce records shall be fined under title 18, im-
14 prisoned for not more than 1 year, or both.

15 **“§ 41044. Entering aircraft or airport area in violation of se-
16 curity requirements**

17 “(a) PROHIBITION.—A person may not knowingly and willfully enter, in
18 violation of security requirements prescribed under section 40911, 40913(b)
19 or (c), or 40916 of this title, an aircraft or an airport area that serves an
20 air carrier or foreign air carrier.

21 “(b) CRIMINAL PENALTY.—

22 “(1) IN GENERAL.—A person violating subsection (a) shall be fined
23 under title 18, imprisoned for not more than 1 year, or both.

24 “(2) INCREASED PENALTY.—A person violating subsection (a) with
25 intent to evade security procedures or restrictions or with intent to
26 commit, in the aircraft or airport area, a felony under a law of the
27 United States or a State shall be fined under title 18, imprisoned for
28 not more than 10 years, or both.

29 “(c) NOTICE OF PENALTIES.—

30 “(1) SIGNS.—Each operator of an airport in the United States that
31 is required to establish an air transportation security program under
32 section 40913(c) of this title shall ensure that signs that meet require-
33 ments the Secretary may prescribe for providing notice of the penalties
34 imposed under subsection (b) and section 41021(b)(2)(A) of this title
35 are displayed near all screening locations, all locations where pas-
36 sengers exit the sterile area, and other locations at the airport that the
37 Secretary determines appropriate.

38 “(2) EFFECT OF SIGNS ON PENALTIES.—An individual is subject to
39 a penalty imposed under subsection (b) or section 41021(b)(2)(A) of
40 this title without regard to whether signs are displayed at an airport
41 as required by paragraph (1).

1 **“§ 41045. General criminal penalty when specific penalty**
2 **not provided**

3 “When another criminal penalty is not provided under this chapter, a per-
4 son that knowingly and willfully violates section 40912, 40913(d), 40914,
5 40917, 40918, or 40919 of this title, or a regulation prescribed or order
6 issued by the Administrator under section 40912, 40913(d), 40914, 40917,
7 40918, or 40919 of this title, shall be fined under title 18. A separate viola-
8 tion occurs for each day the violation continues.

9 **“Subchapter VI—Special Aircraft**
10 **Jurisdiction of the United States**

11 **“§ 41061. Definitions**

12 “In this subchapter:

13 “(1) AIRCRAFT IN FLIGHT.—The term ‘aircraft in flight’ means an
14 aircraft from the moment all external doors are closed following board-
15 ing—

16 “(A) through the moment when one external door is opened to
17 allow passengers to leave the aircraft; or

18 “(B) until, if a forced landing, competent authorities take over
19 responsibility for the aircraft and individuals and property on the
20 aircraft.

21 “(2) COMMIT AN OFFENSE.—The term ‘commit an offense’ means,
22 in the case of an individual and for the purposes of the Convention for
23 the Suppression of Unlawful Seizure of Aircraft, when the individual,
24 when on an aircraft in flight—

25 “(A) by any form of intimidation, unlawfully seizes, exercises
26 control of, or attempts to seize or exercise control of, the aircraft;
27 or

28 “(B) is an accomplice of an individual referred to in subpara-
29 graph (A).

30 “(3) SPECIAL AIRCRAFT JURISDICTION OF THE UNITED STATES.—
31 The term ‘special aircraft jurisdiction of the United States’ includes
32 any of the following aircraft in flight:

33 “(A) A civil aircraft of the United States.

34 “(B) An aircraft of the armed forces of the United States.

35 “(C) Another aircraft in the United States.

36 “(D) Another aircraft outside the United States—

37 “(i) that has its next scheduled destination or last place of
38 departure in the United States, if the aircraft next lands in
39 the United States;

40 “(ii) on which an individual commits an offense (as speci-
41 fied in the Convention for the Suppression of Unlawful Sei-

1 zure of Aircraft) if the aircraft lands in the United States
2 with the individual still on the aircraft; or

3 “(iii) against which an individual commits an offense (as
4 specified in subsection (d) or (e) of article I, section I of the
5 Convention for the Suppression of Unlawful Acts against the
6 Safety of Civil Aviation) if the aircraft lands in the United
7 States with the individual still on the aircraft.

8 “(E) Any other aircraft leased without crew to a lessee whose
9 principal place of business is in the United States or, if the lessee
10 does not have a principal place of business, whose permanent resi-
11 dence is in the United States.

12 **“§ 41062. Aircraft piracy**

13 “(a) AIRCRAFT PIRACY IN SPECIAL AIRCRAFT JURISDICTION.—

14 “(1) DEFINITION OF AIRCRAFT PIRACY.—In this subsection, the
15 term ‘aircraft piracy’ means seizing or exercising control of an aircraft
16 in the special aircraft jurisdiction of the United States by force, vio-
17 lence, threat of force or violence, or any form of intimidation, and with
18 wrongful intent.

19 “(2) WHEN ATTEMPT TO COMMIT AIRCRAFT PIRACY DEEMED TO BE
20 IN SPECIAL AIRCRAFT JURISDICTION.—An attempt to commit aircraft
21 piracy is deemed to be in the special aircraft jurisdiction of the United
22 States, although the aircraft is not in flight at the time of the attempt,
23 if the aircraft would have been in the special aircraft jurisdiction of the
24 United States had the aircraft piracy been completed.

25 “(3) CRIMINAL PENALTY.—An individual committing or attempting
26 or conspiring to commit aircraft piracy—

27 “(A) shall be imprisoned for at least 20 years; or

28 “(B) notwithstanding section 3559(b) of title 18, if the death
29 of another individual results from the commission or attempt, shall
30 be put to death or imprisoned for life.

31 “(b) AIRCRAFT PIRACY OUTSIDE SPECIAL AIRCRAFT JURISDICTION.—

32 “(1) DEFINITION OF NATIONAL OF THE UNITED STATES.—In this
33 subsection, the term ‘national of the United States’ has the meaning
34 given the term in section 101(a) of the Immigration and Nationality
35 Act (8 U.S.C. 1101(a)).

36 “(2) CRIMINAL PENALTY.—An individual committing or conspiring
37 to commit an offense (as specified in the Convention for the Suppres-
38 sion of Unlawful Seizure of Aircraft) on an aircraft in flight outside
39 the special aircraft jurisdiction of the United States—

40 “(A) shall be imprisoned for at least 20 years; or

1 “(B) notwithstanding section 3559(b) of title 18, if the death
2 of another individual results from the commission or attempt, shall
3 be put to death or imprisoned for life.

4 “(3) JURISDICTION.—There is jurisdiction over the offense in para-
5 graph (2) if—

6 “(A) a national of the United States was aboard the aircraft;

7 “(B) an offender is a national of the United States; or

8 “(C) an offender is afterwards found in the United States.

9 **“§ 41063. Interference with security screening personnel**

10 “An individual in an area in a commercial service airport in the United
11 States who, by assaulting a Federal, airport, or air carrier employee who
12 has security duties in the airport, interferes with the performance of the du-
13 ties of the employee or lessens the ability of the employee to perform those
14 duties shall be fined under title 18, imprisoned for not more than 10 years,
15 or both. If the individual uses a dangerous weapon in committing the as-
16 sault or interference, the individual may be imprisoned for any term of
17 years or for life.

18 **“§ 41064. Interference with flight crew members and attend-
19 ants**

20 “An individual on an aircraft in the special aircraft jurisdiction of the
21 United States who, by assaulting or intimidating a flight crew member or
22 flight attendant of the aircraft, interferes with the performance of the duties
23 of the member or attendant or lessens the ability of the member or attend-
24 ant to perform those duties, or attempts or conspires to do such an act,
25 shall be fined under title 18, imprisoned for not more than 20 years, or
26 both. If a dangerous weapon is used in assaulting or intimidating the mem-
27 ber or attendant, the individual shall be imprisoned for any term of years
28 or for life.

29 **“§ 41065. Carrying a weapon or explosive on an aircraft**

30 “(a) DEFINITION OF LOADED FIREARM.—In this section, the term ‘load-
31 ed firearm’ means a starter gun or a weapon designed or converted to expel
32 a projectile through an explosive, that has a cartridge, a detonator, or pow-
33 der in the chamber, magazine, cylinder, or clip.

34 “(b) GENERAL CRIMINAL PENALTY.—An individual shall be fined under
35 title 18, imprisoned for not more than 10 years, or both, if the individual—

36 “(1) when on, or attempting to get on, an aircraft in, or intended
37 for operation in, air transportation or intrastate air transportation, has
38 on or about the individual or the property of the individual a concealed
39 dangerous weapon that is or would be accessible to the individual in
40 flight;

1 “(2) has placed, attempted to place, or attempted to have placed a
2 loaded firearm on that aircraft in property not accessible to passengers
3 in flight; or

4 “(3) has on or about the individual, or has placed, attempted to
5 place, or attempted to have placed on that aircraft, an explosive or in-
6 cendiary device.

7 “(c) CRIMINAL PENALTY INVOLVING DISREGARD FOR HUMAN LIFE.—An
8 individual who willfully and without regard for the safety of human life, or
9 with reckless disregard for the safety of human life, violates subsection (b)
10 shall be fined under title 18, imprisoned for not more than 20 years, or
11 both, and, if death results to any person, shall be imprisoned for any term
12 of years or for life.

13 “(d) NONAPPLICATION.—Subsection (b)(1) does not apply to—

14 “(1) a law enforcement officer of a State or political subdivision of
15 a State, or an officer or employee of the United States Government,
16 authorized to carry arms in an official capacity;

17 “(2) another individual the Administrator of the Federal Aviation
18 Administration or the Administrator of the Transportation Security
19 Administration by regulation authorizes to carry a dangerous weapon
20 in air transportation or intrastate air transportation; or

21 “(3) an individual transporting a weapon (except a loaded firearm)
22 in baggage not accessible to a passenger in flight if the air carrier was
23 informed of the presence of the weapon.

24 “(e) CONSPIRACY.—If 2 or more individuals conspire to violate subsection
25 (b) or (c), and any of the individuals does any act to effect the object of
26 the conspiracy, each of the parties to the conspiracy shall be punished as
27 provided in subsection (b) or (c).

28 “**§ 41066. Application of certain criminal laws to acts on an**
29 **aircraft**

30 “An individual on an aircraft in the special aircraft jurisdiction of the
31 United States who commits an act that—

32 “(1) if committed in the special maritime and territorial jurisdiction
33 of the United States (as defined in section 7 of title 18) would violate
34 section 113, 114, 661, 662, 1111, 1112, 1113, or 2111 or chapter
35 109A of title 18, shall be fined under title 18, imprisoned under that
36 section or chapter, or both; or

37 “(2) if committed in the District of Columbia would violate section
38 9 of the Act of July 29, 1892 (D.C. Code 22-1312), shall be fined
39 under title 18, imprisoned under section 9 of the Act, or both.

1 **“§ 41067. False information and threats**

2 “An individual shall be fined under title 18, imprisoned for not more than
3 5 years, or both, if the individual—

4 “(1) knowing the information to be false, willfully and maliciously or
5 with reckless disregard for the safety of human life, gives, or causes
6 to be given, under circumstances in which the information reasonably
7 may be believed, false information about an alleged attempt being made
8 or to be made to do an act that would violate section 41062(a), 41064,
9 41065, or 41066 of this title; or

10 “(2) threatens to violate section 41062(a), 41064, 41065, or 41066
11 of this title, or causes a threat to violate any of those sections to be
12 made, and has the apparent determination and will to carry out the
13 threat.”.

14 (2) In the table of contents for chapter 409, by inserting after the
15 item relating to 40963 the following:

“40964. General authority.

“40965. Withholding information.

“Subchapter IV—Alcohol and Controlled Substances Testing

“40981. Definition of controlled substance.

“40982. Applicaiton.

“40983. Alcohol and controlled substances testing program.

“40984. Prohibited service.

“40985. Testing and laboratory requirements.

“40986. Rehabilitation.

“40987. Relationship to other laws, regulations, standards, and orders.

“Subchapter V—Enforcement and Penalties

“Part A—Enforcement

“41001. Complaints and investigations.

“41002. Proceedings.

“41002. Service of notice, process, and actions.

“41004. Evidence.

“41005. Regulations and orders.

“41006. Enforcement by the Department.

“41007. Enforcement by Attorney General.

“41008. Joinder and intervention.

“41009. Judicial review.

“Part B—Penalties

“Subpart 1—Civil Penalties

“41021. General penalties.

“41022. False information.

“41023. Carrying a weapon.

“41024. Liens on aircraft.

“41025. Actions to recover civil penalties.

“Subpart 2—Criminal Penalties

“41041. Reporting and recordkeeping violations.

“41042. Unlawful disclosure of information.

“41043. Refusing to appear or produce records.

“41044. Entering aircraft or airport area in violation of security requirements.

“41045. General criminal penalty when specific penalty not provided.

“Subchapter VI—Special Aircraft Jurisdiction of the United States

“41061. Definitions.

“41062. Aircraft piracy.

“41063. Interference with security screening personnel.

“41064. Interference with flight crew members and attendants.

“41065. Carrying a weapon or explosive on an aircraft.

“41066. Application of certain criminal laws to acts on an aircraft.
“41067. False information and threats.”.

1 (b) TITLE 49, UNITED STATES CODE.—Title 49, United States Code, is
2 amended as follows:

3 (1) Chapter 51 is amended—

4 (A) by inserting after section 5110 the following:

5 **“§ 5111. Hazardous materials highway route plans**

6 “(a) ROUTE PLAN GUIDANCE.—The Secretary of Transportation, in con-
7 sultation with the Secretary of Homeland Security, shall—

8 “(1) document existing and proposed routes for the transportation
9 of radioactive and nonradioactive hazardous materials by motor carrier,
10 and develop a framework for using a geographic information system-
11 based approach to characterize routes in the national hazardous mate-
12 rials route registry;

13 “(2) assess and characterize existing and proposed routes for the
14 transportation of radioactive and nonradioactive hazardous materials
15 by motor carrier for the purpose of identifying measurable criteria for
16 selecting routes based on safety and security concerns;

17 “(3) analyze current route-related hazardous materials regulations in
18 the United States, Canada, and Mexico to identify cross-border dif-
19 ferences and conflicting regulations;

20 “(4) document the safety and security concerns of the public, motor
21 carriers, and State, local, territorial, and tribal governments about the
22 highway routing of hazardous materials;

23 “(5) prepare guidance materials for State officials to assist them in
24 identifying and reducing both safety concerns and security risks when
25 designating highway routes for hazardous materials consistent with the
26 13 safety-based nonradioactive materials routing criteria and radio-
27 active materials routing criteria in subparts C and D of part 397 of
28 title 49, Code of Federal Regulations;

29 “(6) develop a tool that will enable State officials to examine poten-
30 tial routes for the highway transportation of hazardous materials, as-
31 sess specific security risks associated with each route, and explore al-
32 ternative mitigation measures; and

33 “(7) transmit to the appropriate congressional committees (as de-
34 fined in section 10101 of title 6) a report on the actions taken to fulfill
35 paragraphs (1) through (6) and any recommended changes to the rout-
36 ing requirements for the highway transportation of hazardous materials
37 in part 397 of title 49, Code of Federal Regulations.

38 “(b) ROUTE PLANS.—

1 “(1) ASSESSMENT.—The Secretary of Transportation shall complete
2 an assessment of the safety and national security benefits achieved
3 under existing requirements for route plans, in written or electronic
4 format, for explosives and radioactive materials. The assessment shall,
5 at a minimum—

6 “(A) compare the percentage of Department of Transportation
7 recordable incidents and the severity of the incidents for shipments
8 of explosives and radioactive materials for which route plans are
9 required with the percentage of recordable incidents and the sever-
10 ity of the incidents for shipments of explosives and radioactive ma-
11 terials not subject to route plans; and

12 “(B) quantify the security and safety benefits, feasibility, and
13 costs of requiring each motor carrier that is required to have a
14 hazardous materials safety permit under part 385 of title 49, Code
15 of Federal Regulations, to maintain, follow, and carry a route plan
16 that meets the requirements of section 397.101 of that title when
17 transporting the type and quantity of hazardous materials de-
18 scribed in section 385.403 of that title, taking into account the
19 various segments of the motor carrier industry, including tank
20 truck, truckload, and less-than-truckload carriers.

21 “(2) REPORT.—The Secretary of Transportation shall submit a re-
22 port to the appropriate congressional committees containing the find-
23 ings and conclusions of the assessment.

24 “(c) REQUIREMENT.—The Secretary shall require a motor carrier that
25 has a hazardous materials safety permit under part 385 of title 49, Code
26 of Federal Regulations, to maintain, follow, and carry a route plan, in writ-
27 ten or electronic format, that meets the requirements of section 397.101 of
28 that title when transporting the type and quantity of hazardous materials
29 described in section 385.403 of that title if the Secretary determines, under
30 the assessment required in subsection (b), that such a requirement would
31 enhance security and safety without imposing unreasonable costs or burdens
32 upon motor carriers.”;

33 (B) by inserting after section 5118 the following:

34 “**§5118a. Hazardous materials security inspections and**
35 **study**

36 “(a) IN GENERAL.—The Secretary of Transportation shall consult with
37 the Secretary of Homeland Security to limit, to the extent practicable, dupli-
38 cative reviews of the hazardous materials security plans required under part
39 172, title 49, Code of Federal Regulations.

40 “(b) TRANSPORTATION COSTS STUDY.—The Secretary of Transportation,
41 in conjunction with the Secretary of Homeland Security, shall study to what

1 extent the insurance, security, and safety costs borne by railroad carriers,
2 motor carriers, pipeline carriers, air carriers, and maritime carriers associ-
3 ated with the transportation of hazardous materials are reflected in the
4 rates paid by offerors of the commodities as compared to the costs and
5 rates, respectively, for the transportation of nonhazardous materials.”; and

6 (C) in the table of contents—

7 (i) by inserting the following after the item relating to sec-
8 tion 5110:

“5111. Hazardous materials highway route plans.”;

9 and

10 (ii) by inserting the following after the item relating to sec-
11 tion 5118:

“5118a. Hazardous materials security inspections and study.”.

12 (2) Section 40113(a) is amended—

13 (A) by striking “or the Administrator of the Transportation Se-
14 curity Administration with respect to security duties and powers
15 designated to be carried out by that Administrator”; and

16 (B) by striking “, Administrator of the Transportation Security
17 Administration,”.

18 (3) Chapter 461 is amended—

19 (A) in sections 46101(a)(1), 46102(a), 46103(a), 46104(a),
20 46105(a), 46106, 46107(b), 46109, and 46110(a), by striking “or
21 the Administrator of the Transportation Security Administration
22 with respect to security duties and powers designated to be carried
23 out by the Administrator of the Transportation Security Adminis-
24 tration” and

25 (B) in sections 46101, 46102, 46103, 46104, 46105, 46107,
26 and 46110, by striking “, Administrator of the Transportation Se-
27 curity Administration,” each place it appears;

28 (C) in section 46102—

29 (i) in subsection (b), by striking “, the Administrator of the
30 Transportation Security Administration,”; and

31 (ii) in subsection (d), by striking “the Administrator of the
32 Transportation Security Administration,”;

33 (D) in section 46104(b), by striking “the Administrator of the
34 Transportation Security Administration,”.

35 (4) Chapter 463 is amended—

36 (A) in section 46301—

37 (i) in subsection (d)(2), by striking the last two sentences
38 and inserting “The Administrator of the Federal Aviation Ad-

1 ministration shall give written notice of the finding of a viola-
2 tion and the penalty.”;

3 (ii) in subsection (d)(3), by striking “Secretary of Home-
4 land Security or”;

5 (iii) in subsection (d)(4), by striking “Secretary of Home-
6 land Security or”;

7 (iv) in subsection (d)(8), by striking “Administrator of the
8 Transportation Security Administration, Administrator of the
9 Federal Aviation Administration,” and inserting “Adminis-
10 trator of the Federal Aviation Administration”; and

11 (v) in subsection (h)(2), by striking “or the Administrator
12 of the Transportation Security Administration with respect to
13 security duties and powers designated to be carried out by the
14 Administrator of the Transportation Security Administra-
15 tion”;

16 (B) in section 46311—

17 (i) in subsection (a), by striking “the Administrator of the
18 Transportation Security Administration with respect to secu-
19 rity duties and powers designated to be carried out by the
20 Administrator of the Transportation Security Administration,
21 or”;

22 (ii) by striking “, Administrator of the Transportation Se-
23 curity Administration, or” each place it appears and inserting
24 “or”; and

25 (iii) by striking “Administrator of the Transportation Secu-
26 rity Administration, Administrator of the Federal Aviation
27 Administration” each place it appears and inserting “Admin-
28 istrator of the Federal Aviation Administration”; and

29 (C) in section 46313, by striking “or the Administrator of the
30 Transportation Security Administration with respect to security
31 duties and powers designated to be carried out by the Adminis-
32 trator of the Transportation Security Administration”.

33 (5) Section 367 of Public Law 108–7 (49 U.S.C. 47110 note) is
34 amended—

35 (A) in subsection (a), by striking “Under Secretary of Trans-
36 portation for Security” and inserting “Administrator of the Trans-
37 portation Security Administration”; and

38 (B) by striking “Under Secretary” each place it appears and in-
39 serting “Administrator”.

40 (6) The table of contents for subtitle VII of title 49, United States
41 Code, is amended as follows:

1 (A) After the item for chapter 448, by striking
2 “**449. Security** **44901**”.

3 (B) After the item for chapter 463, by striking
4 “**465. Special Aircraft Jurisdiction of the United States** **46501**”.

5 **SEC. 5. CONFORMING CROSS REFERENCES.**

6 (a) TITLE 5, UNITED STATES CODE.—Title 5, United States Code, is
7 amended as follows:

8 (1) Section 9701(g) is amended by striking “section 842 of the
9 Homeland Security Act of 2002” and inserting “section 10362 of title
10 6”.

11 (2) Section 10101 is amended—

12 (A) in paragraph (3), by striking “section 602 of the Post-
13 Katrina Emergency Management Reform Act of 2006” and insert-
14 ing “section 20101 of title 6”; and

15 (B) in paragraph (5), by striking “section 624 of the Post-
16 Katrina Emergency Management Reform Act of 2006” and insert-
17 ing “section 20301 of title 6”.

18 (3) Section 10103(b) is amended by striking “section 844 of the
19 Homeland Security Act of 2002” and inserting “section 10366 of title
20 6”.

21 (b) TITLE 8, UNITED STATES CODE.—Section 7202(g)(2)(H) of the In-
22 telligence Reform and Terrorism Prevention Act of 2004 (8 U.S.C.
23 1777(g)(2)(H)) is amended by striking “section 1016(b)” and inserting
24 “section 11908(b) of title 6, United States Code”.

25 (c) TITLE 10, UNITED STATES CODE.—Section 130d of title 10, United
26 States Code, is amended by striking “section 892 of the Homeland Security
27 Act of 2002 (6 U.S.C. 482)” and inserting “section 11907 of title 6”.

28 (d) TITLE 16, UNITED STATES CODE.—Section 402(b)(1)(H) of the
29 Magnuson-Stevens Fishery Conservation and Management Act (16 U.S.C.
30 1881a(b)(1)(H)) is amended by striking “as defined in section 888(a)(2) of
31 the Homeland Security Act of 2002 (6 U.S.C. 468(a)(2))”.

32 (e) TITLE 19, UNITED STATES CODE.—Title 19, United States Code, is
33 amended as follows:

34 (1) Section 13031(f)(2) of Public Law 99–272 (19 U.S.C. 58e(f)(2))
35 is amended by striking “section 415 of the Homeland Security Act of
36 2002 (other than functions performed by the Office of International
37 Affairs referred to in section 415(8) of that Act),” and inserting “sec-
38 tion 11131 of title 6, United States Code (other than functions per-
formed by the Office of International Affairs referred to in section
11131(8) of that title),”.

1 (2) Section 301(h) of Public Law 99–272 (19 U.S.C. 2075(h)) is
2 amended—

3 (A) in paragraph (1), by striking “section 412(b)(2) of the
4 Homeland Security Act of 2002 (6 U.S.C. 212(b)(2))” and “sec-
5 tion 412(b)(1) of such Act” and inserting “section 11132(b)(2) of
6 title 6, United States Code” and “section 11132(b)(1) of such
7 title”, respectively; and

8 (B) in paragraph (2)(A), by striking “section 412(b) of the
9 Homeland Security Act of 2002 (6 U.S.C. 212(b))” and inserting
10 “section 11132(b) of title 6, United States Code.”.

11 (f) TITLE 26, UNITED STATES CODE.—Section 4261(f) of the Internal
12 Revenue Code of 1986 (26 U.S.C. 4261(f)) is amended by striking “44509
13 or 44913(b)” and inserting “40923(b) of title 6, United States Code, or sec-
14 tion 44509”.

15 (g) TITLE 31, UNITED STATES CODE.—Section 3516(f)(3)(A) of title 31,
16 United States Code, is amended by striking “section 874(b)(2) of the
17 Homeland Security Act of 2002” and inserting “section 10396(b)(2) of title
18 6”.

19 (h) TITLE 33, UNITED STATES CODE.—Section 303(b)(4) of Public Law
20 105–384 (33 U.S.C. 892a(b)(4)) is amended by striking “section 641 of the
21 Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 741)”
22 and inserting “section 20501 of title 6, United States Code”.

23 (i) TITLE 38, UNITED STATES CODE.—Section 8117(a)(2)(C) of title 38,
24 United States Code, is amended by striking “section 502(6) of the Home-
25 land Security Act of 2002” and inserting “section 11303(a)(6) of title 6”.

26 (j) TITLE 42, UNITED STATES CODE.—Title 42, United States Code, is
27 amended as follows:

28 (1) Section 319F–1(a)(2)(A) of the Act of July 1, 1944 (42 U.S.C.
29 247d–6a(a)(2)(A)) is amended by striking “sections 302(2) and 304(a)
30 of the Homeland Security Act of 2002” and inserting “sections
31 10901(2) and 10903(a) of title 6, United States Code”.

32 (2) Section 319F–2(c) of the Act of July 1, 1944 (42 U.S.C. 247d–
33 6b(c)) is amended—

34 (A) in paragraph (1)(B)(i)(I), by striking “sections 302(2) and
35 304(a) of the Homeland Security Act of 2002” and inserting “sec-
36 tions 10901(2) and 10903(a) of title 6, United States Code”; and

37 (B) in paragraph (2)(D), by striking “section 202 of the Home-
38 land Security Act of 2002” and inserting “section 10502 of title
39 6, United States Code”.

40 (3) Section 2801(a) of the Act of July 1, 1944 (42 U.S.C. 300hh(a))
41 is amended by striking “section 502(6) of the Homeland Security Act

1 of 2002” and inserting “section 11303(a)(6) of title 6, United States
2 Code”.

3 (4) Section 2802(a)(1) of the Act of July 1, 1944 (42 U.S.C.
4 300hh–1(a)(1)) is amended—

5 (A) by striking “section 504(a)(19) of the Homeland Security
6 Act of 2002” and inserting “section 11303(a)(19) of title 6,
7 United States Code”;

8 (B) by striking “section 501(7) of such Act” and inserting “sec-
9 tion 11301(7) of such title”; and

10 (C) by striking “section 504 of such Act” and inserting “section
11 11303 of such title”.

12 (5) Section 1061(d) of the Intelligence Reform and Terrorism Pre-
13 vention Act of 2004 (42 U.S.C. 2000ee(d)) is amended—

14 (A) in paragraph (1)(A), by striking “subsections (d) and (f) of
15 section 1016” and inserting “section 11908(c) and (d) of title 6,
16 United States Code”;

17 (B) in paragraph (1)(B), by striking “subsections (d) and (f)
18 of section 1016” and inserting “section 11908(c) and (d) of title
19 6, United States Code”; and

20 (C) in paragraph (2)(B), by striking “subsections (d) and (f) of
21 section 1016” and inserting “section 11908(c) and (d) of title 6,
22 United States Code.”.

23 (6) Section 303(b) of the Robert T. Stafford Disaster Relief and
24 Emergency Assistance Act (42 U.S.C. 5144(b)) is amended—

25 (A) in paragraph (1)(B), by striking “section 507 of the Home-
26 land Security Act of 2002” and inserting “section 11307 of title
27 6, United States Code”;

28 (B) in paragraph (2), by striking “section 646(a) of the Post-
29 Katrina Emergency Management Reform Act of 2006” and insert-
30 ing “section 20506(a) of title 6, United States Code”; and

31 (C) in paragraph (4), by striking “section 652(a) of the Post-
32 Katrina Emergency Management Reform Act of 2006” and insert-
33 ing “section 20512(a) of title 6, United States Code”.

34 (k) TITLE 46, UNITED STATES CODE.—Section 70105(l) of title 46,
35 United States Code, is amended by striking “section 2(1) of the SAFE Port
36 Act” and inserting “section 30101(1) of title 6”.

37 (l) TITLE 49, UNITED STATES CODE.—Title 49, United States Code, is
38 amended as follows:

39 (1) Section 46110(a) is amended by striking “this part, part B, or
40 subsection (l) or (s) of section 114” and inserting “this part or part
41 B”.

- 1 (2) Chapter 463 is amended—
2 (A) in section 46301—
3 (i) in subsection (a), by striking paragraph (4) and redesignating paragraphs (5) through (7) as paragraphs (4) through
4 (6);
5 (ii) in subsection (a)(1)(A), by striking “chapter 449 (except sections 44902, 44903(d), 44904, 44907(a)–(d)(1)(A) and (d)(1)(C)–(f), and 44908),”;
6 (iii) in subsection (a)(4)(A)(i) as redesignated by clause (i),
7 by striking “chapter 449 (except sections 44902, 44903(d), 44904, and 44907–44909),”;
8 (iv) in subsection (c)(1)(A), by striking “chapter 423, or section 44909” and inserting “or chapter 423”; and
9 (v) in subsection (f)(1)(A)(i), by striking “chapter 449 (except sections 44902, 44903(d), 44904, 44907(a)–(d)(1)(A) and (d)(1)(C)–(f), 44908, and 44909),”;
10 (B) in section 46302—
11 (i) in subsection (a), by striking “section 46502(a), 46504, 46505, or 46506” and inserting “section 46504”; and
12 (ii) in subsection (b)(1), by striking “The Secretary of Homeland Security and, for a violation relating to section 46504, the Secretary of Transportation,” and inserting “The Secretary of Transportation”;
13 (C) by striking section 46303;
14 (D) in section 46306(d)(1), by striking “Commissioner of Customs” and inserting “Commissioner of U. S. Customs and Border Protection”;
15 (E) by striking section 46314;
16 (F) in section 46316(b), by striking “chapter 447 (except section 44718(a)), and chapter 449 (except sections 44902, 44903(d), 44904, and 44907–44909)” and inserting “and chapter 447 (except section 44718(a))”; and
17 (G) in the table of contents, by striking the items relating to sections 46303 and 46314.
18 (m) TITLE 50, UNITED STATES CODE.—Title 50, United States Code,
19 is amended as follows:
20 (1) Section 1414(b) of the National Defense Authorization Act for Fiscal Year 1997 (50 U.S.C. 2314(b)) is amended by striking “section 502(6) of the Homeland Security Act of 2002 (6 U.S.C. 312(6))” and inserting “section 11303(a)(6) of title 6, United States Code”.

1 (2) Section 1415(a)(2) of the National Defense Authorization Act for
2 Fiscal Year 1997 (50 U.S.C. 2315(a)(2)) is amended by striking “sec-
3 tions 102(c) and 430(c)(1) of the Homeland Security Act of 2002 (6
4 U.S.C. 112(c), 238(c)(1))” and inserting “sections 10322(b)(1) and
5 10341(h) of title 6, United States Code”.

6 (3) Section 102A(f)(1)(B)(iii) of the Act of July 26, 1947 (50
7 U.S.C. 3024(f)(1)(B)(iii)) is amended by striking “sections 201 and
8 892 of the Homeland Security Act of 2002 (6 U.S.C. 121, 482)” and
9 inserting “sections 10501 and 11907 of title 6, United States Code”.

10 **SEC. 6. TRANSITIONAL AND SAVINGS PROVISIONS.**

11 (a) DEFINITIONS.—In this section:

12 (1) RESTATED PROVISION.—The term “restated provision” means a
13 provision of title 6, United States Code, that is enacted by section 3
14 or 4.

15 (2) SOURCE PROVISION.—The term “source provision” means a pro-
16 vision of law that is replaced by a restated provision.

17 (b) CUTOFF DATE.—The restated provisions replace certain provisions of
18 law enacted on or before June 14, 2023. If a law enacted after that date
19 amends or repeals a source provision, that law is deemed to amend or re-
20 peal, as the case may be, the corresponding restated provision. If a law en-
21 acted after that date is otherwise inconsistent with a restated provision or
22 a provision of this Act, that law supersedes the restated provision or provi-
23 sion of this Act to the extent of the inconsistency.

24 (c) ORIGINAL DATE OF ENACTMENT UNCHANGED.—A restated provision
25 is deemed to have been enacted on the date of enactment of the cor-
26 responding source provision.

27 (d) REFERENCE TO RESTATED PROVISION.—A reference to a restated
28 provision is deemed to refer to the corresponding source provision.

29 (e) REFERENCE TO SOURCE PROVISION.—A reference to a source provi-
30 sion, including a reference in a regulation, order, or other law, is deemed
31 to refer to the corresponding restated provision.

32 (f) REGULATIONS, ORDERS, AND OTHER ADMINISTRATIVE ACTIONS.—A
33 regulation, order, or other administrative action in effect under a source
34 provision continues in effect under the corresponding restated provision.

35 (g) ACTIONS TAKEN AND OFFENSES COMMITTED.—An action taken or
36 an offense committed under a source provision is deemed to have been taken
37 or committed under the corresponding restated provision.

38 **SEC. 7. REPEALS.**

39 The following provisions of law are repealed, except with respect to the
40 rights and duties that matured, penalties that were incurred, or proceedings
41 that were begun before the date of enactment of this Act:

Schedule of Laws Repealed
Statutes at Large

Act	Section	United States Code Former Classification
Act of March 3, 1927 (ch. 348)	1	19 U.S.C. 2071.
	3(b)	19 U.S.C. 2073(b).
	4	19 U.S.C. 2084.
Act of August 10, 1956 (ch. 1041)	43	6 U.S.C. 765.
Federal Fire Prevention and Control Act of 1974 (Public Law 93-498)	3	15 U.S.C. 2202.
	4	15 U.S.C. 2203.
	5	15 U.S.C. 2204.
	6	15 U.S.C. 2205.
	7	15 U.S.C. 2206.
	8	15 U.S.C. 2207.
	9	15 U.S.C. 2208.
	10	15 U.S.C. 2209.
	11	15 U.S.C. 2210.
	12	15 U.S.C. 2211.
	13	15 U.S.C. 2212.
	14	15 U.S.C. 2213.
	15	15 U.S.C. 2214.
	16	15 U.S.C. 2215.
	17	15 U.S.C. 2216.
	20	15 U.S.C. 2217.
	21	15 U.S.C. 2218.
	22	15 U.S.C. 2219.
	24	15 U.S.C. 2220.
	25	15 U.S.C. 2221.
28	15 U.S.C. 2224.	
29	15 U.S.C. 2225.	
30	15 U.S.C. 2226.	
31	15 U.S.C. 2227.	
32	15 U.S.C. 2228.	
33	15 U.S.C. 2229.	
34	15 U.S.C. 2229a.	
35	15 U.S.C. 2230.	
36	15 U.S.C. 2231.	
37	15 U.S.C. 2234.	
38	15 U.S.C. 2235.	
Customs and Trade Act of 1990 (Public Law 101-382)	113	19 U.S.C. 2082.
Hotel and Motel Fire Safety Act of 1990 (Public Law 101-391)	6	15 U.S.C. 2225a.
Firefighters' Safety Study Act (Public Law 101-446)	2	15 U.S.C. 2223a.
	3	15 U.S.C. 2223b.
	4	15 U.S.C. 2223c.
	5	15 U.S.C. 2223d.
	6	15 U.S.C. 2223e.
United States Fire Administration Au- thorization Act for Fiscal Years 1998 and 1999 (Public Law 105-108)	7(a), (b)(2)	15 U.S.C. 2218 note.
Floyd D. Spence National Defense Au- thorization Act for Fiscal Year 2001 (Public Law 106-398)	§ 1 [div. A, title XVII, § 1703]	15 U.S.C. 2232.
Aviation and Transportation Security Act (Public Law 107-71)	109	49 U.S.C. 114 note.
Homeland Security Act of 2002 (Public Law 107-296)	2	6 U.S.C. 101.
	3	6 U.S.C. 102.
	101	6 U.S.C. 111.
	102	6 U.S.C. 112.
	103	6 U.S.C. 113.
	201	6 U.S.C. 121.
	202	6 U.S.C. 122.
	203	6 U.S.C. 124.
	204	6 U.S.C. 124a.
	205	6 U.S.C. 124b.
	206	6 U.S.C. 124c.
	207	6 U.S.C. 124d.
	208	6 U.S.C. 124e.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	209	6 U.S.C. 124f.
	210	6 U.S.C. 124g.
	210A	6 U.S.C. 124h.
	210B	6 U.S.C. 124i.
	210C	6 U.S.C. 124j.
	210D	6 U.S.C. 124k.
	210E	6 U.S.C. 124m.
	210F	6 U.S.C. 124m-1.
	210G	6 U.S.C. 124n.
	221	6 U.S.C. 141.
	222	6 U.S.C. 142.
	301	6 U.S.C. 181.
	302	6 U.S.C. 182.
	303	6 U.S.C. 183.
	304	6 U.S.C. 184.
	305	6 U.S.C. 185.
	306	6 U.S.C. 186.
	307	6 U.S.C. 187.
	308	6 U.S.C. 188.
	309	6 U.S.C. 189.
	310	6 U.S.C. 190.
	311	6 U.S.C. 191.
	312	6 U.S.C. 192.
	313	6 U.S.C. 193.
	314	6 U.S.C. 195.
	315	6 U.S.C. 195a.
	316	6 U.S.C. 195b.
	317	6 U.S.C. 195e.
	318	6 U.S.C. 195d.
	319	6 U.S.C. 195e.
	320	6 U.S.C. 195f.
	321	6 U.S.C. 195g.
	322	6 U.S.C. 195h.
	323	6 U.S.C. 195i.
	402	6 U.S.C. 202.
	403	6 U.S.C. 203.
	404	6 U.S.C. 204.
	404	6 U.S.C. 205.
	411	6 U.S.C. 211.
	412	6 U.S.C. 212.
	413	6 U.S.C. 213.
	414	6 U.S.C. 214.
	415	6 U.S.C. 215.
	417	6 U.S.C. 217.
	418	6 U.S.C. 218.
	421	6 U.S.C. 231.
	422	6 U.S.C. 232.
	423	6 U.S.C. 233.
	424	6 U.S.C. 234.
	427	6 U.S.C. 235.
	428	6 U.S.C. 236.
	429	6 U.S.C. 237.
	430	6 U.S.C. 238.
	431	6 U.S.C. 239.
	432	6 U.S.C. 240.
	433	6 U.S.C. 241.
	434	6 U.S.C. 242.
	435	6 U.S.C. 243.
	436	6 U.S.C. 244.
	441	6 U.S.C. 251.
	442	6 U.S.C. 252.
	443	6 U.S.C. 253.
	444	6 U.S.C. 254.
	445	6 U.S.C. 255.
	451	6 U.S.C. 271.
	452	6 U.S.C. 272.
	453	6 U.S.C. 273.
	454	6 U.S.C. 274.
	456	6 U.S.C. 275.
	459	6 U.S.C. 276.
	460	6 U.S.C. 277.
	461	6 U.S.C. 278.
	471	6 U.S.C. 291.
	472	6 U.S.C. 292.
	473	6 U.S.C. 293.
	475	6 U.S.C. 295.
	476	6 U.S.C. 296.
	477	6 U.S.C. 297.
	478(a)	6 U.S.C. 298(a).
	481	6 U.S.C. 301.
	482	6 U.S.C. 301a.
	483	6 U.S.C. 301b.
	484	6 U.S.C. 301e.
	501	6 U.S.C. 311.
	502	6 U.S.C. 312.
	503	6 U.S.C. 313.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	504	6 U.S.C. 314.
	505	6 U.S.C. 315.
	506	6 U.S.C. 316.
	507	6 U.S.C. 317.
	508	6 U.S.C. 318.
	509	6 U.S.C. 319.
	510	6 U.S.C. 320.
	511	6 U.S.C. 321.
	512	6 U.S.C. 321a.
	513	6 U.S.C. 321b.
	514	6 U.S.C. 321e.
	515	6 U.S.C. 321d.
	517	6 U.S.C. 321f.
	518	6 U.S.C. 321g.
	519	6 U.S.C. 321h.
	521	6 U.S.C. 321j.
	522	6 U.S.C. 321k.
	523	6 U.S.C. 321l.
	524	6 U.S.C. 321m.
	525	6 U.S.C. 321n.
	526	6 U.S.C. 321o.
	527	6 U.S.C. 321p.
	528	6 U.S.C. 321q.
	529	6 U.S.C. 321r.
	701	6 U.S.C. 341.
	702	6 U.S.C. 342.
	703	6 U.S.C. 343.
	704	6 U.S.C. 344.
	705	6 U.S.C. 345.
	706	6 U.S.C. 346.
	707	6 U.S.C. 347.
	708	6 U.S.C. 348.
	709	6 U.S.C. 349.
	710	6 U.S.C. 350.
	711	6 U.S.C. 351.
	712	6 U.S.C. 352.
	713	6 U.S.C. 353.
	801	6 U.S.C. 361.
	821	6 U.S.C. 381.
	822	6 U.S.C. 383.
	831	6 U.S.C. 391.
	832	6 U.S.C. 392.
	833	6 U.S.C. 393.
	834	6 U.S.C. 394.
	835	6 U.S.C. 395.
	836	6 U.S.C. 397.
	841(b)	6 U.S.C. 411(b).
	842	6 U.S.C. 412.
	843	6 U.S.C. 413.
	844	6 U.S.C. 414.
	845	6 U.S.C. 415.
	846	6 U.S.C. 417.
	851	6 U.S.C. 421.
	852	6 U.S.C. 422.
	853	6 U.S.C. 423.
	854	6 U.S.C. 424.
	855	6 U.S.C. 425.
	856	6 U.S.C. 426.
	857	6 U.S.C. 427.
	862	6 U.S.C. 441.
	863	6 U.S.C. 442.
	864	6 U.S.C. 443.
	865	6 U.S.C. 444.
	871	6 U.S.C. 451.
	872	6 U.S.C. 452.
	873	6 U.S.C. 453.
	874	6 U.S.C. 454.
	875	6 U.S.C. 455.
	876	6 U.S.C. 456.
	877	6 U.S.C. 457.
	878	6 U.S.C. 458.
	879	6 U.S.C. 459.
	880	6 U.S.C. 460.
	881	6 U.S.C. 461.
	882	6 U.S.C. 462.
	883	6 U.S.C. 463.
	884	6 U.S.C. 464.
	885(a)	6 U.S.C. 465(a).
	887	6 U.S.C. 467.
	888	6 U.S.C. 468.
	890A	6 U.S.C. 473.
	890B	6 U.S.C. 474.
	890C	6 U.S.C. 475.
	890D	6 U.S.C. 475a.
	892(a) through (c)(1), (c)(3) through (g).	6 U.S.C. 482(a) through (c)(1), (c)(3) through (g).

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	893	6 U.S.C. 483.
	894	6 U.S.C. 484.
	895	6 U.S.C. 484a.
	899A	6 U.S.C. 488.
	899B	6 U.S.C. 488a.
	899C	6 U.S.C. 488b.
	899D	6 U.S.C. 488c.
	899E	6 U.S.C. 488d.
	899F	6 U.S.C. 488e.
	899G	6 U.S.C. 488f.
	899H	6 U.S.C. 488g.
	899I	6 U.S.C. 488h.
	899J	6 U.S.C. 488i.
	901	6 U.S.C. 491.
	902	6 U.S.C. 492.
	903	6 U.S.C. 493.
	904	6 U.S.C. 494.
	905	6 U.S.C. 495.
	906	6 U.S.C. 496.
	1001(e)(1)(A), (2)	6 U.S.C. 511(1)(A), (2).
	1006	6 U.S.C. 512.
	1333	6 U.S.C. 665a.
	1502	6 U.S.C. 542.
	1503	6 U.S.C. 543.
	1511	6 U.S.C. 551.
	1513	6 U.S.C. 553.
	1514	6 U.S.C. 554.
	1515	6 U.S.C. 555.
	1601	6 U.S.C. 561.
	1611	6 U.S.C. 563.
	1612	6 U.S.C. 563a.
	1613	6 U.S.C. 563b.
	1614	6 U.S.C. 563c.
	1615	6 U.S.C. 563d.
	1616	6 U.S.C. 563e.
	1617	6 U.S.C. 563f.
	1621	6 U.S.C. 565.
	1714	6 U.S.C. 103.
	1801	6 U.S.C. 571.
	1802	6 U.S.C. 572.
	1803	6 U.S.C. 573.
	1804	6 U.S.C. 574.
	1805	6 U.S.C. 575.
	1806	6 U.S.C. 576.
	1807	6 U.S.C. 577.
	1808	6 U.S.C. 578.
	1809	6 U.S.C. 579.
	1810	6 U.S.C. 580.
	1900	6 U.S.C. 590.
	1901	6 U.S.C. 591.
	1921	6 U.S.C. 591g.
	1922	6 U.S.C. 591h.
	1923	6 U.S.C. 592.
	1924	6 U.S.C. 593.
	1925	6 U.S.C. 594.
	1926	6 U.S.C. 596.
	1927	6 U.S.C. 596a.
	1928	6 U.S.C. 596b.
	1931	6 U.S.C. 597.
	1932	6 U.S.C. 597a.
	2001	6 U.S.C. 601.
	2002	6 U.S.C. 603.
	2003	6 U.S.C. 604.
	2004	6 U.S.C. 605.
	2005	6 U.S.C. 606.
	2006	6 U.S.C. 607.
	2007	6 U.S.C. 608.
	2008	6 U.S.C. 609.
	2009	6 U.S.C. 609a.
	2021(a), (b)	6 U.S.C. 611(a), (b).
	2022	6 U.S.C. 612.
	2023	6 U.S.C. 613.
	2101	6 U.S.C. 621.
	2102	6 U.S.C. 622.
	2103	6 U.S.C. 623.
	2104	6 U.S.C. 624.
	2105	6 U.S.C. 625.
	2106	6 U.S.C. 626.
	2107	6 U.S.C. 627.
	2108	6 U.S.C. 628.
	2109	6 U.S.C. 629.
	2200	6 U.S.C. 650.
	2201	6 U.S.C. 651.
	2202	6 U.S.C. 652.
	2203	6 U.S.C. 653.
	2204	6 U.S.C. 654.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	2205	6 U.S.C. 655.
	2206	6 U.S.C. 656.
	2207(b), (c)	6 U.S.C. 657(b), (c).
	2207(d)(2)	6 U.S.C. 657(d)(2).
	2208	6 U.S.C. 658.
	2209	6 U.S.C. 659.
	2210	6 U.S.C. 660.
	2211	6 U.S.C. 661.
	2212	6 U.S.C. 662.
	2213	6 U.S.C. 663.
	2214	6 U.S.C. 664.
	2215	6 U.S.C. 665.
	2216	6 U.S.C. 665b.
	2217	6 U.S.C. 665c.
	2218	6 U.S.C. 665d.
	2219	6 U.S.C. 665e.
	2220	6 U.S.C. 665f.
	2220A	6 U.S.C. 665g.
	2220B	6 U.S.C. 665h.
	2220C	6 U.S.C. 665i.
	2220D	6 U.S.C. 665k.
	2220E	6 U.S.C. 665n.
	2222	6 U.S.C. 671.
	2223	6 U.S.C. 672.
	2224	6 U.S.C. 673.
	2225	6 U.S.C. 674.
	2232	6 U.S.C. 677a.
	2233	6 U.S.C. 677b.
	2234	6 U.S.C. 677c.
	2235	6 U.S.C. 677d.
	2236	6 U.S.C. 677e.
	2237	6 U.S.C. 677f.
	2238	6 U.S.C. 677g.
	2240	6 U.S.C. 681.
	2241	6 U.S.C. 681a.
	2242	6 U.S.C. 681b.
	2243	6 U.S.C. 681c.
	2244	6 U.S.C. 681d.
	2245	6 U.S.C. 681e.
	2246	6 U.S.C. 681f.
Department of Homeland Security Appropriations Act, 2004 (Public Law 108–90)	(2d proviso under heading “SALARIES AND EXPENSES” under heading “FEDERAL LAW ENFORCEMENT TRAINING CENTER”, 117 Stat. 1150). (3d proviso under heading “SALARIES AND EXPENSES” under heading “FEDERAL LAW ENFORCEMENT TRAINING CENTER”, 117 Stat. 1151). (4th proviso under heading “SALARIES AND EXPENSES” UNDER HEADING “FEDERAL LAW ENFORCEMENT TRAINING CENTER”, 117 Stat. 1151). (last proviso under heading “SALARIES AND EXPENSES” under heading “FEDERAL LAW ENFORCEMENT TRAINING CENTER”, 117 Stat. 1151). 505	6 U.S.C. 464b. 6 U.S.C. 464c. 6 U.S.C. 464d. 6 U.S.C. 464e. 6 U.S.C. 453a. 6 U.S.C. 469.
Firefighting Research and Coordination Act (Public Law 108—169)	204(b)	15 U.S.C. 2206 note.
	204(c)	15 U.S.C. 2206 note.
Department of Homeland Security Appropriations Act, 2005 (Public Law 108–334)	515(b)	49 U.S.C. 44945 note.
Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458)	1016	6 U.S.C. 485.
	4016(a)	49 U.S.C. 44917 note.
	4016(e)	49 U.S.C. 44917 note.
	7215	6 U.S.C. 123.
	7303(a) through (g)	6 U.S.C. 194(a) through (g).
	7405	6 U.S.C. 112 note.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	8306	6 U.S.C. 112 note.
Department of Homeland Security Ap- propriations Act, 2006 (Public Law 109-90)	503(e)	6 U.S.C. 103 note.
	514	49 U.S.C. 114 note.
	537	6 U.S.C. 114.
	540	49 U.S.C. 114 note.
	541	6 U.S.C. 486.
USA PATRIOT Improvement and Reau- thorization Act of 2005 (Public Law 109-177)	125	15 U.S.C. 2233.
Department of Homeland Security Ap- propriations Act, 2007 (Public Law 109-295)	532	6 U.S.C. 382.
	558	6 U.S.C. 981a.
	602	6 U.S.C. 701.
	624	6 U.S.C. 711.
	632	6 U.S.C. 721.
	634	6 U.S.C. 722.
	635	6 U.S.C. 723.
	636	6 U.S.C. 724.
	637	6 U.S.C. 725.
	639	6 U.S.C. 726.
	640	6 U.S.C. 727.
	640a	6 U.S.C. 728.
	641	6 U.S.C. 741.
	642	6 U.S.C. 742.
	643	6 U.S.C. 743.
	644	6 U.S.C. 744.
	645	6 U.S.C. 745.
	646	6 U.S.C. 746.
	647	6 U.S.C. 747.
	648	6 U.S.C. 748.
	649	6 U.S.C. 749.
	650	6 U.S.C. 750.
	651	6 U.S.C. 751.
	652	6 U.S.C. 752.
	653	6 U.S.C. 753.
	654	6 U.S.C. 754.
	661	6 U.S.C. 761.
	662	6 U.S.C. 762.
	663	6 U.S.C. 763.
	664	6 U.S.C. 764.
	675	6 U.S.C. 571 note.
	682	6 U.S.C. 771.
	683	6 U.S.C. 772.
	689(a)	6 U.S.C. 773.
	689b(a), (b), (d)	6 U.S.C. 774(a), (b), (d).
	689c	6 U.S.C. 775.
	689i	6 U.S.C. 776.
	689j	6 U.S.C. 777.
	691	6 U.S.C. 791.
	693	6 U.S.C. 793.
	695	6 U.S.C. 794.
	696(a), (b)	6 U.S.C. 795.
	697	6 U.S.C. 796.
	698	6 U.S.C. 797.
	699	6 U.S.C. 811.
Security and Accountability for Every Port Act of 2006 (Public Law 109- 347)	2	6 U.S.C. 901.
	114	6 U.S.C. 912.
	115	6 U.S.C. 913.
	121	6 U.S.C. 921.
	123	6 U.S.C. 923.
	125	6 U.S.C. 924.
	126	6 U.S.C. 925.
	128	6 U.S.C. 926.
	201	6 U.S.C. 941.
	202	6 U.S.C. 942.
	203	6 U.S.C. 943.
	204	6 U.S.C. 944.
	205	6 U.S.C. 945.
	211	6 U.S.C. 961.
	212	6 U.S.C. 962.
	213	6 U.S.C. 963.
	214	6 U.S.C. 964.
	215	6 U.S.C. 965.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	216	6 U.S.C. 966.
	217	6 U.S.C. 967.
	218	6 U.S.C. 968.
	219	6 U.S.C. 969.
	220	6 U.S.C. 970.
	221	6 U.S.C. 971.
	222	6 U.S.C. 972.
	223	6 U.S.C. 973.
	231	6 U.S.C. 981.
	232	6 U.S.C. 982.
	233(a)	6 U.S.C. 983.
	236	6 U.S.C. 985.
	301(b)	6 U.S.C. 1001.
	301(c)	6 U.S.C. 239 note.
	302(e)	6 U.S.C. 1002.
	303	6 U.S.C. 1003.
	401	6 U.S.C. 115.
	502	6 U.S.C. 592a.
	612	6 U.S.C. 314a.
	702	6 U.S.C. 470.
	707	6 U.S.C. 220.
U.S. Troop Readiness, Veterans' Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007 (Public Law 110-28)	6405	6 U.S.C. 396.
Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53)	502(b)	6 U.S.C. 124a note.
	1104	6 U.S.C. 921a.
	1201	6 U.S.C. 1101.
	1203(b)	49 U.S.C. 114 note.
	1204	6 U.S.C. 1102.
	1205	6 U.S.C. 1103.
	1206	6 U.S.C. 1104.
	1301	6 U.S.C. 1111.
	1303	6 U.S.C. 1112.
	1304	6 U.S.C. 1113.
	1305	6 U.S.C. 1114.
	1306	6 U.S.C. 1115.
	1307	6 U.S.C. 1116.
	1310	6 U.S.C. 1117.
	1402	6 U.S.C. 1131.
	1404	6 U.S.C. 1133.
	1405	6 U.S.C. 1134.
	1406	6 U.S.C. 1135.
	1407	6 U.S.C. 1136.
	1408	6 U.S.C. 1137.
	1409	6 U.S.C. 1138.
	1410	6 U.S.C. 1139.
	1411	6 U.S.C. 1140.
	1412	6 U.S.C. 1141.
	1413	6 U.S.C. 1142.
	1414	6 U.S.C. 1143.
	1415	6 U.S.C. 1144.
	1501	6 U.S.C. 1151.
	1502	6 U.S.C. 1152.
	1503(b)	6 U.S.C. 1153.
	1504	6 U.S.C. 1154.
	1511	6 U.S.C. 1161.
	1512	6 U.S.C. 1162.
	1513	6 U.S.C. 1163.
	1514	6 U.S.C. 1164.
	1515	6 U.S.C. 1165.
	1516	6 U.S.C. 1166.
	1517	6 U.S.C. 1167.
	1518	6 U.S.C. 1168.
	1519	6 U.S.C. 1169.
	1522	6 U.S.C. 1170.
	1524	6 U.S.C. 1171.
	1526(b)	6 U.S.C. 1172.
	1531	6 U.S.C. 1181.
	1532	6 U.S.C. 1182.
	1533	6 U.S.C. 1183.
	1534	6 U.S.C. 1184.
	1535	6 U.S.C. 1185.
	1541	6 U.S.C. 1186.
	1551	6 U.S.C. 1201.
	1552	6 U.S.C. 1202.
	1553	6 U.S.C. 1203.
	1554	6 U.S.C. 1204.
	1555	6 U.S.C. 1205.
	1556(b)	6 U.S.C. 1206.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	1557	6 U.S.C. 1207.
	1558	6 U.S.C. 1208.
	2205	6 U.S.C. 194 note.
	2403	6 U.S.C. 121 note.
Border Infrastructure and Technology Modernization Act of 2007 (Public Law 110–161)	602	6 U.S.C. 1401.
	606	6 U.S.C. 1405.
American Recovery and Reinvestment Act of 2009 (Public Law 111–5)	604	6 U.S.C. 453b.
Department of Homeland Security Ap- propriations Act, 2010 (Public Law 111–83)	554	6 U.S.C. 469a.
Coast Guard Authorization Act of 2010 (Public Law 111–281)	825	6 U.S.C. 945 note.
Anti-Border Corruption Act of 2010 (Public Law 111–376)	3	6 U.S.C. 221.
Consolidated Appropriations Act, 2012 (Public Law 112–74)	div. D, title II, (1st proviso in paragraph under heading “CONSTRUCTION AND FACILITIES MANAGEMENT”, 125 Stat. 949). div. D, title V, § 526	6 U.S.C. 214 note. 6 U.S.C. 453c. 6 U.S.C. 190 note. 6 U.S.C. 124j note. 6 U.S.C. 222.
Border Tunnel Prevention Act of 2012 (Public Law 112–127)	8	6 U.S.C. 257.
Intelligence Authorization Act for Fiscal Year 2013 (Public Law 112–277)	501	6 U.S.C. 121a.
Department of Homeland Security Ap- propriations Act, 2013 (Public Law 113–6)	div. D, title III, 2d proviso on p. 357. div. D, title III, last proviso on p. 359. div. D, title V, § 540	6 U.S.C. 462 note. 6 U.S.C. 763a. 6 U.S.C. 416.
Department of Homeland Security Ap- propriations Act, 2014 (Public Law 113–76)	div. F, title V, § 569	6 U.S.C. 471.
Cybersecurity Workforce Assessment Act (Public Law 113–246)	2	6 U.S.C. 146 note.
	3	6 U.S.C. 146.
Protecting and Securing Chemical Facili- ties from Terrorist Attacks Act of 2014 (Public Law 113–254)	5	6 U.S.C. 621 note.
Homeland Security Cybersecurity Work- force Assessment Act (Public Law 113–277)	4(b) through (e)	6 U.S.C. 146 note.
National Cybersecurity Protection Act of 2014 (Public Law 113–282)	8	6 U.S.C. 659 note.
Intelligence Authorization Act for Fiscal Year 2015 (Public Law 113–293)	324	6 U.S.C. 125.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
Department of Homeland Security Appropriations Act, 2015 (Public Law 114-4)	562	6 U.S.C. 472.
Justice for Victims of Trafficking Act of 2015 (Public Law 114-22)	901	6 U.S.C. 641.
	902	6 U.S.C. 642.
	903	6 U.S.C. 643.
	904	6 U.S.C. 644.
	906	6 U.S.C. 645.
Department of Homeland Security Interoperable Communications Act (Public Law 114-29)	2 through 6	6 U.S.C. 194 note.
Border Jobs for Veterans Act of 2015 (Public Law 114-68)	3 through 6	6 U.S.C. 211 note.
Federal Cybersecurity Enhancement Act of 2015 (Public Law 114-113)	div. N, title I, § 102	6 U.S.C. 1501.
	div. N, title I, § 103	6 U.S.C. 1502.
	div. N, title I, § 104	6 U.S.C. 1503.
	div. N, title I, § 105	6 U.S.C. 1504.
	div. N, title I, § 106	6 U.S.C. 1505.
	div. N, title I, § 107	6 U.S.C. 1506.
	div. N, title I, § 108	6 U.S.C. 1507.
	div. N, title I, § 109	6 U.S.C. 1508.
	div. N, title I, § 110	6 U.S.C. 1509.
	div. N, title I, § 111	6 U.S.C. 1510.
	div. N, title II, § 222	6 U.S.C. 1521.
	div. N, title II, § 223(b)	6 U.S.C. 663 note.
	div. N, title II, § 224	6 U.S.C. 1522.
	div. N, title II, § 225	6 U.S.C. 1523.
	div. N, title II, § 226	6 U.S.C. 1524.
	div. N, title II, § 227	6 U.S.C. 1525.
	div. N, title IV, § 403	6 U.S.C. 1531.
	div. N, title IV, § 404	6 U.S.C. 1532.
	div. N, title IV, § 405	6 U.S.C. 1533.
U.S. Customs and Border Protection Authorization Act (Public Law 114-125)	title VIII, § 802(j)	8 U.S.C. 1185 note.
National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328)	div. A, title X, § 1086	6 U.S.C. 104.
	div. A, title X, § 1092	6 U.S.C. 223.
United States Fire Administration, AFG, and SAFER Program Reauthorization Act of 2017 (Public Law 115-98)	5	15 U.S.C. 2229 note.
	6	15 U.S.C. 2229 note.
Disaster Recovery Reform Act of 2018 (Public Law 115-254)	div. D, § 1208	6 U.S.C. 748a.
	div. D, § 1209	6 U.S.C. 721 note.
Maritime Security Improvement Act of 2018 (Public Law 115-254)	div. J, § 1803	46 U.S.C. 70102 note.
	div. J, § 1805(a)	46 U.S.C. 70112 note.
	div. J, § 1805(c)(2)	46 U.S.C. 70112 note.
TSA Modernization Act (Public Law 115-254)	div. K, § 1910	49 U.S.C. 114 note.
	div. K, § 1911	49 U.S.C. 114 note.
	div. K, § 1912	49 U.S.C. 114 note.
	div. K, § 1919	6 U.S.C. 1118.
	div. K, §§ 1926 through 1929	6 U.S.C. 1116 note.
	div. K, § 1930(a)	6 U.S.C. 1112 note.
	div. K, § 1931	49 U.S.C. 114 note.
	div. K, § 1932	49 U.S.C. 114 note.
	div. K, § 1938	49 U.S.C. 44919 note.
	div. K, § 1959(a) through (c)(4)	49 U.S.C. 44917 note.
	div. K, § 1963(i)	49 U.S.C. 44921 note.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	div. K, § 1963(j)	49 U.S.C. 44921 note.
	div. K, § 1964	49 U.S.C. 114 note.
	div. K, § 1965	49 U.S.C. 114 note.
	div. K, § 1967	49 U.S.C. 114 note.
	div. K, § 1968(a)	49 U.S.C. 114 note.
	div. K, § 1971	6 U.S.C. 1116 note.
	div. K, § 1974	6 U.S.C. 1164 note.
	div. K, § 1976	6 U.S.C. 1155.
	div. K, § 1977	6 U.S.C. 1119.
	div. K, § 1979	6 U.S.C. 982 note.
	div. K, § 1982	49 U.S.C. 114 note.
	div. K, § 1984	6 U.S.C. 1156.
	div. K, § 1986	49 U.S.C. 114 note.
	div. K, § 1987	49 U.S.C. 114 note.
	div. K, § 1988(d)	49 U.S.C. 44948 note.
Department of Homeland Security Data Framework Act of 2018 (Public Law 115-331)	2	6 U.S.C. 126.
Countering Weapons of Mass Destruction Act of 2018 (Public Law 115-387)	2(g)	6 U.S.C. 591 note.
Strengthening and Enhancing Cybercapabilities by Utilizing Risk Exposure Technology Act (Public Law 115-390)	101	6 U.S.C. 663 note.
	102	6 U.S.C. 663 note.
Trafficking Victims Protection Act of 2017 (Public Law 115-393)	403	6 U.S.C. 645a.
National Defense Authorization Act for Fiscal Year 2020 (Public Law 116-92)	div. A, title XVII, § 1756	6 U.S.C. 3210-1.
Protecting America's Food and Agriculture Act of 2019 (Public Law 116-122)	3(2), 4	6 U.S.C. 211 note.
DHS Opioid Detection Resilience Act of 2019 (Public Law 116-254)	2, 3	6 U.S.C. 211 note.
DOTGOV Online Trust in Government Act of 2020 (Public Law 116-260)	903, 904(a), (b)(1)(B), (2)(B), 907.	6 U.S.C. 665 notes.
Missing Persons and Unidentified Remains Act of 2019 (Public Law 116-277)	5	6 U.S.C. 224.
William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116283)	div. A, title III, § 363	6 U.S.C. 105.
	div. A, title III, § 364	6 U.S.C. 106.
	div. A, title XVII, § 1716(b)	6 U.S.C. 659 note.
	div. A, title XVII, § 1717(a)(2)	6 U.S.C. 665c note.
	div. A, title XVII, § 1717(a)(3)	not classified.
	div. A, title XVII, § 1717(a)(4)	6 U.S.C. 665c note.
	div. A, title XVII, § 1752	6 U.S.C. 1500.
	div. H, title XC, § 9002	6 U.S.C. 652a.
	div. H, title XCVI, § 9603	6 U.S.C. 322.
Securing America's Ports Act (Public Law 116-299)	§ 2	6 U.S.C. 211 note.
k-12 Cybersecurity Act of 2021 (Public Law 11747)	§ 3	6 U.S.C. 652 note.
National Defense Authorization Act for Fiscal Year 2022 (Public Law 11781)	div. A, title XV, § 1544	6 U.S.C. 663 note.
	div. A, title XV, § 1550	6 U.S.C. 652 note.
	div. F, title LXIV, § 6413	49 U.S.C. 114 note.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	div. F, title LXIV, § 6417	49 U.S.C. 44919 note.
	div. F, title LXIV, § 6418	6 U.S.C. 124h-1.
	div. F, title LXIV, § 6419	6 U.S.C. 1137a.
	div. F, title LXIV, § 6423(b) ..	49 U.S.C. 114 note.
Department of Homeland Security Appropriations Act, 2022 (Public Law 117103)	div. F, title V, § 538	6 U.S.C. 103a.
Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Public Law 117103)	div. Y, § 102	6 U.S.C. 665j note.
	div. Y, § 104	6 U.S.C. 681g.
	div. Y, § 105	6 U.S.C. 652 note.
	div. Y, § 106	6 U.S.C. 665j.
National Cybersecurity Preparedness Consortium Act of 2021 (Public Law 117122)	§ 2	6 U.S.C. 652 note.
Luke and Alex School Safety Act of 2022 (Public Law 117159)	div. A, title III, §§ 13303 through 13305.	6 U.S.C. 665k note.
Protecting Firefighters from Adverse Substances Act (Public Law 117248)	§ 2	6 U.S.C. 323.
Quantum Computing Cybersecurity Preparedness Act (Public Law 117260) ..	§ 3	6 U.S.C. 1526 note.
	§ 4	6 U.S.C. 1526.
James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117-263)	div. G, title LXXI, § 7103	6 U.S.C. 665l.
	div. G, title LXXI, § 7113	6 U.S.C. 112 note.
	div. G, title LXXI, § 7116(a) ..	6 U.S.C. 451 note.
	div. G, title LXXI, § 7121	6 U.S.C. 665m.
	div. G, title LXXI, § 7132	49 U.S.C. 44901 note.
	div. G, title LXXI, § 7134	6 U.S.C. 257 note.
	div. G, title LXXI, § 7135(e) ..	6 U.S.C. 216 note.
	div. G, title LXXI, § 7136	6 U.S.C. 225.
	div. G, title LXXIII, § 7302	6 U.S.C. 821.
	div. G, title LXXIII, § 7303	6 U.S.C. 822.
	div. G, title LXXIII, § 7304	6 U.S.C. 823.
	div. G, title LXXIII, § 7305	6 U.S.C. 824.
	div. G, title LXXIII, § 7309	6 U.S.C. 825.
	div. K, title CXII, § 11264	6 U.S.C. 245.
Countering Human Trafficking Act of 2021 (Public Law 117-322)	§ 5	6 U.S.C. 242b.
	§ 6	6 U.S.C. 242 note.
Abolish Trafficking Reauthorization Act of 2022 (Public Law 117-347)	title IV, § 401	6 U.S.C. 1534.
	title IV, § 406(b)	6 U.S.C. 242a note.

United States Code

Title	Section
49	114
.....	115
.....	44901
.....	44902
.....	44903
.....	44904
.....	44905
.....	44906
.....	44907
.....	44908
.....	44909
.....	44910
.....	44911
.....	44912

United States Code

Title	Section
.....	44913
.....	44914
.....	44915
.....	44916
.....	44917
.....	44918
.....	44919
.....	44920
.....	44921
.....	44922
.....	44923
.....	44924
.....	44925
.....	44926
.....	44927
.....	44928
.....	44929
.....	44931
.....	44932
.....	44933
.....	44934
.....	44935
.....	44936
.....	44937
.....	44938
.....	44939
.....	44940
.....	44941
.....	44942
.....	44943
.....	44944
.....	44945
.....	44946
.....	44947
.....	44948
.....	46501
.....	46502
.....	46503
.....	46504
.....	46505
.....	46506
.....	46507