

115TH CONGRESS
2D SESSION

H. R. 6063

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

JUNE 8, 2018

Mr. SENSENBRENNER 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,*

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

4 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.

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

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

7 (1) to enact certain existing laws relating to domestic security as
8 title 6, United States Code, “Domestic Security”; and

1 (2) to make technical amendments to improve the United States
 2 Code.

3 (b) CONFORMITY WITH ORIGINAL INTENT.—In the codification of laws
 4 by this Act, the intent is to conform to the understood policy, intent, and
 5 purpose of Congress in the original enactments, with such amendments and
 6 corrections as will remove ambiguities, contradictions, and other imperfec-
 7 tions, in accordance with section 205(c)(1) of House Resolution No. 988,
 8 93d Congress, as enacted into law by Public Law 93–554 (2 U.S.C.
 9 285b(1)).

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

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

13 **TITLE 6—DOMESTIC SECURITY**

Subtitle I—Homeland Security Organization

Chap.	Sec.
101. General	10101
103. Department of Homeland Security	10301
105. Information Analysis and Infrastructure Protection	10501
107. Science and Technology in Support of Homeland Security	10701
109. Border, Maritime, and Transportation Security	10901
111. National Emergency Management	11101
113. Transportation Security Administration	11301
115. Management	11501
117. Coordination With Other Entities	11701
119. Homeland Security Council	11901
121. Emergency Communications	12101
123. Domestic Nuclear Detection Office	12301
125. Homeland Security Grants	12501
127. Anti-Trafficking Training for Department Personnel	12701

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 priate 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).

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

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

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

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

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

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

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

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

17 (A) the United States Secret Service; and

18 (B) the Coast Guard, when operating under the direct authority
19 of the Secretary of Defense or Secretary of the Navy under section
20 3 of title 14, except that nothing in this paragraph shall affect or
21 diminish the authority and responsibilities of the Commandant of
22 the Coast Guard to command or control the Coast Guard as an
23 armed force or the authority of the Director of National Intel-
24 ligence with respect to the Coast Guard as an element of the intel-
25 ligence community (as defined under section 3 of the National Se-
26 curity Act of 1947 (50 U.S.C. 3003)).

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

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

31 (A) a county, municipality, city, town, township, local public au-
32 thority, school district, special district, intrastate district, council
33 of governments (regardless of whether the council of governments
34 is incorporated as a nonprofit corporation under State law), re-
35 gional or interstate government entity, or agency or instrumen-
36 tality of a local government;

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

39 (C) a rural community, unincorporated town or village, or other
40 public entity.

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

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

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

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

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

12 (A) involves an act that—

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

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

17 (B) appears to be intended—

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

19 (ii) to influence the policy of a government by intimidation
 20 or coercion; or

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

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

27 (20) VOLUNTARY PREPAREDNESS STANDARDS.—The term “vol-
 28 untary preparedness standards” means a common set of criteria for
 29 preparedness, disaster management, emergency management, and busi-
 30 ness continuity programs, such as the American National Standards
 31 Institute’s National Fire Protection Association Standard on Disaster/
 32 Emergency Management and Business Continuity Programs (ANSI/
 33 NFPA 1600).

34 **§ 10102. Construction; relationship to other laws**

35 (a) CONSTRUCTION; SEVERABILITY.—A provision of this subtitle held to
 36 be invalid or unenforceable by its terms, or as applied to a person or cir-
 37 cumstance, shall be construed so as to give it the maximum effect permitted
 38 by law, unless the holding shall be one of utter invalidity or unenforceability,
 39 in which event the provision shall be deemed severable from this subtitle and
 40 shall not affect the remainder of the subtitle, or the application of the provi-

1 sion to other persons not similarly situated or to other, dissimilar cir-
2 cumstances.

3 (b) RELATIONSHIP TO OTHER LAWS.—

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

11 (2) ATOMIC ENERGY ACT OF 1954.—Nothing in this subtitle shall su-
12 persede any requirement made by or under the Atomic Energy Act of
13 1954 (42 U.S.C. 2011 et seq.). Restricted data or formerly restricted
14 data shall be handled, protected, classified, downgraded, and declas-
15 sified in conformity with the Atomic Energy Act of 1954 (42 U.S.C.
16 2011 et seq.).

17 (3) STANDARDS AND TECHNOLOGY ACT.—Nothing in this subtitle
18 (or an amendment made by the Homeland Security Act of 2002 (Pub-
19 lic Law 107–296, 116 Stat. 2135)) affects the authority of the Na-
20 tional Institute of Standards and Technology or the Department of
21 Commerce relating to the development and promulgation of standards
22 or guidelines under paragraphs (1) and (2) of section 20(a) of the Na-
23 tional Institute of Standards and Technology Act (15 U.S.C. 278g-
24 3(a)(1), (2)).

25 (4) IMMIGRATION AND NATIONALITY LAW.—Nothing in the definition
26 of “United States” in section 10101 of this title or another provision
27 of this subtitle shall be construed to modify the definition of “United
28 States” for the purposes of the Immigration and Nationality Act (8
29 U.S.C. 1101 et seq.) or any other immigration or nationality law.

30 **Chapter 103—Department of Homeland**
31 **Security**

Subchapter I—Organization

Sec.

- 10301. Establishment; mission; seal.
- 10302. Secretary and other officers.
- 10303. Office of Intelligence and Analysis.
- 10304. Office of Infrastructure Protection.
- 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. Office of Emergency Communications.

- 10315. Domestic Nuclear Detection Office.
- 10316. Office of Counternarcotics Enforcement.
- 10317. Office of International Affairs.
- 10318. Office for National Capital Region Coordination.
- 10319. Office of Cargo Security Policy.
- 10320. Transportation Security Oversight Board.
- 10321. Special Assistant to the Secretary.
- 10322. Border Enforcement Security Task Force.
- 10323. Office for Domestic Preparedness.
- 10324. Social media working group.
- 10325. Office of Strategy, Policy, and Plans.

Subchapter II—Functions

- 10331. In general.
- 10332. Trade and customs revenue functions.
- 10333. Military activities.
- 10334. Sensitive Security Information.

Subchapter III—Acquisitions

- 10341. Personal services.
- 10342. Prohibition on contracts with corporate expatriates.
- 10343. Lead system integrator; financial interests.

Subchapter IV—Human Resources Management

- 10351. Establishment of human resources management system.
- 10352. Labor-management relations.
- 10353. Use of counternarcotics enforcement activities in certain employee performance appraisals.
- 10354. Compliance with laws protecting equal employment opportunity and providing whistleblower protections.
- 10355. Use of protective equipment or measures by employees.
- 10356. Homeland Security Rotation Program.
- 10357. Homeland Security Education Program.

Subchapter V—Cybersecurity

- 10371. Workforce assessment and strategy.
- 10372. Homeland Workforce Measurement Initiative.
- 10373. Recruitment and retention.

Subchapter VI—Miscellaneous Provisions

- 10381. Advisory committees.
- 10382. Use of appropriated funds.
- 10383. Reports and consultation addressing use of appropriated funds.
- 10384. Buy America requirements.
- 10385. Horse adoption program.
- 10386. Future Years Homeland Security Program.
- 10387. Federal Law Enforcement Training Centers.
- 10388. Fees.
- 10389. Reports to Committee on Commerce, Science, and Transportation.
- 10390. Annual ammunition and weaponry reports.
- 10391. Clearances.
- 10392. National identification system not authorized.
- 10393. Functions and authorities of Administrator of General Services not affected.
- 10394. Research and development pilot 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;

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

4 (E) ensure that the functions of the agencies and subdivisions
 5 in the Department that are not related directly to securing the
 6 homeland are not diminished or neglected except by a specific ex-
 7 plicit Act of Congress;

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

11 (G) ensure that the civil rights and civil liberties of persons are
 12 not diminished by efforts, activities, and programs aimed at secur-
 13 ing the homeland; and

14 (H) monitor connections between illegal drug trafficking and
 15 terrorism, coordinate efforts to sever the connections, and other-
 16 wise contribute to efforts to interdict illegal drug trafficking.

17 (2) RESPONSIBILITY FOR INVESTIGATING AND PROSECUTING TER-
 18 RORISM.—Except as specifically provided by law with respect to entities
 19 transferred to the Department under this subtitle, primary responsi-
 20 bility for investigating and prosecuting acts of terrorism shall be vested
 21 not in the Department, but rather in Federal, State, and local law en-
 22 forcement agencies with jurisdiction over the acts in question.

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

25 **§ 10302. Secretary and other officers**

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

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

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

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

37 (B) Under Secretary for Science and Technology.

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

39 (D) Administrator of the Federal Emergency Management
 40 Agency.

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

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

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

5 (H) Under Secretary responsible for overseeing critical infra-
6 structure protection, cybersecurity, and other related programs of
7 the Department.

8 (I) Not more than 12 Assistant Secretaries.

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

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

12 (2) ASSISTANT SECRETARIES.—If any of the Assistant Secretaries
13 referred to under paragraph (1)(I) is designated to be the Assistant
14 Secretary for Health Affairs, the Assistant Secretary for Legislative
15 Affairs, or the Assistant Secretary for Public Affairs, that Assistant
16 Secretary shall be appointed by the President without the advice and
17 consent of the Senate.

18 (3) ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICA-
19 TIONS.—There is in the Department an Assistant Secretary for Cyber-
20 security and Communications.

21 (4) UNITED STATES FIRE ADMINISTRATOR.—The Administrator of
22 the United States Fire Administration shall have a rank equivalent to
23 an assistant secretary of the Department.

24 (c) INSPECTOR GENERAL.—There is in the Department the Office of In-
25 spector General and an Inspector General at the head of the office, as pro-
26 vided in the Inspector General Act of 1978 (5 U.S.C. App.).

27 (d) COMMANDANT OF THE COAST GUARD.—To assist the Secretary in
28 the performance of the Secretary's functions, there is a Commandant of the
29 Coast Guard, who shall be appointed as provided in section 44 of title 14,
30 and who shall report directly to the Secretary. In addition to duties provided
31 in this subtitle and as assigned to the Commandant by the Secretary, the
32 duties of the Commandant shall include those required by section 2 of title
33 14.

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

36 (f) CHIEF MEDICAL OFFICER.—There is in the Department a Chief Med-
37 ical Officer. The Chief Medical Officer is appointed by the President. The
38 individual appointed as Chief Medical Officer shall possess a demonstrated
39 ability in and knowledge of medicine and public health.

40 (g) CHIEF HUMAN CAPITAL OFFICER.—There is in the Department a
41 Chief Human Capital Officer.

1 (h) OTHER OFFICERS.—To assist the Secretary in the performance of the
 2 Secretary's functions, there are the following officers, appointed by the
 3 President:

4 (1) Director of the Secret Service.

5 (2) Chief Information Officer.

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

7 (4) Director for Domestic Nuclear Detection.

8 (5) Any Director of a Joint Task Force under section 11508 of this
 9 title.

10 (i) ABSENCE, DISABILITY, OR VACANCY OF SECRETARY OR DEPUTY SEC-
 11 RETARY AND FURTHER ORDER OF SUCCESSION.—

12 (1) ABSENCE, DISABILITY, OR VACANCY OF SECRETARY OR DEPUTY
 13 SECRETARY.—

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

20 (B) NOTIFICATION OF VACANCIES.—The Secretary shall notify
 21 the Committee on Homeland Security and Governmental Affairs
 22 of the Senate and the Committee on Homeland Security of the
 23 House of Representatives of any vacancies that require notification
 24 under sections 3345 through 3349d of title 5.

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

28 **§ 10303. Office of Intelligence and Analysis**

29 (a) IN GENERAL.—There is in the Department the Office of Intelligence
 30 and Analysis. The Under Secretary for Intelligence and Analysis is the head
 31 of the Office. The Under Secretary is appointed by the President, by and
 32 with the advice and consent of the Senate, and serves as the Chief Intel-
 33 ligence Officer of the Department.

34 (b) HOMELAND SECURITY INTELLIGENCE PROGRAM.—The Homeland Se-
 35 curity Intelligence Program in the Department coordinates the intelligence
 36 activities of the Office of Intelligence and Analysis that serve predominantly
 37 department missions.

38 **§ 10304. Office of Infrastructure Protection**

39 There is in the Department the Office of Infrastructure Protection. The
 40 Assistant Secretary for Infrastructure Protection is the head of the Office.
 41 The Assistant Secretary is appointed by the President.

1 **§ 10305. Directorate of Science and Technology**

2 There is in the Department the Directorate of Science and Technology.
3 The Under Secretary for Science and Technology is the head of the Direc-
4 torate.

5 **§ 10306. U.S. Customs and Border Protection**

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

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

12 (c) COMMISSIONER.—

13 (1) HEAD OF U.S. CUSTOMS AND BORDER PROTECTION.—The Com-
14 missioner of U.S. Customs and Border Protection (in this section re-
15 ferred to as the “Commissioner”) is the head of U.S. Customs and
16 Border Protection.

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

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

24 (e) U.S. BORDER PATROL.—

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

27 (2) CHIEF.—The Chief of the U.S. Border Patrol is the head of the
28 U.S. Border Patrol. The Chief of the U.S. Border Patrol shall report
29 to the Commissioner.

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

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

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

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

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

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

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

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

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

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

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

16 (D) administer the Air and Marine Operations Center; and

17 (E) carry out other duties and powers the Commissioner pre-
18 scribes.

19 (4) AIR AND MARINE OPERATIONS CENTER.—

20 (A) IN GENERAL.—There is in the Office of Air and Marine Op-
21 erations an Air and Marine Operations Center.

22 (B) EXECUTIVE DIRECTOR.—The Executive Director is the
23 head of the Air and Marine Operations Center. The Executive Di-
24 rector shall report to the Assistant Commissioner of the Office of
25 Air and Marine Operations.

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

27 (i) manage the air and maritime domain awareness of the
28 Department;

29 (ii) monitor and coordinate the airspace for Unmanned
30 Aerial Systems operations of the Office of Air and Marine
31 Operations;

32 (iii) detect, identify, and coordinate a response to threats
33 to national security in the air domain;

34 (iv) provide aviation and marine support to other Federal,
35 State, tribal, and local agencies; and

36 (v) carry out other duties and powers prescribed by the As-
37 sistant Commissioner.

38 (g) OFFICE OF FIELD OPERATIONS.—

39 (1) IN GENERAL.—There is in U.S. Customs and Border Protection
40 an Office of Field Operations.

1 (2) EXECUTIVE ASSISTANT COMMISSIONER.—An Executive Assistant
2 Commissioner is the head of the Office of Field Operations. The Execu-
3 tive Assistant Commissioner shall report to the Commissioner.

4 (3) DUTIES.—The Office of Field Operations shall coordinate the en-
5 forcement activities of U.S. Customs and Border Protection at United
6 States air, land, and sea ports of entry to—

7 (A) deter and prevent terrorists and terrorist weapons from en-
8 tering the United States at those ports of entry;

9 (B) conduct inspections at those ports of entry to safeguard the
10 United States from terrorism and illegal entry of persons;

11 (C) prevent illicit drugs, agricultural pests, and contraband
12 from entering the United States;

13 (D) in coordination with the Commissioner, facilitate and expe-
14 dited the flow of legitimate travelers and trade;

15 (E) administer the National Targeting Center;

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

19 (G) carry out other duties and powers the Commissioner pre-
20 scribes.

21 (4) NATIONAL TARGETING CENTER.—

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

24 (B) EXECUTIVE DIRECTOR.—An Executive Director is the head
25 of the National Targeting Center. The Executive Director shall re-
26 port to the Executive Assistant Commissioner of the Office of
27 Field Operations.

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

29 (i) serve as the primary forum for targeting operations in
30 U.S. Customs and Border Protection to collect and analyze
31 traveler and cargo information in advance of arrival in the
32 United States;

33 (ii) identify, review, and target travelers and cargo for ex-
34 amination;

35 (iii) coordinate the examination of entry and exit of trav-
36 elers and cargo;

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

39 (v) coordinate with the Transportation Security Adminis-
40 tration, as appropriate;

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

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

6 (5) ANNUAL REPORT ON STAFFING.—

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

14 (B) FORM.—The report required under subparagraph (A) shall,
 15 to the greatest extent practicable, be submitted in unclassified
 16 form, but may be submitted in classified form, if the Executive As-
 17 sistant Commissioner determines that a classified form is appro-
 18 priate and informs the Committee on Homeland Security and the
 19 Committee on Ways and Means of the House of Representatives
 20 and the Committee on Homeland Security and Governmental Af-
 21 fairs and the Committee on Finance of the Senate of the rea-
 22 soning for a classified report.

23 (h) OFFICE OF INTELLIGENCE.—

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

26 (2) ASSISTANT COMMISSIONER.—An Assistant Commissioner is the
 27 head of the Office of Intelligence. The Assistant Commissioner shall re-
 28 port to the Commissioner.

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

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

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

35 (C) establish, in coordination with the Chief Intelligence Officer
 36 of the Department, as appropriate, intelligence-sharing relation-
 37 ships with Federal, State, local, and tribal agencies and intel-
 38 ligence agencies;

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

1 (E) carry out other duties and powers the Commissioner pre-
2 scribes.

3 (i) OFFICE OF INTERNATIONAL AFFAIRS.—

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

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

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

11 (A) coordinate and support U.S. Customs and Border Protec-
12 tion’s foreign initiatives, policies, programs, and activities;

13 (B) coordinate and support U.S. Customs and Border Protec-
14 tion’s personnel stationed abroad;

15 (C) maintain partnerships and information sharing agreements
16 and arrangements with foreign governments, international organi-
17 zations, and United States agencies in support of U.S. Customs
18 and Border Protection duties and responsibilities;

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

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

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

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

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

32 (I) advise the Commissioner regarding international agreements
33 to which the United States is a party as the agreements relate to
34 the policies and procedures of U.S. Customs and Border Protec-
35 tion; and

36 (J) carry out other duties and powers the Commissioner pre-
37 scribes.

38 (j) OFFICE OF PROFESSIONAL RESPONSIBILITY.—

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

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

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

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

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

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

13 (D) carry out other duties and powers the Commissioner pre-
14 scribes.

15 (k) OFFICE OF TRADE.—

16 (1) DEFINITIONS.—In this subsection, the terms “customs and trade
17 laws of the United States”, “trade enforcement”, and “trade facilita-
18 tion” have the meanings given the terms in section 2 of the Trade Fa-
19 cilitation and Trade Enforcement Act of 2015 (19 U.S.C. 4301).

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

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

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

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

29 (B) advise the Commissioner with respect to the impact on
30 trade facilitation and trade enforcement of any policy or regulation
31 otherwise proposed or administered by U.S. Customs and Border
32 Protection;

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

38 (D) direct the development and implementation of matters relat-
39 ing to the priority trade issues identified by the Commissioner in
40 the joint strategic plan on trade facilitation and trade enforcement

1 required under section 105 of the Trade Facilitation and Trade
2 Enforcement Act of 2015 (19 U.S.C. 4314);

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

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

7 (G) oversee the trade modernization activities of U.S. Customs
8 and Border Protection, including the development and implemen-
9 tation of the Automated Commercial Environment computer sys-
10 tem authorized under section 13031(f)(5) of the Consolidated Om-
11 nibus Budget and Reconciliation Act of 1985 (19 U.S.C.
12 58c(f)(5)) and support for the establishment of the International
13 Trade Data System under the oversight of the Department of
14 Treasury pursuant to section 411(d) of the Tariff Act of 1930 (19
15 U.S.C. 1411(d));

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

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

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

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

27 (5) TRANSFER OF ASSETS, FUNCTIONS, AND PERSONNEL.—The
28 Commissioner may transfer any assets, functions, or personnel in U.S.
29 Customs and Border Protection to the Office of Trade. Not less than
30 90 days prior to the transfer, the Commissioner shall notify the Com-
31 mittee on Finance of the Senate, the Committee on Homeland Security
32 and Government Affairs of the Senate, the Committee on Ways and
33 Means of the House of Representatives, and the Committee on Home-
34 land Security of the House of Representatives of the specific assets,
35 functions, or personnel to be transferred, and the reason for the trans-
36 fer.

37 (l) OTHER AUTHORITIES.—

38 (1) IN GENERAL.—The Secretary may establish such other offices or
39 positions of Assistant Commissioners (or other similar officers or offi-
40 cials) as the Secretary determines necessary to carry out the missions,

1 duties, functions, and authorities of U.S. Customs and Border Protec-
2 tion.

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

8 (3) OTHER FEDERAL AGENCIES.—Nothing in paragraphs (1) and (2)
9 and subsections (a) through (h) may be construed as affecting in any
10 manner the authority, existing on February 23, 2016, of any other
11 Federal agency or component of the Department.

12 **§ 10307. U. S. Immigration and Customs Enforcement**

13 There is in the Department an agency known as U.S. Immigration and
14 Customs Enforcement. The Director of Immigration and Customs Enforce-
15 ment is the head of U.S. Immigration and Customs Enforcement. The Di-
16 rector reports directly to the Secretary and shall have a minimum of 5 years
17 professional experience in law enforcement and a minimum of 5 years of
18 management experience.

19 **§ 10308. U.S. Citizenship and Immigration Services**

20 There is in the Department an agency known as U.S. Citizenship and Im-
21 migration Services. The Director of U.S. Citizenship and Immigration Serv-
22 ices is the head of U.S. Citizenship and Immigration Services. The Director
23 of U.S. Citizenship and Immigration Services reports directly to the Deputy
24 Secretary of Homeland Security, shall have a minimum of 5 years of man-
25 agement experience, and shall be paid at the same level as the Director of
26 Immigration and Customs Enforcement.

27 **§ 10309. Federal Emergency Management Agency**

28 (a) ESTABLISHMENT.—There is in the Department the Federal Emer-
29 gency Management Agency. The Federal Emergency Management Agency
30 is a distinct entity in the Department.

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

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

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

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

1 **§ 10310. Transportation Security Administration**

2 (a) ESTABLISHMENT.—The Transportation Security Administration is a
3 distinct entity in the Department.

4 (b) ADMINISTRATOR.—

5 (1) IN GENERAL.—The Administrator of the Transportation Security
6 Administration is the head of the Administration. The Administrator
7 shall be appointed by the President, by and with the advice and consent
8 of the Senate. The Administrator shall be a citizen of the United States
9 and have experience in a field directly related to transportation or secu-
10 rity.

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

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

17 **§ 10311. United States Secret Service**

18 (a) IN GENERAL.—The United States Secret Service is a distinct entity
19 in the Department. The Secretary succeeds to the functions, personnel, as-
20 sets, and obligations of the Secret Service, including the functions of the
21 Secretary of the Treasury relating to the Secret Service.

22 (b) USE OF PROCEEDS DERIVED FROM CRIMINAL INVESTIGATIONS.—

23 (1) IN GENERAL.—With respect to any undercover investigative oper-
24 ation of the United States Secret Service that is necessary for the de-
25 tection and prosecution of crimes against the United States—

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

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

40 (C) sums appropriated for the Secret Service, including unobli-
41 gated balances available from prior fiscal years and the proceeds

1 from the undercover operation, may be deposited in banks or other
2 financial institutions, without regard to section 648 of title 18 and
3 section 3302 of title 31; and

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

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

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

19 (4) REPORTING AND DEPOSIT OF PROCEEDS ON DISPOSITION OF
20 CERTAIN BUSINESS ENTITIES.—If a corporation or business entity es-
21 tablished or acquired as part of an undercover investigative operation
22 under paragraph (2) with a net value of over \$50,000 is to be liq-
23 uidated, sold, or otherwise disposed of, the Secret Service, as much in
24 advance as the Director or designee determines is practicable, shall re-
25 port the circumstance to the Secretary. The proceeds of the liquidation,
26 sale, or other disposition, after obligations are met, shall be deposited
27 in the Treasury as miscellaneous receipts.

28 (5) FINANCIAL AUDITS AND REPORTS.—

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

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

1 **§ 10312. Coast Guard**

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

5 (b) TRANSFER.—

6 (1) IN GENERAL.—The authorities, functions, personnel, and assets
7 of the Coast Guard, including the authorities and functions of the Sec-
8 retary of Transportation relating to the Coast Guard, are transferred
9 to the Secretary. Notwithstanding any other provision of this subtitle,
10 the authorities, functions, and capabilities of the Coast Guard to per-
11 form its missions shall be maintained intact and without significant re-
12 duction, except as specified in Acts subsequent to the Homeland Secu-
13 rity Act of 2002 (Public Law 107–296, 116 Stat. 2135).

14 (2) CERTAIN TRANSFERS PROHIBITED.—No mission, function, or
15 asset (including for purposes of this paragraph a ship, aircraft, or heli-
16 copter) of the Coast Guard may be diverted to the principal and con-
17 tinuing use of another organization, unit, or entity of the Department,
18 except for details or assignments that do not reduce the Coast Guard’s
19 capability to perform its missions.

20 (c) CHANGES TO MISSIONS.—

21 (1) PROHIBITION.—The Secretary may not substantially or signifi-
22 cantly reduce the missions of the Coast Guard or the Coast Guard’s
23 capability to perform those missions, except as specified in Acts subse-
24 quent to the Homeland Security Act of 2002 (Public Law 107–296,
25 116 Stat. 2135).

26 (2) WAIVER.—The Secretary may waive the restrictions under para-
27 graph (1) for a period of not to exceed 90 days upon a declaration and
28 certification by the Secretary to Congress that a clear, compelling, and
29 immediate need exists for a waiver. A certification under this para-
30 graph shall include a detailed justification for the declaration and cer-
31 tification, including the reasons and specific information that dem-
32 onstrate that the Nation and the Coast Guard cannot respond effec-
33 tively if the restrictions under paragraph (1) are not waived.

34 (d) NONAPPLICABILITY TO OPERATION AS A SERVICE IN THE NAVY.—
35 None of the conditions and restrictions in this section shall apply when the
36 Coast Guard operates as a service in the Navy under section 3 of title 14.

37 **§ 10313. Office for State and Local Government Coordina-**
38 **tion**

39 There is in the Office of the Secretary the Office for State and Local
40 Government Coordination.

1 **§ 10314. Office of Emergency Communications**

2 There is in the Department the Office of Emergency Communications.
3 The Director for Emergency Communications is the head of the Office. The
4 Director reports to the Assistant Secretary for Cybersecurity and Commu-
5 nications.

6 **§ 10315. Domestic Nuclear Detection Office**

7 There is in the Department the Domestic Nuclear Detection Office. The
8 Director for Domestic Nuclear Detection is the head of the Office. The Di-
9 rector is appointed by the President.

10 **§ 10316. Office of Counternarcotics Enforcement**

11 (a) OFFICE.—There is in the Department the Office of Counternarcotics
12 Enforcement. The Director is the head of the Office. The Director is ap-
13 pointed by the President.

14 (b) ASSIGNMENT OF PERSONNEL.—

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

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

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

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

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

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

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

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

40 (5) to be a representative of the Department on all task forces, com-
41 mittees, or other entities whose purpose is to coordinate the counter-

1 narcotics enforcement activities of the Department and other Federal,
2 State or local agencies.

3 (e) SAVINGS CLAUSE.—Nothing in this section shall be construed to au-
4 thorize direct control of the operations conducted by the Directorate of Bor-
5 der and Transportation Security, the Coast Guard, or joint terrorism task
6 forces.

7 (f) REPORTS TO CONGRESS.—

8 (1) ANNUAL BUDGET REVIEW.—The Director of the Office of Coun-
9 ternarcotics Enforcement shall, not later than 30 days after the sub-
10 mission by the President to Congress of a request for expenditures for
11 the Department, submit to the Committees on Appropriations and the
12 authorizing committees of jurisdiction of the House of Representatives
13 and the Senate a review and evaluation of the request. The review and
14 evaluation shall—

15 (A) identify a request or subpart of a request that affects or
16 may affect the counternarcotics activities of the Department or its
17 subdivisions, or that affects the ability of the Department or a
18 subdivision of the Department to meet its responsibility to stop
19 the entry of illegal drugs into the United States;

20 (B) describe with particularity how requested funds would be or
21 could be expended in furtherance of counternarcotics activities;
22 and

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

25 (2) EVALUATION OF COUNTERNARCOTICS ACTIVITIES.—The Director
26 of the Office of Counternarcotics Enforcement shall, not later than
27 February 1 each year, submit to the Committees on Appropriations
28 and the authorizing committees of jurisdiction of the House of Rep-
29 resentatives and the Senate a review and evaluation of the counter-
30 narcotics activities of the Department for the previous fiscal year. The
31 review and evaluation shall—

32 (A) describe the counternarcotics activities of the Department
33 and each subdivision of the Department (whether individually or
34 in cooperation with other subdivisions of the Department, or in co-
35 operation with other branches of the Federal Government or with
36 State or local agencies), including the methods, procedures, and
37 systems (including computer systems) for collecting, analyzing,
38 sharing, and disseminating information concerning narcotics activ-
39 ity within the Department and between the Department and other
40 Federal, State, and local agencies;

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

3 (C) state whether those activities were sufficient to meet the re-
4 sponsibility of the Department to stop the entry of illegal drugs
5 into the United States, including a description of the performance
6 measures of effectiveness that were used in making that deter-
7 mination; and

8 (D) recommend, where appropriate, changes to those activities
9 to improve the performance of the Department in meeting its re-
10 sponsibility to stop the entry of illegal drugs into the United
11 States.

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

20 **§ 10317. Office of International Affairs**

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

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

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

30 (A) Exchange of information on research and development on
31 homeland security technologies.

32 (B) Joint training exercises of first responders.

33 (C) Exchange of expertise on terrorism prevention, response,
34 and crisis management.

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

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

1 (4) To manage international activities in the Department in coordi-
2 nation with other Federal officials responsible for counterterrorism
3 matters.

4 **§ 10318. Office for National Capital Region Coordination**

5 There is in the Office of the Secretary the Office of National Capital Re-
6 gion Coordination. The Director is the head of the Office. The Director is
7 appointed by the Secretary.

8 **§ 10319. Office of Cargo Security Policy**

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

12 **§ 10320. Transportation Security Oversight Board**

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

15 (b) MEMBERSHIP.—

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

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

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

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

21 (D) The Secretary of Defense, or the Secretary of Defense’s
22 designee.

23 (E) The Secretary of the Treasury, or the Secretary of the
24 Treasury’s designee.

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

27 (G) One member appointed by the President to represent the
28 National Security Council.

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

30 (c) DUTIES.—The Board shall—

31 (1) review and ratify or disapprove a regulation or security directive
32 issued by the Administrator of the Transportation Security Administra-
33 tion under section 11307(b) of this title within 30 days after the date
34 of issuance of the regulation or directive;

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

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

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

4 (5) review plans for transportation security;

5 (6) make recommendations to the Under Secretary regarding mat-
6 ters reviewed under paragraph (5).

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

8 (e) CONSIDERATION OF SECURITY INFORMATION.—A majority of the
9 Board may vote to close a meeting of the Board to the public, except that
10 meetings shall be closed to the public whenever classified, sensitive security
11 information, or information protected under section 40119(b) of title 49,
12 will be discussed.

13 **§ 10321. Special Assistant to the Secretary**

14 The Secretary shall appoint a Special Assistant to the Secretary. The
15 Special Assistant is responsible for—

16 (1) creating and fostering strategic communications with the private
17 sector to enhance the primary mission of the Department to protect the
18 American homeland;

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

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

24 (4) creating and managing private-sector advisory councils composed
25 of representatives of industries and associations designated by the Sec-
26 retary to—

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

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

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

34 (i) promoting voluntary preparedness standards to the pri-
35 vate sector; and

36 (ii) assisting the private sector in adopting voluntary pre-
37 paredness standards;

38 (5) working with Federal laboratories, federally funded research and
39 development centers, other federally funded organizations, academia,
40 and the private sector to develop innovative approaches to address

1 homeland security challenges to produce and deploy the best available
2 technologies for homeland security missions;

3 (6) promoting existing public-private partnerships and developing
4 new public-private partnerships to provide for collaboration and mutual
5 support to address homeland security challenges;

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

8 (8) providing information to the private sector regarding voluntary
9 preparedness standards and the business justification for preparedness
10 and promoting to the private sector the adoption of voluntary prepared-
11 ness standards;

12 (9) coordinating industry efforts, with respect to functions of the De-
13 partment, to identify private-sector resources and capabilities that
14 could be effective in supplementing Federal, State, and local govern-
15 ment agency efforts to prevent or respond to a terrorist attack;

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

20 (11) consulting with the Office for State and Local Government Co-
21 ordination on all matters of concern to the private sector, including the
22 tourism industry.

23 **§ 10322. Border Enforcement Security Task Force**

24 There is in the Department the Border Enforcement Security Task
25 Force.

26 **§ 10323. Office for Domestic Preparedness**

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

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

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

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

40 (3) directing and supervising terrorism preparedness grant programs
41 of the Federal Government (other than those programs administered by

1 the Department of Health and Human Services) for all emergency re-
 2 sponse providers;

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

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

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

14 (7) assisting and supporting the Secretary, in coordination with
 15 other Directorates and entities outside the Department, in conducting
 16 appropriate risk analysis and risk management activities of State, local,
 17 and tribal governments consistent with the mission and functions of the
 18 Department;

19 (8) administering those elements of the Office of National Prepared-
 20 ness of the Federal Emergency Management Agency that relate to ter-
 21 rorism, which shall be consolidated in the Department in the Office for
 22 Domestic Preparedness; and

23 (9) helping to ensure the acquisition of interoperable communication
 24 technology by State and local governments and emergency response
 25 providers.

26 **§ 10324. Social media working group**

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

29 (b) PURPOSE.—To enhance the dissemination of information through so-
 30 cial media technologies between the Department and appropriate stake-
 31 holders and to improve use of social media technologies in support of pre-
 32 paredness, response, and recovery, the Group shall identify, and provide
 33 guidance and best practices to the emergency preparedness and response
 34 community on, the use of social media technologies before, during, and after
 35 a natural disaster or an act of terrorism or other man-made disaster.

36 (c) MEMBERSHIP.—

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

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

1 (B) The Office of the Chief Information Officer of the Depart-
2 ment.

3 (C) The Privacy Office of the Department.

4 (D) The Federal Emergency Management Agency.

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

7 (F) The American Red Cross.

8 (G) The Forest Service.

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

10 (I) The United States Geological Survey.

11 (J) The National Oceanic and Atmospheric Administration.

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

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

17 (B) include—

18 (i) not fewer than 3 representatives from the private sector;
19 and

20 (ii) representatives from—

21 (I) State, local, tribal, and territorial entities, includ-
22 ing from—

23 (aa) law enforcement;

24 (bb) fire services;

25 (cc) emergency management; and

26 (dd) public health entities;

27 (II) universities and academia; and

28 (III) nonprofit disaster relief organizations.

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

31 (d) CHAIRPERSON AND CO-CHAIRPERSON.—

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

34 (2) Co-chairperson.—The chairperson shall designate, on a rotating
35 basis, a representative from a State or local government who is a mem-
36 ber of the Group to serve as the co-chairperson of the Group.

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

40 (f) MEETINGS.—

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

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

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

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

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

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

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

16 (3) Recommendations to improve the Department’s use of social
17 media technologies for emergency management purposes.

18 (4) Recommendations to improve public awareness of—

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

22 (B) how to access the information.

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

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

29 (h) TERMINATION AND RENEWAL.—

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

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

1 **§ 10325. Office of Strategy, Policy, and Plans**

2 (a) ESTABLISHMENT.—There is in the Department an Office of Strategy,
3 Policy, and Plans. The Under Secretary for Strategy, Policy, and Plans is
4 the head of the Office. The Under Secretary is appointed by the President,
5 by and with the advice and consent of the Senate.

6 (b) DEPUTY UNDER SECRETARY.—

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

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

11 (B) POLITICAL APPOINTEE.—The term “political employee”
12 means an employee who occupies a position that has been excepted
13 from the competitive service by reason of its confidential policy-
14 determining, policy-making, or policy-advocating character.

15 (2) ESTABLISHMENT.—The Secretary may—

16 (A) establish in the Office of Strategy, Policy, and Plans a posi-
17 tion of Deputy Under Secretary to support the Under Secretary
18 for Strategy, Policy, and Plans in carry out the Under Secretary’s
19 responsibilities; and

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

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

25 **Subchapter II—Functions**

26 **§ 10331. In general**

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

30 (b) REORGANIZATION.—

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

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

1 (c) PERFORMANCE OF FUNCTIONS.—Subject to the provisions of this
 2 subtitle, every officer of the Department shall perform the functions speci-
 3 fied by law for the official’s office or prescribed by the Secretary.

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

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

8 (1) except as otherwise provided by this subtitle, may delegate any
 9 of the Secretary’s functions to an officer, employee, or organizational
 10 unit of the Department;

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

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

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

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

28 (6) has the same authorities that the Secretary of Transportation
 29 has with respect to the Department of Transportation under section
 30 324 of title 49.

31 (f) REGULATORY AUTHORITY.—

32 (1) VESTING AND TRANSFER OF AUTHORITY.—Except as otherwise
 33 provided in sections 10622(c) and 10705(c) of this title and section
 34 1315(c) of title 40, this subtitle—

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

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

39 (i) existed on November 25, 2002, in an agency, program,
 40 or function transferred to the Department pursuant to the

1 Homeland Security Act of 2002 (Public Law 107–296, 116
2 Stat. 2135); or

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

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

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

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

23 (h) COORDINATION WITH NON-FEDERAL ENTITIES.—With respect to
24 homeland security, the Secretary shall coordinate through the Office for
25 State and Local Government Coordination (including the provision of train-
26 ing and equipment) with State and local government personnel, agencies,
27 and authorities, with the private sector, and with other entities, including
28 by—

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

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

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

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

1 (j) ISSUANCE OF REGULATIONS.—The issuance of regulations by the Sec-
 2 retary shall be governed by the provisions of chapter 5 of title 5, except as
 3 specifically provided in this subtitle, in laws granting regulatory authorities
 4 that are transferred by this subtitle, and in laws enacted after November
 5 25, 2002.

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

10 **§ 10332. Trade and customs revenue functions**

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

14 (b) TRADE AND CUSTOMS REVENUE FUNCTIONS.—

15 (1) DESIGNATION OF APPROPRIATE OFFICIAL.—The Secretary shall
 16 designate an appropriate senior official in the Office of the Secretary
 17 who shall—

18 (A) ensure that the trade and customs revenue functions of the
 19 Department are coordinated within the Department and with
 20 other Federal departments and agencies, and that the impact on
 21 legitimate trade is taken into account in an action impacting the
 22 functions; and

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

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

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

35 (B) coordinate the development of Department-wide policies re-
 36 garding trade and customs revenue functions and trade facilita-
 37 tion; and

38 (C) coordinate the trade and customs revenue-related policies of
 39 the Department with the policies of other Federal departments
 40 and agencies.

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

1 (1) BUSINESS COMMUNITY CONSULTATIONS.—The Secretary shall
2 consult with representatives of the business community involved in
3 international trade, including seeking the advice and recommendations
4 of the Commercial Operations Advisory Committee, on Department
5 policies and actions that have a significant impact on international
6 trade and customs revenue functions.

7 (2) CONGRESSIONAL CONSULTATION AND NOTIFICATION.—

8 (A) IN GENERAL.—Subject to subparagraph (B), the Secretary
9 shall notify the appropriate congressional committees not later
10 than 30 days prior to the finalization of Department policies, ini-
11 tiatives, or actions that will have a major impact on trade and cus-
12 toms revenue functions. The notifications shall include a descrip-
13 tion of the proposed policies, initiatives, or actions and any com-
14 ments or recommendations provided by the Commercial Operations
15 Advisory Committee and other relevant groups regarding the pro-
16 posed policies, initiatives, or actions.

17 (B) EXCEPTION.—If the Secretary determines that it is impor-
18 tant to the national security interest of the United States to final-
19 ize any Department policies, initiatives, or actions prior to the
20 consultation described in subparagraph (A), the Secretary shall—

21 (i) notify and provide any recommendations of the Com-
22 mercial Operations Advisory Committee received to the appro-
23 priate congressional committees not later than 45 days after
24 the date on which the policies, initiatives, or actions are final-
25 ized; and

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

29 (d) NOTIFICATION OF REORGANIZATION OF CUSTOMS REVENUE FUNC-
30 TIONS.—

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

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

1 (B) an explanation of how the reorganization meets the require-
 2 ments of section 10912(b) of this title that the Department not
 3 diminish the customs revenue and trade facilitation functions for-
 4 merly performed by the United States Customs Service; and

5 (C) any comments or recommendations provided by the Com-
 6 mercial Operations Advisory Committee regarding the reorganiza-
 7 tion.

8 (2) ANALYSIS.—A congressional committee referred to in paragraph
 9 (1) may request that the Commercial Operations Advisory Committee
 10 provide a report to the committee analyzing the impact of the reorga-
 11 nization and providing any recommendations for modifying the reorga-
 12 nization.

13 (3) REPORT.—Not later than 1 year after a reorganization referred
 14 to in paragraph (1) takes place, the Secretary, in consultation with the
 15 Commercial Operations Advisory Committee, shall submit a report to
 16 the Committee on Finance of the Senate and the Committee on Ways
 17 and Means of the House of Representatives. The report shall include
 18 an assessment of the impact of, and any suggested modifications to,
 19 the reorganization.

20 **§ 10333. Military activities**

21 Nothing in this subtitle shall confer upon the Secretary authority to en-
 22 gage in warfighting, the military defense of the United States, or other mili-
 23 tary activities, nor shall anything in this subtitle limit the existing authority
 24 of the Department of Defense or the armed forces to engage in warfighting,
 25 the military defense of the United States, or other military activities.

26 **§ 10334. Sensitive Security Information**

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

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

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

38 (1) IN GENERAL.—The Secretary shall promulgate guidance that in-
 39 cludes common but extensive examples of SSI that further define the
 40 individual categories of information cited under 49 CFR 1520(b)(1)

1 through (16) and that eliminates judgment by covered individuals in
2 the application of the SSI marking.

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

6 **Subchapter III—Acquisitions**

7 **§ 10341. Personal services**

8 The Secretary—

9 (1) may procure the temporary or intermittent services of experts or
10 consultants (or organizations thereof) under section 3109 of title 5;
11 and

12 (2) may, whenever necessary due to an urgent homeland security
13 need, procure temporary (not to exceed 1 year) or intermittent personal
14 services, including the services of experts or consultants (or organiza-
15 tions thereof), without regard to the pay limitations of section 3109.

16 **§ 10342. Prohibition on contracts with corporate expatriates**

17 (a) DEFINITIONS AND SPECIAL RULES.—

18 (1) DEFINITIONS.—In this section:

19 (A) DOMESTIC.—The term “domestic” has the meaning given
20 the term in section 7701(a)(4) of the Internal Revenue Code of
21 1986 (26 U.S.C. 7701(a)(4)).

22 (B) EXPANDED AFFILIATED GROUP.—The term “expanded af-
23 filiated group” means an affiliated group as defined in section
24 1504(a) of the Internal Revenue Code of 1986 (26 U.S.C.
25 1504(a)) (without regard to section 1504(b) of the Code (26
26 U.S.C. 1504(b))), except that section 1504 of the Code (26 U.S.C.
27 1504) shall be applied by substituting “more than 50 percent” for
28 “at least 80 percent” each place it appears.

29 (C) FOREIGN.—The term “foreign” has the meaning given the
30 term in section 7701(a)(5) of the Internal Revenue Code of 1986
31 (26 U.S.C. 7701(a)(5)).

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

36 (E) PERSON.—The term “person” has the meaning given the
37 term in section 7701(a)(1) of the Internal Revenue Code of 1986
38 (26 U.S.C. 7701(a)(1)).

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

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

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

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

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

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

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

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

26 (i) treat warrants, options, contracts to acquire stock, con-
 27 vertible debt instruments, and other similar interests as stock;
 28 and

29 (ii) treat stock as not stock.

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

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

36 (1) the entity completes before, on, or after November 25, 2002, the
 37 direct or indirect acquisition of substantially all of the properties held
 38 directly or indirectly by a domestic corporation or substantially all of
 39 the properties constituting a trade or business of a domestic partner-
 40 ship;

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

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

6 (B) in the case of an acquisition with respect to a domestic
7 partnership, by former partners of the domestic partnership by
8 reason of holding a capital or profits interest in the domestic part-
9 nership; and

10 (3) the expanded affiliated group which after the acquisition includes
11 the entity does not have substantial business activities in the foreign
12 country in which or under the law of which the entity is created or or-
13 ganized when compared to the total business activities of the expanded
14 affiliated group.

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

18 **§ 10343. Lead system integrator; financial interests**

19 (a) IN GENERAL.—With respect to contracts entered into after July 1,
20 2007, and except as provided in subsection (b), no entity performing lead
21 system integrator functions in the acquisition of a major system by the De-
22 partment may have a direct financial interest in the development or con-
23 struction of an individual system or element of a system of systems.

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

27 (1) the Secretary certifies to the Committees on Appropriations of
28 the Senate and the House of Representatives, the Committee on Home-
29 land Security of the House of Representatives, the Committee on
30 Transportation and Infrastructure of the House of Representatives, the
31 Committee on Homeland Security and Governmental Affairs of the
32 Senate, and the Committee on Commerce, Science and Transportation
33 of the Senate that—

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

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

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

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

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

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

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

15 **Subchapter IV—Human Resources** 16 **Management**

17 **§ 10351. Establishment of human resources management** 18 **system**

19 (a) POSITIONS COMPENSATED IN ACCORDANCE WITH EXECUTIVE
 20 SCHEDULE.—A person who, on the day preceding the person’s date of
 21 transfer pursuant to the Homeland Security Act of 2002 (Public Law 107–
 22 296, 116 Stat. 2135), held a position compensated in accordance with the
 23 Executive Schedule prescribed in chapter 53 of title 5, and who, without a
 24 break in service, is appointed in the Department to a position having duties
 25 comparable to the duties performed immediately preceding the appointment
 26 shall continue to be compensated in the new position at not less than the
 27 rate provided for the position, for the duration of the service of the person
 28 in the new position.

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

32 **§ 10352. Labor-management relations**

33 (a) LIMITATION ON EXCLUSIONARY AUTHORITY.—

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

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

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

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

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

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

11 (b) PROVISIONS RELATING TO BARGAINING UNITS.—

12 (1) LIMITATION RELATING TO APPROPRIATE UNITS.—Each unit rec-
13 ognized as an appropriate unit for purposes of chapter 71 of title 5,
14 as of January 23, 2003 (and a subdivision of a unit), shall, if the unit
15 (or subdivision) is transferred to the Department pursuant to the
16 Homeland Security Act of 2002 (Public Law 107–296, 116 Stat.
17 2135), continue to be so recognized for those purposes, unless—

18 (A) the mission and responsibilities of the unit (or subdivision)
19 materially change; and

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

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

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

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

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

39 (d) COORDINATION RULE.—No other provision of this subtitle or the
40 Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2135), or
41 of an amendment made by the Act, may be construed or applied in a man-

ner so as to limit, supersede, or otherwise affect the provisions of this section, except to the extent that it does so by specific reference to this section.

(e) **RULE OF CONSTRUCTION.**—Nothing in section 9701(e) of title 5 shall be considered to apply with respect to an agency or subdivision of an agency, which is excluded from the coverage of chapter 71 of title 5 by virtue of an order issued under section 7103(b) of the title and the preceding provisions of this section (as applicable), or to an employee of the agency or subdivision or to an individual or entity representing the employees or representatives thereof.

§ 10353. Use of counternarcotics enforcement activities in certain employee performance appraisals

(a) **DEFINITIONS.**—In this section:

(1) **NATIONAL DRUG CONTROL PROGRAM AGENCY.**—The term “National Drug Control Program agency” means—

(A) a National Drug Control Program agency, as defined in section 702 of the Office of National Drug Control Policy Reauthorization Act of 1998 (21 U.S.C. 1701); and

(B) a subdivision of the Department that has a significant counternarcotics responsibility, as determined by—

(i) the counternarcotics officer, appointed under section 10316 of this title; or

(ii) if applicable, the counternarcotics officer’s successor in function (as determined by the Secretary).

(2) **PERFORMANCE APPRAISAL SYSTEM.**—The term “performance appraisal system” means a system under which periodic appraisals of job performance of employees are made, whether under chapter 43 of title 5, or otherwise.

(b) **IN GENERAL.**—Each subdivision of the Department that is a National Drug Control Program agency shall include as one of the criteria in its performance appraisal system, for each employee directly or indirectly involved in the enforcement of Federal, State, or local narcotics laws, the performance of that employee with respect to the enforcement of Federal, State, or local narcotics laws, relying to the greatest extent practicable on objective performance measures, including—

(1) the contribution of that employee to seizures of narcotics and arrests of violators of Federal, State, or local narcotics laws; and

(2) the degree to which that employee cooperated with or contributed to the efforts of other employees, either in the Department or other Federal, State, or local agencies, in counternarcotics enforcement.

1 **§ 10354. Compliance with laws protecting equal employment**
 2 **opportunity and providing whistleblower protec-**
 3 **tions**

4 Nothing in this subtitle shall be construed as exempting the Department
 5 from requirements applicable with respect to executive agencies—

6 (1) to provide equal employment protection for employees of the De-
 7 partment (including under section 2302(b)(1) of title 5 and the Notifi-
 8 cation and Federal Employee Antidiscrimination and Retaliation Act of
 9 2002 (Public Law 107–174, 5 U.S.C. 2301 note)); or

10 (2) to provide whistleblower protections for employees of the Depart-
 11 ment (including under paragraphs (8) and (9) of section 2302(b) of
 12 title 5 and the Notification and Federal Employee Antidiscrimination
 13 and Retaliation Act of 2002 (Public Law 107–174, 5 U.S.C. 2301
 14 note)).

15 **§ 10355. Use of protective equipment or measures by em-**
 16 **ployees**

17 No funds may be used to propose or effect a disciplinary or adverse ac-
 18 tion, with respect to any Department employee who engages regularly with
 19 the public in the performance of his or her official duties, solely because
 20 that employee elects to utilize protective equipment or measures, including
 21 surgical masks, N95 respirators, gloves, or hand-sanitizers, where use of the
 22 equipment or measures is in accord with Department policy, and Centers
 23 for Disease Control and Prevention and Office of Personnel Management
 24 guidance.

25 **§ 10356. Homeland Security Rotation Program**

26 (a) ESTABLISHMENT.—The Secretary shall establish the Homeland Secu-
 27 rity Rotation Program (in this section referred to as the “Rotation Pro-
 28 gram”) for employees of the Department. The Rotation Program shall use
 29 applicable best practices, including those from the Chief Human Capital Of-
 30 ficers Council.

31 (b) GOALS.—The Rotation Program established by the Secretary shall—

32 (1) be established in accordance with the Human Capital Strategic
 33 Plan of the Department;

34 (2) provide middle and senior level employees in the Department the
 35 opportunity to broaden their knowledge through exposure to other com-
 36 ponents of the Department;

37 (3) expand the knowledge base of the Department by providing for
 38 rotational assignments of employees to other components;

39 (4) build professional relationships and contacts among the employ-
 40 ees in the Department;

1 (5) invigorate the workforce with exciting and professionally reward-
2 ing opportunities;

3 (6) incorporate Department human capital strategic plans and activi-
4 ties, and address critical human capital deficiencies, recruitment and
5 retention efforts, and succession planning in the Federal workforce of
6 the Department; and

7 (7) complement and incorporate (but not replace) rotational pro-
8 grams in the Department in effect on October 4, 2006.

9 (c) ADMINISTRATION.—

10 (1) IN GENERAL.—The Chief Human Capital Officer shall admin-
11 ister the Rotation Program.

12 (2) RESPONSIBILITIES.—The Chief Human Capital Officer shall—

13 (A) provide oversight of the establishment and implementation
14 of the Rotation Program;

15 (B) establish a framework that supports the goals of the Rota-
16 tion Program and promotes cross-disciplinary rotational opportuni-
17 ties;

18 (C) establish eligibility for employees to participate in the Rota-
19 tion Program and select participants from employees who apply;

20 (D) establish incentives for employees to participate in the Ro-
21 tation Program, including promotions and employment pref-
22 erences;

23 (E) ensure that the Rotation Program provides professional
24 education and training;

25 (F) ensure that the Rotation Program develops qualified em-
26 ployees and future leaders with broad-based experience throughout
27 the Department;

28 (G) provide for greater interaction among employees in compo-
29 nents of the Department; and

30 (H) coordinate with rotational programs in the Department in
31 effect on October 4, 2006.

32 (d) ALLOWANCES, PRIVILEGES, AND BENEFITS.—All allowances, privi-
33 leges, rights, seniority, and other benefits of employees participating in the
34 Rotation Program shall be preserved.

35 **§ 10357. Homeland Security Education Program**

36 (a) ESTABLISHMENT.—The Secretary, acting through the Administrator
37 of the Federal Emergency Management Agency, shall establish a graduate-
38 level Homeland Security Education Program in the National Capital Region
39 to provide educational opportunities to senior Federal officials and selected
40 State and local officials with homeland security and emergency management

1 responsibilities. The Administrator shall appoint an individual to administer
2 the activities under this section.

3 (b) LEVERAGING OF EXISTING RESOURCES.—To maximize efficiency and
4 effectiveness in carrying out the Homeland Security Education Program,
5 the Administrator shall use existing Department-reviewed Master’s Degree
6 curricula in homeland security, including curricula pending accreditation, to-
7 gether with associated learning materials, quality assessment tools, digital
8 libraries, exercise systems, and other educational facilities, including the Na-
9 tional Domestic Preparedness Consortium, the National Fire Academy, and
10 the Emergency Management Institute. The Administrator may develop addi-
11 tional educational programs, as appropriate.

12 (c) STUDENT ENROLLMENT.—

13 (1) SOURCES.—The student body of the Homeland Security Edu-
14 cation Program shall include officials from Federal, State, local, and
15 tribal governments, and from other sources designated by the Adminis-
16 trator.

17 (2) ENROLLMENT PRIORITIES AND SELECTION CRITERIA.—The Ad-
18 ministrator shall establish policies governing student enrollment prior-
19 ities and selection criteria that are consistent with the mission of the
20 Homeland Security Education Program.

21 (3) DIVERSITY.—The Administrator shall take reasonable steps to
22 ensure that the student body represents racial, gender, and ethnic di-
23 versity.

24 (d) SERVICE COMMITMENT.—

25 (1) IN GENERAL.—Before an employee selected for the Homeland
26 Security Education Program may be assigned to participate in the pro-
27 gram, the employee shall agree in writing—

28 (A) to continue in the service of the agency sponsoring the em-
29 ployee during the 2-year period beginning on the date on which
30 the employee completes the program, unless the employee is invol-
31 untarily separated from the service of that agency for reasons
32 other than a reduction in force; and

33 (B) to pay to the Government the amount of the additional ex-
34 penses incurred by the Government in connection with the employ-
35 ee’s education if the employee is voluntarily separated from the
36 service of the agency before the end of the period described in sub-
37 paragraph (A).

38 (2) PAYMENT OF EXPENSES.—

39 (A) EXEMPTION.—An employee who leaves the service of the
40 sponsoring agency to enter into the service of another agency in
41 any branch of the Government shall not be required to make a

1 payment under paragraph (1)(B), unless the head of the agency
 2 that sponsored the education of the employee notifies that em-
 3 ployee before the date on which the employee enters the service
 4 of the other agency that payment is required under that para-
 5 graph.

6 (B) AMOUNT OF PAYMENT.—If an employee is required to make
 7 a payment under paragraph (1)(B), the agency that sponsored the
 8 education of the employee shall determine the amount of the pay-
 9 ment, except that the amount may not exceed the pro rata share
 10 of the expenses incurred for the time remaining in the 2-year pe-
 11 riod.

12 (3) RECOVERY OF PAYMENT.—If an employee who is required to
 13 make a payment under this subsection does not make the payment, a
 14 sum equal to the amount of the expenses incurred by the Government
 15 for the education of that employee is recoverable by the Government
 16 from the employee or his estate by—

17 (A) setoff against accrued pay, compensation, amount of retire-
 18 ment credit, or other amount due the employee from the Govern-
 19 ment; or

20 (B) another method provided by law for the recovery of amounts
 21 owing to the Government.

22 **Subchapter V—Cybersecurity**

23 **§ 10371. Workforce assessment and strategy**

24 (a) DEFINITIONS.—In this section:

25 (1) CYBERSECURITY CATEGORY.—The term “Cybersecurity Cat-
 26 egory” means a position’s or incumbent’s primary work function involv-
 27 ing cybersecurity, which is further defined by Specialty Area.

28 (2) SPECIALTY AREA.—The term “Specialty Area” means any of the
 29 common types of cybersecurity work as recognized by the National Ini-
 30 tiative for Cybersecurity Education’s National Cybersecurity Workforce
 31 Framework report.

32 (b) WORKFORCE ASSESSMENT.—Not later than 180 days after December
 33 18, 2014, and annually afterwards for 3 years, the Secretary shall assess
 34 the cybersecurity workforce of the Department. The assessment shall in-
 35 clude, at a minimum—

36 (1) an assessment of the readiness and capacity of the workforce of
 37 the Department to meet its cybersecurity mission;

38 (2) information on where cybersecurity workforce positions are lo-
 39 cated in the Department;

40 (3) information on which cybersecurity workforce positions are—

41 (A) performed by—

- 1 (i) permanent full-time equivalent employees of the Depart-
 2 ment, including, to the greatest extent practicable, demo-
 3 graphic information about the employees;
- 4 (ii) independent contractors; and
- 5 (iii) individuals employed by other Federal agencies, includ-
 6 ing the National Security Agency; or
- 7 (B) vacant; and
- 8 (4) information on—
- 9 (A) the percentage of individuals in each Cybersecurity Category
 10 and Specialty Area who received essential training to perform their
 11 jobs; and
- 12 (B) in cases in which that essential training was not received,
 13 what challenges, if any, were encountered with respect to the pro-
 14 vision of the essential training.
- 15 (c) WORKFORCE STRATEGY.—
- 16 (1) ESTABLISHMENT, MAINTENANCE, AND UPDATES.—The Secretary
 17 shall—
- 18 (A) develop a comprehensive workforce strategy to enhance the
 19 readiness, capacity, training, recruitment, and retention of the cy-
 20 bersecurity workforce of the Department; and
- 21 (B) maintain and, as necessary, update the comprehensive
 22 workforce strategy developed under subparagraph (A).
- 23 (2) CONTENTS.—The comprehensive workforce strategy developed
 24 under paragraph (1) shall include a description of—
- 25 (A) a multi-phased recruitment plan, including with respect to
 26 experienced professionals, members of disadvantaged or under-
 27 served communities, the unemployed, and veterans;
- 28 (B) a 5-year implementation plan;
- 29 (C) a 10-year projection of the cybersecurity workforce needs of
 30 the Department;
- 31 (D) any obstacle impeding the hiring and development of a cy-
 32 bersecurity workforce in the Department; and
- 33 (E) any gap in the existing cybersecurity workforce of the De-
 34 partment and a plan to fill the gap.
- 35 (d) UPDATES.—The Secretary shall submit to the appropriate congres-
 36 sional committees annual updates on—
- 37 (1) the cybersecurity workforce assessment required under subsection
 38 (b); and
- 39 (2) the progress of the Secretary in carrying out the comprehensive
 40 workforce strategy required to be developed under subsection (c).

1 **§ 10372. Homeland Workforce Measurement Initiative**

2 (a) DEFINITIONS.—In this section:

3 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
4 priate congressional committees” means—

5 (A) the Committee on Homeland Security and Governmental
6 Affairs of the Senate;

7 (B) the Committee on Homeland Security of the House of Rep-
8 resentatives; and

9 (C) the Committee on House Administration of the House of
10 Representatives.

11 (2) CYBERSECURITY WORK CATEGORY; DATA ELEMENT CODE; SPE-
12 CIALTY AREA.—The terms “Cybersecurity Work Category”, “Data Ele-
13 ment Code”, and “Specialty Area” have the same meanings given the
14 terms in the Office of Personnel Management’s Guide to Data Stand-
15 ards.

16 (3) DIRECTOR.—The term “Director” means the Director of the Of-
17 fice of Personnel Management.

18 (b) NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIA-
19 TIVE.—

20 (1) IN GENERAL.—The Secretary shall—

21 (A) identify all cybersecurity workforce positions in the Depart-
22 ment;

23 (B) determine the primary Cybersecurity Work Category and
24 Specialty Area of those positions; and

25 (C) assign the corresponding Data Element Code, as set forth
26 in the Office of Personnel Management’s Guide to Data Standards
27 that is aligned with the National Initiative for Cybersecurity Edu-
28 cation’s National Cybersecurity Workforce Framework report, in
29 accordance with paragraph (2).

30 (2) EMPLOYMENT CODES.—

31 (A) PROCEDURES.—The Secretary shall establish procedures
32 to—

33 (i) identify open positions that include cybersecurity func-
34 tions (as defined in the Office of Personnel Management
35 Guide to Data Standards); and

36 (ii) assign the appropriate employment code to each posi-
37 tion, using agreed standards and definitions.

38 (B) CODE ASSIGNMENTS.—The Secretary shall assign the ap-
39 propriate employment code to—

40 (i) each employee in the Department who carries out cyber-
41 security functions; and

1 (ii) each open position in the Department that has been
2 identified as having cybersecurity functions.

3 (3) PROGRESS REPORT.—The Director shall submit a progress re-
4 port on the implementation of this subsection to the appropriate con-
5 gressional committees.

6 (c) IDENTIFICATION OF CYBERSECURITY SPECIALTY AREAS OF CRITICAL
7 NEED.—

8 (1) IN GENERAL.—Annually through 2021, the Secretary, in con-
9 sultation with the Director, shall—

10 (A) identify Cybersecurity Work Categories and Specialty Areas
11 of critical need in the Department’s cybersecurity workforce; and

12 (B) submit a report to the Director that—

13 (i) describes the Cybersecurity Work Categories and Spe-
14 cialty Areas identified under subparagraph (A); and

15 (ii) substantiates the critical need designations.

16 (2) GUIDANCE.—The Director shall provide the Secretary with time-
17 ly guidance for identifying Cybersecurity Work Categories and Spe-
18 cialty Areas of critical need, including—

19 (A) current Cybersecurity Work Categories and Specialty Areas
20 with acute skill shortages; and

21 (B) Cybersecurity Work Categories and Specialty Areas with
22 emerging skill shortages.

23 (3) CYBERSECURITY CRITICAL NEEDS REPORT.—Not later than 18
24 months after December 18, 2014, the Secretary, in consultation with
25 the Director, shall—

26 (A) identify Specialty Areas of critical need for cybersecurity
27 workforce across the Department; and

28 (B) submit a progress report on the implementation of this sub-
29 section to the appropriate congressional committees.

30 (d) GOVERNMENT ACCOUNTABILITY OFFICE STATUS REPORTS.—The
31 Comptroller General shall—

32 (1) analyze and monitor the implementation of subsections (b) and
33 (c); and

34 (2) not later than 3 years after December 18, 2014, submit a report
35 to the appropriate congressional committees that describes the status
36 of the implementation.

37 **§ 10373. Recruitment and retention**

38 (a) DEFINITIONS.—In this section

39 (1) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appro-
40 priate committees of Congress” means the Committee on Homeland Se-
41 curity and Governmental Affairs and the Committee on Appropriations

1 of the Senate and the Committee on Homeland Security and the Com-
2 mittee on Appropriations of the House of Representatives.

3 (2) COLLECTIVE BARGAINING AGREEMENT.—The term “collective
4 bargaining agreement” has the same meaning given that term in sec-
5 tion 7103(a)(8) of title 5.

6 (3) EXCEPTED SERVICE.—The term “excepted service” has the same
7 meaning given that term in section 2103 of title 5.

8 (4) PREFERENCE ELIGIBLE.—The term “preference eligible” has the
9 same meaning given that term in section 2108 of title 5.

10 (5) QUALIFIED POSITION.—The term “qualified position” means a
11 position, designated by the Secretary for the purpose of this section,
12 in which the incumbent performs, manages, or supervises functions
13 that execute the responsibilities of the Department relating to cyberse-
14 curity.

15 (6) SENIOR EXECUTIVE SERVICE.—The term “Senior Executive
16 Service” has the same meaning given that term in section 2101a of
17 title 5.

18 (b) GENERAL AUTHORITY OF SECRETARY.—

19 (1) ESTABLISH POSITIONS, APPOINT PERSONNEL, AND FIX RATES OF
20 PAY.—

21 (A) IN GENERAL.—The Secretary may—

22 (i) establish, as positions in the excepted service, such
23 qualified positions in the Department as the Secretary deter-
24 mines necessary to carry out the responsibilities of the De-
25 partment relating to cybersecurity, including positions for-
26 merly identified as—

27 (I) senior level positions designated under section
28 5376 of title 5; and

29 (II) positions in the Senior Executive Service;

30 (ii) appoint an individual to a qualified position (after tak-
31 ing into consideration the availability of preference eligibles
32 for appointment to the position); and

33 (iii) subject to the requirements of paragraphs (2) and (3),
34 fix the compensation of an individual for service in a qualified
35 position.

36 (B) CONSTRUCTION WITH OTHER LAWS.—The authority of the
37 Secretary under this subsection applies without regard to the pro-
38 visions of any other law relating to the appointment, number, clas-
39 sification, or compensation of employees.

40 (2) BASIC PAY.—

1 (A) AUTHORITY TO FIX RATES OF BASIC PAY.—In accordance
2 with this section, the Secretary shall fix the rates of basic pay for
3 any qualified position established under paragraph (1) in relation
4 to the rates of pay provided for employees in comparable positions
5 in the Department of Defense and subject to the same limitations
6 on maximum rates of pay established for those employees by law
7 or regulation.

8 (B) PREVAILING RATE SYSTEMS.—The Secretary may, con-
9 sistent with section 5341 of title 5, adopt such provisions of that
10 title as provide for prevailing rate systems of basic pay and may
11 apply those provisions to qualified positions for employees in or
12 under which the Department may employ individuals described by
13 section 5342(a)(2)(A) of title 5.

14 (3) ADDITIONAL COMPENSATION, INCENTIVES, AND ALLOWANCES.—

15 (A) ADDITIONAL COMPENSATION BASED ON TITLE 5 AUTHOR-
16 IZATION.—The Secretary may provide employees in qualified posi-
17 tions compensation (in addition to basic pay), including benefits,
18 incentives, and allowances, consistent with, and not in excess of
19 the level authorized for, comparable positions authorized by title
20 5.

21 (B) ALLOWANCES IN NONFOREIGN AREAS.—An employee in a
22 qualified position whose rate of basic pay is fixed under paragraph
23 (2)(A) is eligible for an allowance under section 5941 of title 5,
24 on the same basis and to the same extent as if the employee was
25 an employee covered by section 5941, including eligibility condi-
26 tions, allowance rates, and all other terms and conditions in law
27 or regulation.

28 (4) PLAN FOR EXECUTION OF AUTHORITIES.—The Secretary shall
29 submit a report to the appropriate committees of Congress with a plan
30 for the use of the authorities provided under this subsection.

31 (5) COLLECTIVE BARGAINING AGREEMENTS.—Nothing in paragraph
32 (1) may be construed to impair the continued effectiveness of a collec-
33 tive bargaining agreement with respect to an office, component, sub-
34 component, or equivalent of the Department that is a successor to an
35 office, component, subcomponent, or equivalent of the Department cov-
36 ered by the agreement before the succession.

37 (6) REQUIRED REGULATIONS.—The Secretary, in coordination with
38 the Director of the Office of Personnel Management, shall prescribe
39 regulations for the administration of this section.

1 (c) ANNUAL REPORT.—Not later than December 18, 2016, 2017, and
2 2018, the Secretary shall submit to the appropriate committees of Congress
3 a detailed report that—

4 (1) discusses the process used by the Secretary in accepting applica-
5 tions, assessing candidates, ensuring adherence to veterans' preference,
6 and selecting applicants for vacancies to be filled by an individual for
7 a qualified position;

8 (2) describes—

9 (A) how the Secretary plans to fulfill the critical need of the De-
10 partment to recruit and retain employees in qualified positions;

11 (B) the measures that will be used to measure progress; and

12 (C) any actions taken during the reporting period to fulfill that
13 critical need;

14 (3) discusses how the planning and actions taken under paragraph
15 (2) are integrated into the strategic workforce planning of the Depart-
16 ment;

17 (4) provides metrics on actions occurring during the reporting pe-
18 riod, including—

19 (A) the number of employees in qualified positions hired by oc-
20 cupation and grade and level or pay band;

21 (B) the placement of employees in qualified positions by direc-
22 torate and office in the Department;

23 (C) the total number of veterans hired;

24 (D) the number of separations of employees in qualified posi-
25 tions by occupation and grade and level or pay band;

26 (E) the number of retirements of employees in qualified posi-
27 tions by occupation and grade and level or pay band; and

28 (F) the number and amounts of recruitment, relocation, and re-
29 tention incentives paid to employees in qualified positions by occu-
30 pation and grade and level or pay band; and

31 (5) describes the training provided to supervisors of employees in
32 qualified positions at the Department on the use of the new authorities.

33 (d) THREE-YEAR PROBATIONARY PERIOD.—The probationary period for
34 all employees hired under the authority established in this section is 3 years.

35 (e) INCUMBENTS OF EXISTING COMPETITIVE SERVICE POSITIONS.—

36 (1) IN GENERAL.—An individual serving in a position on December
37 18, 2014, that is selected to be converted to a position in the excepted
38 service under this section shall have the right to refuse the conversion.

39 (2) SUBSEQUENT CONVERSION.—After the date on which an indi-
40 vidual who refuses a conversion under paragraph (1) stops serving in

1 the position selected to be converted, the position may be converted to
2 a position in the excepted service.

3 (f) REPORT.—The National Protection and Programs Directorate shall
4 submit a report regarding the availability of, and benefits (including cost
5 savings and security) of using, cybersecurity personnel and facilities outside
6 of the National Capital Region (as defined in section 2674 of title 10) to
7 serve the Federal and national need to—

8 (1) the Subcommittee on Homeland Security of the Committee on
9 Appropriations and the Committee on Homeland Security and Govern-
10 mental Affairs of the Senate; and

11 (2) the Subcommittee on Homeland Security of the Committee on
12 Appropriations and the Committee on Homeland Security of the House
13 of Representatives.

14 **Subchapter VI—Miscellaneous Provisions**

15 **§ 10381. Advisory committees**

16 (a) IN GENERAL.—The Secretary may establish, appoint members of, and
17 use the services of, advisory committees, that the Secretary considers nec-
18 essary. An advisory committee established under this section may be ex-
19 empted by the Secretary from Public Law 92–463 (5 U.S.C. App.), but the
20 Secretary shall publish notice in the Federal Register announcing the estab-
21 lishment of the committee and identifying its purpose and membership. Not-
22 withstanding the preceding sentence, members of an advisory committee
23 that is exempted by the Secretary under the preceding sentence who are
24 special Government employees (as that term is defined in section 202 of
25 title 18) shall be eligible for certifications under section 208(b)(3) of title
26 18, for official actions taken as a member of the advisory committee.

27 (b) TERMINATION.—An advisory committee established by the Secretary
28 shall terminate 2 years after the date of its establishment, unless the Sec-
29 retary makes a written determination to extend the advisory committee to
30 a specified date, which shall not be more than 2 years after the date on
31 which the determination is made. The Secretary may make any number of
32 subsequent extensions consistent with this subsection.

33 **§ 10382. Use of appropriated funds**

34 (a) IN GENERAL.—Unless otherwise provided, funds may be used for the
35 following:

36 (1) Purchase of uniforms without regard to the general purchase
37 price limitation for the current fiscal year;

38 (2) Purchase of insurance for official motor vehicles operated in for-
39 eign countries;

1 (3) Entering into contracts with the Department of State to furnish
2 health and medical services to employees and their dependents serving
3 in foreign countries;

4 (4) Services authorized by section 3109 of title 5, United States
5 Code.

6 (5) The hire and purchase of motor vehicles, as authorized by section
7 1343 of title 31.

8 (b) POLICE-LIKE USE OF VEHICLES.—The purchase for police-type use
9 of passenger vehicles may be made without regard to the general purchase
10 price limitation for the current fiscal year.

11 (c) DISPOSAL OF PROPERTY.—

12 (1) STRICT COMPLIANCE.—If specifically authorized to dispose of
13 real property in this subtitle or any law, the Secretary shall exercise
14 this authority in strict compliance with subchapter IV of chapter 5 of
15 title 40.

16 (2) DEPOSIT OF PROCEEDS.—The Secretary shall deposit the pro-
17 ceeds of an exercise of property disposal authority into the miscella-
18 neous receipts of the Treasury under section 3302(b) of title 31.

19 (d) GIFTS.—Except as authorized by section 10387 or 11122 of this title,
20 section 2601 of title 10, or section 93 of title 14, gifts or donations of serv-
21 ices or property of or for the Department may not be accepted, used, or
22 disposed of unless specifically permitted in advance in an appropriations Act
23 and only under the conditions and for the purposes specified in the appro-
24 priations Act.

25 (e) BUDGET REQUEST.—Under section 1105 of title 31, the President
26 shall submit to Congress a detailed budget request for the Department for
27 each fiscal year.

28 **§ 10383. Reports and consultation addressing use of appro-**
29 **riated funds**

30 (a) IN GENERAL.—Notwithstanding any other provision of this subtitle,
31 a report, notification, or consultation addressing directly or indirectly the
32 use of appropriated funds and stipulated by this subtitle to be submitted
33 to, or held with, Congress or a Congressional committee shall also be sub-
34 mitted to, or held with, the Committees on Appropriations of the Senate
35 and the House of Representatives under the same conditions and with the
36 same restrictions as stipulated by this subtitle.

37 (b) REPROGRAMMING AND TRANSFER OF FUNDS.—Notifications by the
38 Department under an authority for reprogramming or transfer of funds
39 shall be made solely to the Committees on Appropriations of the Senate and
40 the House of Representatives.

1 **§ 10384. 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 ITEMS.—

27 (1) DEFINITION OF COMMERCIAL.—In this section, the word “com-
28 mercial” has the meaning given the term in the Federal Acquisition
29 Regulation—Part 2.

30 (2) IN GENERAL.—This section is applicable to contracts and sub-
31 contracts for the procurement of commercial items notwithstanding sec-
32 tion 1906 of title 41, with the exception of commercial items listed
33 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 2304(g) 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 **§ 10385. 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.

§ 10386. Future Years Homeland Security Program

(a) IN GENERAL.—Each budget request submitted to Congress for the Department under section 1105 of title 31, shall, at or about the same time, be accompanied by a Future Years Homeland Security Program.

(b) CONTENTS.—The Future Years Homeland Security Program shall—

(1) include the same type of information, organizational structure, and level of detail as the future years defense program submitted to Congress by the Secretary of Defense under section 221 of title 10;

(2) set forth the homeland security strategy of the Department, which shall be developed and updated as appropriate annually by the Secretary, that was used to develop program planning guidance for the Future Years Homeland Security Program; and

(3) include an explanation of how the resource allocations included in the Future Years Homeland Security Program correlate to the homeland security strategy set forth under paragraph (2).

§ 10387. Federal Law Enforcement Training Centers

(a) DEFINITIONS.—In this section:

(1) BASIC TRAINING.—The term “basic training” means the entry-level training required to instill in new Federal law enforcement personnel fundamental knowledge of criminal laws, law enforcement and investigative techniques, laws and rules of evidence, rules of criminal procedure, constitutional rights, search and seizure, and related issues.

(2) DETAILED INSTRUCTORS.—The term “detailed instructors” means personnel who are assigned to the Federal Law Enforcement Training Centers (in this section referred to as “FLETC”) for a period of time to serve as instructors for the purpose of conducting basic and advanced training.

(3) DIRECTOR.—The term “Director” means the Director of FLETC.

(4) DISTRIBUTED LEARNING.—The term “distributed learning” means education in which students take academic courses by accessing information and communicating with the instructor, from various locations, on an individual basis, over a computer network or via other technologies.

(5) EMPLOYEE.—The term “employee” has the meaning given the term in section 2105 of title 5.

(6) FEDERAL AGENCY.—The term “Federal agency” means—

(A) an executive department as defined in section 101 of title 5;

(B) an independent establishment as defined in section 104 of 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 of the United States,
27 the District of Columbia, Puerto Rico, the Virgin Islands, Guam,
28 American Samoa, the Northern Mariana Islands, and any possession
29 of the United States.

30 (11) STUDENT INTERN.—The term “student intern” means any eli-
31 gible baccalaureate or graduate degree student participating in
32 FLETC’s College Intern Program.

33 (b) ESTABLISHMENT.—The Secretary shall maintain in the Department
34 the Federal Law Enforcement Training Centers. The Director—

35 (1) is the head of FLETC;

36 (2) shall occupy a career-reserved position in the Senior Executive
37 Service; and

38 (3) shall report to the Secretary.

39 (c) FUNCTIONS OF THE DIRECTOR.—The Director shall—

40 (1) develop training goals and establish strategic and tactical organi-
41 zational program plans and priorities;

1 (2) provide direction and management for FLETC's training facilities,
2 programs, and support activities while ensuring that organizational
3 program goals and priorities are executed in an effective and efficient
4 manner;

5 (3) develop homeland security and law enforcement training curricula,
6 including curricula relating to domestic preparedness and response to
7 threats or acts of terrorism, for Federal, State, local, tribal, territorial,
8 and international law enforcement and security agencies and
9 private-sector security agencies;

10 (4) monitor progress toward strategic and tactical FLETC plans regarding
11 training curricula, including curricula relating to domestic preparedness
12 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 international
15 law enforcement and security agencies and the private sector to achieve
16 the training goals for those entities, in accordance with paragraph (1);
17

18 (6) carry out delegated acquisition responsibilities in a manner that—
19

20 (A) fully complies with—

21 (i) Federal law;

22 (ii) the Federal Acquisition Regulation, including requirements
23 regarding agency obligations to contract only with responsible
24 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 components
28 and offices on digital learning and training resources, as appropriate;
29

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 activities
34 relating to domestic preparedness and response to threats or acts of terrorism;
35

36 (9) collaborate with the Secretary and relevant officials at other Federal
37 departments and agencies, as appropriate, to improve international instructional
38 development, training, and technical assistance provided by the Federal Government
39 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 Under Secretary responsible for
29 overseeing critical infrastructure protection, cybersecurity,
30 and other related programs of the Department and with pri-
31 vate sector stakeholders, including critical infrastructure own-
32 ers and operators, to provide training pertinent to improving
33 coordination, security, and resiliency of critical infrastructure.

34 (B) PROVISION OF INFORMATION.—The Director shall provide
35 to the Committee on Homeland Security of the House of Rep-
36 resentatives and the Committee on Homeland Security and Gov-
37 ernmental Affairs of the Senate, on request, information on activi-
38 ties undertaken in the previous year pursuant to subparagraph

39 (A).

40 (5) FLETC DETAILS TO DEPARTMENT.—The Director may detail
41 employees of FLETC to positions throughout the Department in fur-

1 therance of improving the effectiveness and quality of training provided
2 by the Department and, as appropriate, the development of critical de-
3 partmental programs and initiatives.

4 (6) DETAIL OF INSTRUCTIONS TO FLETC.—Partner organizations
5 that wish to participate in FLETC training programs shall assign non-
6 reimbursable detailed instructors to FLETC for designated time peri-
7 ods to support all training programs at FLETC, as appropriate. The
8 Director shall determine the number of detailed instructors that is pro-
9 portional to the number of training hours requested by each partner
10 organization scheduled by FLETC for each fiscal year. If a partner or-
11 ganization is unable to provide a proportional number of detailed in-
12 structors, the partner organization shall reimburse FLETC for the sal-
13 ary equivalent for the detailed instructors, as appropriate.

14 (7) PARTNER ORGANIZATION EXPENSES REQUIREMENTS.—

15 (A) IN GENERAL.—Partner organizations shall be responsible
16 for the following expenses:

17 (i) Salaries, travel expenses, lodging expenses, and miscella-
18 neous per diem allowances of their personnel attending train-
19 ing courses at FLETC.

20 (ii) Salaries and travel expenses of instructors and support
21 personnel involved in conducting advanced training at
22 FLETC for partner organization personnel and the cost of
23 expendable supplies and special equipment for the training,
24 unless the supplies and equipment are common to FLETC-
25 conducted training and have been included in FLETC's bud-
26 get for the applicable fiscal year.

27 (B) EXCESS BASIC AND ADVANCED FEDERAL TRAINING.—All
28 hours of advanced training and hours of basic training provided
29 in excess of the training for which appropriations were made avail-
30 able shall be paid by the partner organizations and provided to
31 FLETC on a reimbursable basis in accordance with section 4104
32 of title 5.

33 (8) PROVISION OF NON-FEDERAL TRAINING.—

34 (A) IN GENERAL.—The Director may charge and retain fees
35 that would pay for FLETC's actual costs of the training for the
36 following:

37 (i) State, local, tribal, and territorial law enforcement per-
38 sonnel.

39 (ii) Foreign law enforcement officials, including provision of
40 the training at the International Law Enforcement Academies
41 wherever established.

1 (iii) Private-sector security officers, participants in the
2 Federal Flight Deck Officer program under section 40930 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.—The Director may appoint and maintain, as
18 necessary, Federal annuitants who have expert knowledge and ex-
19 perience to meet the training responsibilities under this subsection.

20 (B) NO REDUCTION IN RETIREMENT PAY.—A Federal annuitant
21 employed pursuant to this paragraph shall not be subject to any
22 reduction in pay for annuity allocable to the period of actual em-
23 ployment under the provisions of section 8344 or 8468 of title 5
24 or a similar provision of any other retirement system for employ-
25 ees.

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 10382(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 **§ 10388. 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 40957(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 40957(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 (3) ANNUAL REPORT.—The Secretary shall provide a report annually
 10 to the Committees on Appropriations of the Senate and the House of
 11 Representatives, providing the level of collections and a summary by
 12 agency of the purposes and levels of expenditures for the prior fiscal
 13 year.

14 **§ 10389. Reports to Committee on Commerce, Science, and**
 15 **Transportation**

16 The Committee on Commerce, Science, and Transportation of the Senate
 17 shall receive the reports required by the following provisions of law in the
 18 same manner and to the same extent that the reports are to be received
 19 by the Committee on Homeland Security and Governmental Affairs of the
 20 Senate:

21 (1) Section 10501(b)(25) of this title.

22 (2) Section 12510(a)(3)(D) of this title.

23 (3) Section 7209(b)(1)(C) of the Intelligence Reform and Terrorism
 24 Prevention Act of 2004 (Public Law 108–458, 8 U.S.C. 1185 note).

25 (4) Title III of the Implementing Recommendations of the 9/11
 26 Commission Act of 2007 (Public Law 110–53, 121 Stat. 296).

27 (5) Section 511(d) of the Implementing Recommendations of the 9/
 28 11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 323).

29 (6) Section 804(c) of the Implementing Recommendations of the 9/
 30 11 Commission Act of 2007 (42 U.S.C. 2000ee–3(c)).

31 (7) Section 901(b) of the Implementing Recommendations of the 9/
 32 11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 370).

33 **§ 10390. Annual ammunition and weaponry reports**

34 (a) IN GENERAL.—The Secretary annually shall submit to Congress
 35 along with the submission of the President’s budget proposal pursuant to
 36 section 1105(a) of title 31 the following:

37 (1) A comprehensive report on the purchase and usage of ammuni-
 38 tion, subdivided by ammunition type.

39 (2) A comprehensive report on the purchase and usage of weapons,
 40 subdivided by weapon type.

41 (b) CONTENTS.—

1 (1) AMMUNITION REPORT.—The ammunition report shall include—

2 (A) the quantity of ammunition in inventory at the end of the
3 preceding calendar year, and the amount of ammunition expended
4 and purchased, subdivided by ammunition type, during the year
5 for each relevant component or agency in the Department;

6 (B) a description of how the quantity, usage, and purchase
7 aligns to each component or agency’s mission requirements for
8 certification, qualification, training, and operations; and

9 (C) details on all contracting practices applied by the Depart-
10 ment, including comparative details regarding other contracting
11 options with respect to cost and availability.

12 (2) WEAPONRY REPORT.—The weaponry report shall include—

13 (A) the quantity of weapons in inventory at the end of the pre-
14 ceding calendar year, and the amount of weapons, subdivided by
15 weapon type, included in the budget request for each relevant com-
16 ponent or agency in the Department;

17 (B) a description of how the quantity and purchase aligns to
18 each component or agency’s mission requirements for certification,
19 qualification, training, and operations; and

20 (C) details on all contracting practices applied by the Depart-
21 ment, including comparative details regarding other contracting
22 options with respect to cost and availability.

23 (e) REPORT SUBMITTED IN APPROPRIATE FORMAT.—Each report shall
24 be submitted in an appropriate format to ensure the safety of law enforce-
25 ment personnel.

26 **§ 10391. Clearances**

27 The Secretary shall make available the process of application for security
28 clearances under Executive Order 13549 (50 U.S.C. 3161 note) or any suc-
29 cessor Executive Order to appropriate representatives of sector coordinating
30 councils, sector information sharing and analysis organizations (as defined
31 in section 10531(6) of this title), owners and operators of critical infrastruc-
32 ture, and any other person that the Secretary determines appropriate.

33 **§ 10392. National identification system not authorized**

34 Nothing in this subtitle or the Homeland Security Act of 2002 (Public
35 Law 107–296, 116 Stat. 2135) shall be construed to authorize the develop-
36 ment of a national identification system or card.

37 **§ 10393. Functions and authorities of Administrator of Gen-
38 eral Services not affected**

39 (a) OPERATION, MAINTENANCE, AND PROTECTION OF FEDERAL BUILD-
40 INGS AND GROUNDS.—Nothing in this subtitle may be construed to affect
41 the functions or authorities of the Administrator of General Services with

1 respect to the operation, maintenance, and protection of buildings and
2 grounds owned or occupied by the Federal Government and under the juris-
3 diction, custody, or control of the Administrator. Except for the law enforce-
4 ment and related security functions transferred under section
5 10901(b)(1)(C) of this title, the Administrator shall retain all powers, func-
6 tions, and authorities vested in the Administrator under chapters 1 (except
7 section 121(e)(2)(A)) and 5 through 11 of title 40, and other provisions of
8 law that are necessary for the operation, maintenance, and protection of the
9 buildings and grounds.

10 (b) LIMITATION ON COLLECTION AND USE OF RENTS AND FEES AND
11 FEDERAL BUILDINGS FUND.—

12 (1) STATUTORY CONSTRUCTION.—Nothing in this subtitle may be
13 construed—

14 (A) to direct the transfer of, or affect, the authority of the Ad-
15 ministrator of General Services to collect rents and fees, including
16 fees collected for protective services; or

17 (B) to authorize the Secretary or another official in the Depart-
18 ment to obligate amounts in the Federal Buildings Fund estab-
19 lished by section 592 of title 40.

20 (2) USE OF TRANSFERRED AMOUNTS.—Amounts transferred by the
21 Administrator of General Services to the Secretary out of rents and
22 fees collected by the Administrator shall be used by the Secretary solely
23 for the protection of buildings or grounds owned or occupied by the
24 Federal Government.

25 **§ 10394. Research and development pilot program**

26 (a) AUTHORITY.—Until September 30, 2017, and subject to subsection
27 (c), the Secretary may carry out a pilot program under which, when the
28 Secretary carries out basic, applied, and advanced research and development
29 projects, including the expenditure of funds for the projects, the Secretary
30 may exercise the same authority (subject to the same limitations and condi-
31 tions) with respect to the research and projects as the Secretary of Defense
32 may exercise under section 2371 of title 10 (except for subsections (b) and
33 (f)), after making a determination that the use of a contract, grant, or coop-
34 erative agreement for the project is not feasible or appropriate.

35 (b) PROCUREMENT OF TEMPORARY AND INTERMITTENT SERVICES.—The
36 Secretary may—

37 (1) procure the temporary or intermittent services of experts or con-
38 sultants (or organizations of experts or consultants) in accordance with
39 section 3109(b) of title 5; and

40 (2) whenever necessary due to an urgent homeland security need,
41 procure temporary (not to exceed 1 year) or intermittent personal serv-

- 10544. Enhancement of Federal and non-Federal cybersecurity.
- 10545. National Cybersecurity and Communications Integration Center.
- 10546. Cybersecurity plans.
- 10547. NET Guard.
- 10548. Prohibition on new regulatory authority.
- 10549. Federal intrusion detection and prevention system.
- 10550. Cybersecurity strategy.

Part B—Cybersecurity Information Sharing

- 10561. Definitions
- 10562. Procedures for sharing information by Federal Government.
- 10563. Authorization for preventing, detecting, analyzing, and mitigating cybersecurity threats.
- 10564. Sharing of cyber threat indicators and defensive measures with Federal Government.
- 10565. Protection from liability.
- 10566. Oversight of Government activities.
- 10567. Report on cybersecurity threats.
- 10568. Exception to limitation on authority of Secretary of Defense to disseminate information.
- 10569. Construction and preemption.
- 10570. Effective period.

Part C—Federal Cybersecurity Enhancement

- 10581. Definitions.
- 10582. Advanced internal defenses.
- 10583. Federal cybersecurity requirements.
- 10584. Assessment; reports.

Part D—Other Cyber Matters

- 10591. Apprehension and prosecution of international cyber criminals.
- 10592. Enhancement of emergency services.
- 10593. Improving cybersecurity in the health care industry.

Subchapter IV—Supporting Anti-Terrorism by Fostering Effective Technologies

- 10621. Definitions.
- 10622. Administration.
- 10623. Litigation management.
- 10624. Risk management.

Subchapter V—Secure Handling of Ammonium Nitrate

- 10631. Definitions.
- 10632. Regulation of the sale and transfer of ammonium nitrate.
- 10633. Inspection and auditing of records.
- 10634. Administrative provisions.
- 10635. Theft reporting requirement.
- 10636. Prohibitions and penalty.
- 10637. Protection from civil liability.
- 10638. Preemption of other laws.

Subchapter VI—Chemical Facilities

- 10651. Definitions.
- 10652. Chemical Facility Anti-Terrorism Standards Program.
- 10653. Protection and sharing of information.
- 10654. Civil enforcement.
- 10655. Whistleblower protections.
- 10656. Relationship to other laws.
- 10657. CFATS regulations.
- 10658. Small covered chemical facilities.
- 10659. Outreach to chemical facilities of interest.
- 10660. Termination.

1 **Subchapter I—Directorate for Information**
2 **Analysis and Infrastructure Protection**
3 **§ 10501. Information and analysis and infrastructure protec-**
4 **tion**

- 5 (a) DISCHARGE OF RESPONSIBILITIES.—The Secretary shall ensure that
6 the responsibilities of the Department relating to information analysis and
7 infrastructure protection, including those described in subsection (b), are

1 carried out through the Under Secretary appointed under section
2 10302(b)(1)(H) of this title.

3 (b) RESPONSIBILITIES OF SECRETARY RELATING TO INTELLIGENCE AND
4 ANALYSIS AND INFRASTRUCTURE PROTECTION.—The responsibilities of the
5 Secretary relating to intelligence and analysis and infrastructure protection
6 shall be as follows:

7 (1) To access, receive, and analyze law enforcement information, in-
8 telligence information, and other information from agencies of the Fed-
9 eral Government, State and local government agencies (including law
10 enforcement agencies), and private-sector entities, and to integrate the
11 information, in support of the mission responsibilities of the Depart-
12 ment and the functions of the National Counterterrorism Center estab-
13 lished under section 119 of the National Security Act of 1947 (50
14 U.S.C. 3056), in order to—

15 (A) identify and assess the nature and scope of terrorist threats
16 to the homeland;

17 (B) detect and identify threats of terrorism against the United
18 States; and

19 (C) understand the threats in light of actual and potential
20 vulnerabilities of the homeland.

21 (2) To carry out comprehensive assessments of the vulnerabilities of
22 the key resources and critical infrastructure of the United States, in-
23 cluding the performance of risk assessments to determine the risks
24 posed by particular types of terrorist attacks within the United States
25 (including an assessment of the probability of success of attacks and
26 the feasibility and potential efficacy of various countermeasures to the
27 attacks).

28 (3) To integrate relevant information, analysis, and vulnerability as-
29 sessments (regardless of whether the information, analysis or assess-
30 ments are provided by or produced by the Department) in order to—

31 (A) identify priorities for protective and support measures re-
32 garding terrorist and other threats to homeland security by the
33 Department, other agencies of the Federal Government, State, and
34 local government agencies and authorities, the private sector, and
35 other entities; and

36 (B) prepare finished intelligence and information products in
37 both classified and unclassified formats, as appropriate, whenever
38 reasonably expected to be of benefit to a State, local, or tribal gov-
39 ernment (including a State, local, or tribal law enforcement agen-
40 cy) or a private-sector entity.

1 (4) To ensure, under section 10502 of this title, the timely and effi-
2 cient access by the Department to all information necessary to dis-
3 charge the responsibilities under this section, including obtaining the
4 information from other agencies of the Federal Government.

5 (5) To develop a comprehensive national plan for securing the key
6 resources and critical infrastructure of the United States, including
7 power production, generation, and distribution systems, information
8 technology and telecommunications systems (including satellites), elec-
9 tronic financial and property record storage and transmission systems,
10 emergency preparedness communications systems, and the physical and
11 technological assets that support the systems.

12 (6) To recommend measures necessary to protect the key resources
13 and critical infrastructure of the United States in coordination with
14 other agencies of the Federal Government and in cooperation with
15 State and local government agencies and authorities, the private sector,
16 and other entities.

17 (7) To review, analyze, and make recommendations for improve-
18 ments to the policies and procedures governing the sharing of informa-
19 tion within the scope of the information sharing environment estab-
20 lished under section 11708 of this title, including homeland security in-
21 formation, terrorism information, and weapons of mass destruction in-
22 formation, and policies, guidelines, procedures, instructions, or stand-
23 ards established under that section.

24 (8) To disseminate, as appropriate, information analyzed by the De-
25 partment within the Department, to other agencies of the Federal Gov-
26 ernment with responsibilities relating to homeland security, and to
27 agencies of State and local governments and private-sector entities with
28 equivalent responsibilities in order to assist in the deterrence, preven-
29 tion, preemption of, or response to, terrorist attacks against the United
30 States.

31 (9) To consult with the Director of National Intelligence and other
32 appropriate intelligence, law enforcement, or other elements of the Fed-
33 eral Government to establish collection priorities and strategies for in-
34 formation, including law enforcement-related information, relating to
35 threats of terrorism against the United States through such means as
36 the representation of the Department in discussions regarding require-
37 ments and priorities in the collection of the information.

38 (10) To consult with State and local governments and private-sector
39 entities to ensure appropriate exchanges of information, including law
40 enforcement-related information, relating to threats of terrorism
41 against the United States.

1 (11) To ensure that—

2 (A) material received pursuant to this subtitle is protected from
3 unauthorized disclosure and handled and used only for the per-
4 formance of official duties; and

5 (B) intelligence information under this subtitle is shared, re-
6 tained, and disseminated consistent with the authority of the Di-
7 rector of National Intelligence to protect intelligence sources and
8 methods under the National Security Act of 1947 (50 U.S.C. 3001
9 et seq.) and related procedures and, as appropriate, similar au-
10 thorities of the Attorney General concerning sensitive law enforce-
11 ment information.

12 (12) To request additional information from other agencies of the
13 Federal Government, State and local government agencies, and the pri-
14 vate sector relating to threats of terrorism in the United States, or re-
15 lating to other areas of responsibility assigned by the Secretary, includ-
16 ing the entry into cooperative agreements through the Secretary to ob-
17 tain the information.

18 (13) To establish and utilize, in conjunction with the chief informa-
19 tion officer of the Department, a secure communications and informa-
20 tion technology infrastructure, including data-mining and other ad-
21 vanced analytical tools, in order to access, receive, and analyze data
22 and information in furtherance of the responsibilities under this sec-
23 tion, and to disseminate information acquired and analyzed by the De-
24 partment, as appropriate.

25 (14) To ensure, in conjunction with the chief information officer of
26 the Department, that information databases and analytical tools devel-
27 oped or utilized by the Department—

28 (A) are compatible with one another and with relevant informa-
29 tion databases of other agencies of the Federal Government; and

30 (B) treat information in the databases in a manner that com-
31 plies with applicable Federal law on privacy.

32 (15) To coordinate training and other support to the elements and
33 personnel of the Department, other agencies of the Federal Govern-
34 ment, and State and local governments that provide information to the
35 Department, or are consumers of information provided by the Depart-
36 ment, in order to facilitate the identification and sharing of information
37 revealed in their ordinary duties and the optimal utilization of informa-
38 tion received from the Department.

39 (16) To coordinate with elements of the intelligence community and
40 with Federal, State, and local law enforcement agencies, and the pri-
41 vate sector, as appropriate.

1 (17) To provide intelligence and information analysis and support to
2 other elements of the Department.

3 (18) To coordinate and enhance integration among the intelligence
4 components of the Department, including through strategic oversight of
5 the intelligence activities of the components.

6 (19) To establish the intelligence collection, processing, analysis, and
7 dissemination priorities, policies, processes, standards, guidelines, and
8 procedures for the intelligence components of the Department, con-
9 sistent with directions from the President and, as applicable, the Direc-
10 tor of National Intelligence.

11 (20) To establish a structure and process to support the missions
12 and goals of the intelligence components of the Department.

13 (21) To ensure that, whenever possible, the Department—

14 (A) produces and disseminates unclassified reports and analytic
15 products based on open-source information; and

16 (B) produces and disseminates the reports and analytic prod-
17 ucts contemporaneously with reports or analytic products con-
18 cerning the same or similar information that the Department pro-
19 duced and disseminated in a classified format.

20 (22) To establish within the Office of Intelligence and Analysis an
21 internal continuity of operations plan.

22 (23) Based on intelligence priorities set by the President, and guid-
23 ance from the Secretary and, as appropriate, the Director of National
24 Intelligence—

25 (A) to provide to the heads of each intelligence component of
26 the Department guidance for developing the budget pertaining to
27 the activities of the component; and

28 (B) to present to the Secretary a recommendation for a consoli-
29 dated budget for the intelligence components of the Department,
30 together with comments from the heads of the components.

31 (24) To perform other duties relating to the responsibilities the Sec-
32 retary may provide.

33 (25) To prepare and submit to the Committee on Homeland Security
34 and Governmental Affairs of the Senate and the Committee on Home-
35 land Security in the House of Representatives, and to other appropriate
36 congressional committees having jurisdiction over the critical infra-
37 structure or key resources, for each sector identified in the National
38 Infrastructure Protection Plan, a report on the comprehensive assess-
39 ments carried out by the Secretary of the critical infrastructure and
40 key resources of the United States, evaluating threat, vulnerability, and

1 consequence, as required under this subsection. Each report under this
2 paragraph—

3 (A) shall contain, if applicable, actions or countermeasures rec-
4 ommended or taken by the Secretary or the head of another Fed-
5 eral agency to address issues identified in the assessments;

6 (B) shall be submitted annually and not later than 35 days
7 after the last day of the fiscal year covered by the report; and

8 (C) may be classified.

9 (26)(A) Not later than 6 months after December 23, 2016, to con-
10 duct an intelligence-based review and comparison of the risks and con-
11 sequences of EMP and GMD facing critical infrastructure and submit
12 to the Committee on Homeland Security and the Permanent Select
13 Committee on Intelligence of the House of Representatives and the
14 Committee on Homeland Security and Governmental Affairs and the
15 Select Committee on Intelligence of the Senate a recommended strategy
16 to protect and prepare the critical infrastructure of the homeland
17 against threats of EMP and GMD. The recommended strategy shall—

18 (i) be based on findings of the research and development con-
19 ducted under section 10718 of this title;

20 (ii) be developed in consultation with the relevant Federal sec-
21 tor-specific agencies (as defined under Presidential Policy Direc-
22 tive–21) for critical infrastructure;

23 (iii) be developed in consultation with the relevant sector coordi-
24 nating councils for critical infrastructure;

25 (iv) be informed, to the extent practicable, by the findings of the
26 intelligence-based review and comparison of the risks and con-
27 sequences of EMP and GMD facing critical infrastructure; and

28 (v) be submitted in unclassified form, but may include a classi-
29 fied annex.

30 (B) Not less frequently than every 2 years after the strategy is sub-
31 mitted, for the next 6 years, to submit updates of the recommended
32 strategy.

33 (C) The Secretary, if appropriate, may incorporate the recommended
34 strategy into a broader recommendation developed by the Department
35 to help protect and prepare critical infrastructure from terrorism,
36 cyberattacks, and other threats if, as incorporated, the recommended
37 strategy complies with subparagraph (A).

38 (e) STAFF.—

39 (1) IN GENERAL.—The Secretary shall provide the Office of Intel-
40 ligence and Analysis and the Office of Infrastructure Protection with

1 a staff of analysts having appropriate expertise and experience to assist
2 the offices in discharging responsibilities under this section.

3 (2) PRIVATE-SECTOR ANALYSTS.—Analysts under this subsection
4 may include analysts from the private sector.

5 (3) SECURITY CLEARANCES.—Analysts under this subsection shall
6 possess security clearances appropriate for their work under this sec-
7 tion.

8 (d) DETAIL OF PERSONNEL.—

9 (1) IN GENERAL.—In order to assist the Office of Intelligence and
10 Analysis and the Office of Infrastructure Protection in discharging re-
11 sponsibilities under this section, personnel of the agencies listed in
12 paragraph (2) may be detailed to the Department for the performance
13 of analytic functions and related duties.

14 (2) COVERED AGENCIES.—The agencies referred to in paragraph (1)
15 are as follows:

16 (A) The Department of State.

17 (B) The Central Intelligence Agency.

18 (C) The Federal Bureau of Investigation.

19 (D) The National Security Agency.

20 (E) The National Geospatial-Intelligence Agency.

21 (F) The Defense Intelligence Agency.

22 (G) Any other agency of the Federal Government that the
23 President considers appropriate.

24 (3) COOPERATIVE AGREEMENTS.—The Secretary and the head of the
25 agency concerned may enter into cooperative agreements for the pur-
26 pose of detailing personnel under this subsection.

27 (4) BASIS.—The detail of personnel under this subsection may be on
28 a reimbursable or non-reimbursable basis.

29 (e) FUNCTIONS TRANSFERRED.—The Secretary succeeds to, and there is
30 assigned to the Office of Intelligence and Analysis and the Office of Infra-
31 structure Protection, the functions, personnel, assets, and liabilities of the
32 following entities:

33 (1) The National Infrastructure Protection Center of the Federal
34 Bureau of Investigation (other than the Computer Investigations and
35 Operations Section), including the functions of the Attorney General
36 relating thereto.

37 (2) The National Communications System of the Department of De-
38 fense, including the functions of the Secretary of Defense relating
39 thereto.

1 (3) The Critical Infrastructure Assurance Office of the Department
2 of Commerce, including the functions of the Secretary of Commerce re-
3 lating thereto.

4 (4) The National Infrastructure Simulation and Analysis Center of
5 the Department of Energy and the energy security and assurance pro-
6 gram and activities of the Department, including the functions of the
7 Secretary of Energy relating thereto.

8 (5) The Federal Computer Incident Response Center of the General
9 Services Administration, including the functions of the Administrator
10 of General Services relating thereto.

11 **§ 10502. Access to information**

12 (a) IN GENERAL.—

13 (1) THREAT AND VULNERABILITY INFORMATION.—Except as other-
14 wise directed by the President, the Secretary shall have access the Sec-
15 retary considers necessary to all information, including reports, assess-
16 ments, analyses, and unevaluated intelligence relating to threats of ter-
17 rorism against the United States and to other areas of responsibility
18 assigned by the Secretary, and to all information concerning infrastruc-
19 ture or other vulnerabilities of the United States to terrorism, whether
20 or not the information has been analyzed, that may be collected, pos-
21 sessed, or prepared by an agency of the Federal Government.

22 (2) OTHER INFORMATION.—The Secretary also shall have access to
23 other information relating to matters under the responsibility of the
24 Secretary that may be collected, possessed, or prepared by an agency
25 of the Federal Government as the President may further provide.

26 (b) MANNER OF ACCESS.—Except as otherwise directed by the President,
27 with respect to information to which the Secretary has access under this
28 section—

29 (1) the Secretary may obtain the material upon request, and may
30 enter into cooperative arrangements with other executive agencies to
31 provide the material or provide Department officials with access to it
32 on a regular or routine basis, including requests or arrangements in-
33 volving broad categories of material, access to electronic databases, or
34 both; and

35 (2) regardless of whether the Secretary has made a request or en-
36 tered into a cooperative arrangement under paragraph (1), all agencies
37 of the Federal Government shall promptly provide to the Secretary—

38 (A) all reports (including information reports containing intel-
39 ligence which has not been fully evaluated), assessments, and ana-
40 lytical information relating to threats of terrorism against the

1 United States and to other areas of responsibility assigned by the
2 Secretary;

3 (B) all information concerning the vulnerability of the infra-
4 structure of the United States, or other vulnerabilities of the
5 United States, to terrorism, whether or not the information has
6 been analyzed;

7 (C) all other information relating to significant and credible
8 threats of terrorism against the United States, whether or not the
9 information has been analyzed; and

10 (D) other information or material as the President may direct.

11 (e) TREATMENT UNDER CERTAIN LAWS.—The Secretary shall be deemed
12 to be a Federal law enforcement, intelligence, protective, national defense,
13 immigration, or national security official, and shall be provided with all in-
14 formation from law enforcement agencies that is required to be given to the
15 Director of Central Intelligence, under any provision of the following:

16 (1) The USA PATRIOT Act (Public Law 107–56, 115 Stat. 272).

17 (2) Section 2517(6) of title 18.

18 (3) Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure (18
19 App. U.S.C.).

20 (d) ACCESS TO INTELLIGENCE AND OTHER INFORMATION.—

21 (1) ACCESS BY ELEMENTS OF FEDERAL GOVERNMENT.—Nothing
22 in this chapter shall preclude an element of the intelligence community
23 (as that term is defined in section 3 of the National Security Act of
24 1947 (50 U.S.C. 3003)), or any other element of the Federal Govern-
25 ment with responsibility for analyzing terrorist threat information,
26 from receiving intelligence or other information relating to terrorism.

27 (2) SHARING OF INFORMATION.—The Secretary, in consultation
28 with the Director of Central Intelligence, shall work to ensure that in-
29 telligence or other information relating to terrorism to which the De-
30 partment has access is appropriately shared with the elements of the
31 Federal Government referred to in paragraph (1), as well as with State
32 and local governments, as appropriate.

33 **§ 10503. Terrorist travel program**

34 (a) REQUIREMENT TO ESTABLISH.—The Secretary, in consultation with
35 the Director of the National Counterterrorism Center and consistent with
36 the strategy developed under section 7201 of the Intelligence Reform and
37 Terrorism Prevention Act of 2004 (Public Law 108–458, 50 U.S.C. 3056
38 note), shall establish a program to oversee the implementation of the Sec-
39 retary’s responsibilities with respect to terrorist travel.

1 (b) HEAD OF THE PROGRAM.—The Secretary shall designate an official
 2 of the Department to be responsible for carrying out the program. The offi-
 3 cial shall be—

4 (1) the Assistant Secretary for Policy; or

5 (2) an official appointed by the Secretary who reports directly to the
 6 Secretary.

7 (c) DUTIES.—The official designated under subsection (b) shall assist the
 8 Secretary in improving the Department’s ability to prevent terrorists from
 9 entering the United States or remaining in the United States undetected
 10 by—

11 (1) developing relevant strategies and policies;

12 (2) reviewing the effectiveness of existing programs and recom-
 13 mending improvements, if necessary;

14 (3) making recommendations on budget requests and on the alloca-
 15 tion of funding and personnel;

16 (4) ensuring effective coordination, with respect to policies, pro-
 17 grams, planning, operations, and dissemination of intelligence and in-
 18 formation relating to terrorist travel—

19 (A) among appropriate subdivisions of the Department, as de-
 20 termined by the Secretary and including—

21 (i) U.S. Customs and Border Protection;

22 (ii) U.S. Immigration and Customs Enforcement;

23 (iii) U.S. Citizenship and Immigration Services;

24 (iv) the Transportation Security Administration; and

25 (v) the Coast Guard; and

26 (B) between the Department and other appropriate Federal
 27 agencies; and

28 (5) serving as the Secretary’s primary point of contact with the Na-
 29 tional Counterterrorism Center for implementing initiatives related to
 30 terrorist travel and ensuring that the recommendations of the Center
 31 related to terrorist travel are carried out by the Department.

32 **§ 10504. Homeland Security Advisory System**

33 (a) IN GENERAL.—The Secretary shall administer the Homeland Security
 34 Advisory System under this section to provide advisories or warnings re-
 35 garding the threat or risk that acts of terrorism will be committed on the
 36 homeland to Federal, State, local, and tribal government authorities and to
 37 the people of the United States, as appropriate. The Secretary shall exercise
 38 primary responsibility for providing the advisories or warnings.

39 (b) REQUIRED ELEMENTS.—In administering the Homeland Security Ad-
 40 visory System, the Secretary shall—

- 1 (1) establish criteria for the issuance and revocation of the advisories
2 or warnings;
- 3 (2) develop a methodology, relying on the criteria established under
4 paragraph (1), for the issuance and revocation of the advisories or
5 warnings;
- 6 (3) provide, in each advisory or warning, specific information and ad-
7 vice regarding appropriate protective measures and countermeasures
8 that may be taken in response to the threat or risk, at the maximum
9 level of detail practicable, to enable individuals, government entities,
10 emergency response providers, and the private sector to act appro-
11 priately;
- 12 (4) whenever possible, limit the scope of each advisory or warning
13 to a specific region, locality, or economic sector believed to be under
14 threat or at risk; and
- 15 (5) not, in issuing an advisory or warning, use color designations as
16 the exclusive means of specifying homeland security threat conditions
17 that are the subject of the advisory or warning.

18 **§ 10505. Homeland security information sharing**

19 (a) INFORMATION SHARING.—Consistent with section 11708 of this title,
20 the Secretary, acting through the Under Secretary for Intelligence and
21 Analysis, shall integrate the information and standardize the format of the
22 products of the intelligence components of the Department containing home-
23 land security information, terrorism information, weapons of mass destruc-
24 tion information, or national intelligence (as defined in section 3 of the Na-
25 tional Security Act of 1947 (50 U.S.C. 3003)) except for internal security
26 protocols or personnel information of the intelligence components, or other
27 administrative processes that are administered by any chief security officer
28 of the Department.

29 (b) INFORMATION SHARING AND KNOWLEDGE MANAGEMENT OFFI-
30 CERS.—For each intelligence component of the Department, the Secretary
31 shall designate an information sharing and knowledge management officer
32 who shall report to the Under Secretary for Intelligence and Analysis re-
33 garding coordinating the different systems used in the Department to gath-
34 er and disseminate homeland security information or national intelligence
35 (as defined in section 3 of the National Security Act of 1947 (50 U.S.C.
36 3003)).

37 (c) STATE, LOCAL, AND PRIVATE-SECTOR SOURCES OF INFORMATION.—

38 (1) ESTABLISHMENT OF BUSINESS PROCESSES.—The Secretary, act-
39 ing through the Under Secretary for Intelligence and Analysis or the
40 Assistant Secretary for Infrastructure Protection, as appropriate,
41 shall—

1 (A) establish Department-wide procedures for the review and
2 analysis of information provided by State, local, and tribal govern-
3 ments and the private sector;

4 (B) as appropriate, integrate the information into the informa-
5 tion gathered by the Department and other departments and agen-
6 cies of the Federal Government; and

7 (C) make available the information, as appropriate, within the
8 Department and to other departments and agencies of the Federal
9 Government.

10 (2) FEEDBACK.—The Secretary shall develop mechanisms to provide
11 feedback regarding the analysis and utility of information provided by
12 an entity of State, local, or tribal government or the private sector that
13 provides the information to the Department.

14 (d) TRAINING AND EVALUATION OF EMPLOYEES.—

15 (1) TRAINING.—The Secretary, acting through the Under Secretary
16 for Intelligence and Analysis or the Assistant Secretary for Infrastruc-
17 ture Protection, as appropriate, shall provide to employees of the De-
18 partment opportunities for training and education to develop an under-
19 standing of—

20 (A) the definitions of homeland security information and na-
21 tional intelligence (as defined in section 3 of the National Security
22 Act of 1947 (50 U.S.C. 3003)); and

23 (B) how information available to the employees as part of their
24 duties—

25 (i) might qualify as homeland security information or na-
26 tional intelligence; and

27 (ii) might be relevant to the Office of Intelligence and
28 Analysis and the intelligence components of the Department.

29 (2) EVALUATIONS.—The Under Secretary for Intelligence and Anal-
30 ysis shall—

31 (A) on an ongoing basis, evaluate how employees of the Office
32 of Intelligence and Analysis and the intelligence components of the
33 Department are utilizing homeland security information or na-
34 tional intelligence, sharing information within the Department, as
35 described in this title, and participating in the information sharing
36 environment established under section 11708 of this title; and

37 (B) provide to the appropriate component heads regular reports
38 regarding the evaluations under subparagraph (A).

39 (e) RECEIPT OF INFORMATION FROM UNITED STATES SECRET SERV-
40 ICE.—

1 (1) IN GENERAL.—The Under Secretary for Intelligence and Anal-
 2 ysis shall receive from the United States Secret Service homeland secu-
 3 rity information, terrorism information, weapons of mass destruction
 4 information (as these terms are defined in section 11708 of this title),
 5 or national intelligence (as defined in section 3 of the National Security
 6 Act of 1947 (50 U.S.C. 3003)), as well as suspect information obtained
 7 in criminal investigations. The United States Secret Service shall co-
 8 operate with the Under Secretary for Intelligence and Analysis with re-
 9 spect to activities under this section and section 10506 of this title.

10 (2) SAVINGS CLAUSE.—Nothing in the Implementing Recommenda-
 11 tions of the 9/11 Commission Act of 2007 (Public Law 110–53, 121
 12 Stat. 266) shall interfere with the operation of section 3056(g) of title
 13 18, or with the authority of the Secretary or the Director of the United
 14 States Secret Service regarding the budget of the United States Secret
 15 Service.

16 **§ 10506. Comprehensive information technology network ar-**
 17 **chitecture**

18 (a) DEFINITION OF COMPREHENSIVE INFORMATION TECHNOLOGY NET-
 19 WORK ARCHITECTURE.—The term “comprehensive information technology
 20 network architecture” means an integrated framework for evolving or main-
 21 taining existing information technology and acquiring new information tech-
 22 nology to achieve the strategic management and information resources man-
 23 agement goals of the Office of Intelligence and Analysis.

24 (b) ESTABLISHMENT.—The Secretary, acting through the Under Sec-
 25 retary for Intelligence and Analysis, shall establish, consistent with the poli-
 26 cies and procedures developed under section 11708 of this title, and con-
 27 sistent with the enterprise architecture of the Department, a comprehensive
 28 information technology network architecture for the Office of Intelligence
 29 and Analysis that connects the various databases and related information
 30 technology assets of the Office of Intelligence and Analysis and the intel-
 31 ligence components of the Department in order to promote internal informa-
 32 tion sharing among the intelligence and other personnel of the Department.

33 **§ 10507. Coordination with information sharing environ-**
 34 **ment**

35 (a) GUIDANCE.—All activities to comply with sections 10504, 10505, and
 36 10506 of this title shall be—

37 (1) consistent with policies, guidelines, procedures, instructions, or
 38 standards established under section 11708 of this title;

39 (2) implemented in coordination with, as appropriate, the program
 40 manager for the information sharing environment established under
 41 that section;

1 (3) consistent with applicable guidance issued by the Director of Na-
2 tional Intelligence; and

3 (4) consistent with applicable guidance issued by the Secretary relat-
4 ing to the protection of law enforcement information or proprietary in-
5 formation.

6 (b) CONSULTATION.—In carrying out the duties and responsibilities
7 under this subchapter, the Under Secretary for Intelligence and Analysis
8 shall take into account the views of the heads of the intelligence components
9 of the Department.

10 **§ 10508. Intelligence components**

11 Subject to the direction and control of the Secretary, and consistent with
12 applicable guidance issued by the Director of National Intelligence, the re-
13 sponsibilities of the head of each intelligence component of the Department
14 are as follows:

15 (1) To ensure that the collection, processing, analysis, and dissemi-
16 nation of information within the scope of the information sharing envi-
17 ronment, including homeland security information, terrorism informa-
18 tion, weapons of mass destruction information, and national intelligence
19 (as defined in section 3 of the National Security Act of 1947 (50
20 U.S.C. 3003)), are carried out effectively and efficiently in support of
21 the intelligence mission of the Department, as led by the Under Sec-
22 retary for Intelligence and Analysis.

23 (2) To otherwise support and implement the intelligence mission of
24 the Department, as led by the Under Secretary for Intelligence and
25 Analysis.

26 (3) To incorporate the input of the Under Secretary for Intelligence
27 and Analysis with respect to performance appraisals, bonus or award
28 recommendations, pay adjustments, and other forms of commendation.

29 (4) To coordinate with the Under Secretary for Intelligence and
30 Analysis in developing policies and requirements for the recruitment
31 and selection of intelligence officials of the intelligence component.

32 (5) To advise and coordinate with the Under Secretary for Intel-
33 ligence and Analysis on any plan to reorganize or restructure the intel-
34 ligence component that would, if implemented, result in realignments
35 of intelligence functions.

36 (6) To ensure that employees of the intelligence component have
37 knowledge of, and comply with, the programs and policies established
38 by the Under Secretary for Intelligence and Analysis and other appro-
39 priate officials of the Department and that the employees comply with
40 all applicable laws and regulations.

1 (7) To perform other activities relating to the responsibilities that
2 the Secretary may provide.

3 **§ 10509. Training for employees of intelligence components**

4 The Secretary shall provide training and guidance for employees, officials,
5 and senior executives of the intelligence components of the Department to
6 develop knowledge of laws, regulations, operations, policies, procedures, and
7 programs that are related to the functions of the Department relating to
8 the collection, processing, analysis, and dissemination of information within
9 the scope of the information sharing environment, including homeland secu-
10 rity information, terrorism information, and weapons of mass destruction
11 information, or national intelligence (as the term is defined in section 3 of
12 the National Security Act of 1947 (50 U.S.C. 3003)).

13 **§ 10510. Intelligence training development for State and**
14 **local government officials**

15 (a) CURRICULUM.—The Secretary, acting through the Under Secretary
16 for Intelligence and Analysis, shall—

17 (1) develop a curriculum for training State, local, and tribal govern-
18 ment officials, including law enforcement officers, intelligence analysts,
19 and other emergency response providers, in the intelligence cycle and
20 Federal laws, practices, and regulations regarding the development,
21 handling, and review of intelligence and other information; and

22 (2) ensure that the curriculum includes executive level training for
23 senior level State, local, and tribal law enforcement officers, intelligence
24 analysts, and other emergency response providers.

25 (b) TRAINING.—To the extent possible, the Federal Law Enforcement
26 Training Center and other existing Federal entities with the capacity and
27 expertise to train State, local, and tribal government officials based on the
28 curriculum developed under subsection (a) shall be used to carry out the
29 training programs created under this section. If the entities do not have the
30 capacity, resources, or capabilities to conduct the training, the Secretary
31 may approve another entity to conduct the training.

32 (c) CONSULTATION.—In carrying out the duties described in subsection
33 (a), the Under Secretary for Intelligence and Analysis shall consult with the
34 Director of the Federal Law Enforcement Training Center, the Attorney
35 General, the Director of National Intelligence, the Administrator of the Fed-
36 eral Emergency Management Agency, and other appropriate parties, such
37 as private industry, institutions of higher education, nonprofit institutions,
38 and other intelligence agencies of the Federal Government.

39 **§ 10511. Information sharing incentives**

40 (a) AWARDS.—In making cash awards under chapter 45 of title 5, the
41 President or the head of an agency, in consultation with the program man-

1 ager designated under section 11708 of this title, may consider the success
 2 of an employee in appropriately sharing information within the scope of the
 3 information sharing environment established under that section, including
 4 homeland security information, terrorism information, and weapons of mass
 5 destruction information, or national intelligence (as defined in section 3 of
 6 the National Security Act of 1947 (50 U.S.C. 3003)), in a manner con-
 7 sistent with policies, guidelines, procedures, instructions, or standards estab-
 8 lished by the President or, as appropriate, the program manager of that en-
 9 vironment for the implementation and management of that environment.

10 (b) OTHER INCENTIVES.—The head of each department or agency de-
 11 scribed in section 11708(g), in consultation with the program manager des-
 12 ignated under section 11708, shall adopt best practices regarding effective
 13 ways to educate and motivate officers and employees of the Federal Govern-
 14 ment to participate fully in the information sharing environment, includ-
 15 ing—

16 (1) promotions and other nonmonetary awards; and

17 (2) the publicizing of information sharing accomplishments by indi-
 18 vidual employees and, where appropriate, the tangible end benefits that
 19 resulted.

20 **§ 10512. Department of Homeland Security State, Local, and**
 21 **Regional Fusion Center initiative**

22 (a) DEFINITIONS.—In this section:

23 (1) FUSION CENTER.—The term “fusion center” means a collabor-
 24 ative effort of two or more Federal, State, local, or tribal government
 25 agencies that combines resources, expertise, or information with the
 26 goal of maximizing the ability of the agencies to detect, prevent, inves-
 27 tigate, apprehend, and respond to criminal or terrorist activity.

28 (2) INFORMATION SHARING ENVIRONMENT.—The term “information
 29 sharing environment” means the information sharing environment es-
 30 tablished under section 11708 of this title.

31 (3) INTELLIGENCE ANALYST.—The term “intelligence analyst”
 32 means an individual who regularly advises, administers, supervises, or
 33 performs work in the collection, gathering, analysis, evaluation, report-
 34 ing, production, or dissemination of information on political, economic,
 35 social, cultural, physical, geographical, scientific, or military conditions,
 36 trends, or forces in foreign or domestic areas that directly or indirectly
 37 affect national security.

38 (4) INTELLIGENCE-LED POLICING.—The term “intelligence-led polic-
 39 ing” means the collection and analysis of information to produce an in-
 40 telligence end product designed to inform law enforcement decision-
 41 making at the tactical and strategic levels.

1 (5) TERRORISM INFORMATION.—The term “terrorism information”
2 has the meaning given the term in section 11708 of this title.

3 (b) ESTABLISHMENT.—The Secretary, in consultation with the program
4 manager of the information sharing environment established under section
5 11708 of this title, the Attorney General, the Privacy Officer of the Depart-
6 ment, the Officer for Civil Rights and Civil Liberties of the Department,
7 and the Privacy and Civil Liberties Oversight Board established under sec-
8 tion 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004
9 (42 U.S.C. 2000ee), shall establish a Department of Homeland Security
10 State, Local, and Regional Fusion Center Initiative to establish partnerships
11 with State, local, and regional fusion centers.

12 (c) DEPARTMENT SUPPORT AND COORDINATION.—Through the Depart-
13 ment of Homeland Security State, Local, and Regional Fusion Center Ini-
14 tiative, and in coordination with the principal officials of participating State,
15 local, or regional fusion centers and the officers designated as the Homeland
16 Security Advisors of the States, the Secretary shall—

17 (1) provide operational and intelligence advice and assistance to
18 State, local, and regional fusion centers;

19 (2) support efforts to include State, local, and regional fusion centers
20 into efforts to establish an information sharing environment;

21 (3) conduct tabletop and live training exercises to regularly assess
22 the capability of individual and regional networks of State, local, and
23 regional fusion centers to integrate the efforts of the networks with the
24 efforts of the Department;

25 (4) coordinate with other relevant Federal entities engaged in home-
26 land security-related activities;

27 (5) provide analytic and reporting advice and assistance to State,
28 local, and regional fusion centers;

29 (6) review information within the scope of the information sharing
30 environment, including homeland security information, terrorism infor-
31 mation, and weapons of mass destruction information, that is gathered
32 by State, local, and regional fusion centers, and to incorporate the in-
33 formation, as appropriate, into the Department’s own information;

34 (7) provide management assistance to State, local, and regional fu-
35 sion centers;

36 (8) serve as a point of contact to ensure the dissemination of infor-
37 mation within the scope of the information sharing environment, in-
38 cluding homeland security information, terrorism information, and
39 weapons of mass destruction information;

40 (9) facilitate close communication and coordination between State,
41 local, and regional fusion centers and the Department;

1 (10) provide State, local, and regional fusion centers with expertise
2 on Department resources and operations;

3 (11) provide training to State, local, and regional fusion centers and
4 encourage the fusion centers to participate in terrorism threat-related
5 exercises conducted by the Department; and

6 (12) carry out other duties the Secretary determines are appropriate.

7 (d) PERSONNEL ASSIGNMENT.—

8 (1) IN GENERAL.—The Under Secretary for Intelligence and Anal-
9 ysis shall, to the maximum extent practicable, assign officers and intel-
10 ligence analysts from components of the Department to participating
11 State, local, and regional fusion centers.

12 (2) PERSONNEL SOURCES.—Officers and intelligence analysts as-
13 signed to participating fusion centers under this subsection may be as-
14 signed from the following Department components, in coordination with
15 the respective component head and in consultation with the principal
16 officials of participating fusion centers:

17 (A) Office of Intelligence and Analysis.

18 (B) Office of Infrastructure Protection.

19 (C) Transportation Security Administration.

20 (D) U.S. Customs and Border Protection.

21 (E) U.S. Immigration and Customs Enforcement.

22 (F) Coast Guard.

23 (G) Other components of the Department, as determined by the
24 Secretary.

25 (3) QUALIFYING CRITERIA.—

26 (A) IN GENERAL.—The Secretary shall develop qualifying cri-
27 teria for a fusion center to participate in the assigning of Depart-
28 ment officers or intelligence analysts under this section.

29 (B) CRITERIA.—Criteria developed under subparagraph (A)
30 may include—

31 (i) whether the fusion center, through its mission and gov-
32 ernance structure, focuses on a broad counterterrorism ap-
33 proach, and whether that broad approach is pervasive
34 through all levels of the organization;

35 (ii) whether the fusion center has sufficient numbers of
36 adequately trained personnel to support a broad counterter-
37 rorism mission;

38 (iii) whether the fusion center has—

39 (I) access to relevant law enforcement, emergency re-
40 sponse, private sector, open source, and national security
41 data; and

1 (II) the ability to share and analytically utilize that
2 data for lawful purposes;

3 (iv) whether the fusion center is adequately funded by the
4 State, local, or regional government to support its counterter-
5 rorism mission; and

6 (v) the relevancy of the mission of the fusion center to the
7 particular source component of Department officers or intel-
8 ligence analysts.

9 (4) PREREQUISITE.—

10 (A) INTELLIGENCE ANALYSIS, PRIVACY, AND CIVIL LIBERTIES
11 TRAINING.—Before being assigned to a fusion center under this
12 section, an officer or intelligence analyst shall undergo—

13 (i) appropriate intelligence analysis or information sharing
14 training using an intelligence-led policing curriculum that is
15 consistent with—

16 (I) standard training and education programs offered
17 to Department law enforcement and intelligence per-
18 sonnel; and

19 (II) the Criminal Intelligence Systems Operating Poli-
20 cies under part 23 of title 28, Code of Federal Regula-
21 tions (or a corresponding similar rule or regulation);

22 (ii) appropriate privacy and civil liberties training that is
23 developed, supported, or sponsored by the Privacy Officer ap-
24 pointed under section 10543 of this title and the Officer for
25 Civil Rights and Civil Liberties of the Department, in con-
26 sultation with the Privacy and Civil Liberties Oversight
27 Board established under section 1061 of the Intelligence Re-
28 form and Terrorism Prevention Act of 2004 (42 U.S.C.
29 2000ee); and

30 (iii) other training prescribed by the Under Secretary for
31 Intelligence and Analysis.

32 (B) PRIOR WORK EXPERIENCE IN AREA.—In determining the
33 eligibility of an officer or intelligence analyst to be assigned to a
34 fusion center under this section, the Under Secretary for Intel-
35 ligence and Analysis shall consider the familiarity of the officer or
36 intelligence analyst with the State, locality, or region, as deter-
37 mined by such factors as whether the officer or intelligence ana-
38 lyst—

39 (i) has been previously assigned in the geographic area; or

1 (ii) has previously worked with intelligence officials or law
2 enforcement or other emergency response providers from that
3 State, locality, or region.

4 (5) EXPEDITED SECURITY CLEARANCE PROCESSING.—The Under
5 Secretary for Intelligence and Analysis—

6 (A) shall ensure that each officer or intelligence analyst as-
7 signed to a fusion center under this section has the appropriate
8 security clearance to contribute effectively to the mission of the fu-
9 sion center; and

10 (B) may request that security clearance processing be expedited
11 for each officer or intelligence analyst and may use available funds
12 for this purpose.

13 (6) ADDITIONAL QUALIFICATIONS.—Each officer or intelligence ana-
14 lyst assigned to a fusion center under this section shall satisfy any
15 other qualifications the Under Secretary for Intelligence and Analysis
16 may prescribe.

17 (e) RESPONSIBILITIES.—An officer or intelligence analyst assigned to a
18 fusion center under this section shall—

19 (1) assist law enforcement agencies and other emergency response
20 providers of State, local, and tribal governments and fusion center per-
21 sonnel in using information within the scope of the information sharing
22 environment, including homeland security information, terrorism infor-
23 mation, and weapons of mass destruction information, to develop a
24 comprehensive and accurate threat picture;

25 (2) review homeland security-relevant information from law enforce-
26 ment agencies and other emergency response providers of State, local,
27 and tribal government;

28 (3) create intelligence and other information products derived from
29 the information and other homeland security-relevant information pro-
30 vided by the Department; and

31 (4) assist in the dissemination of the products, as coordinated by the
32 Under Secretary for Intelligence and Analysis, to law enforcement
33 agencies and other emergency response providers of State, local, and
34 tribal government, other fusion centers, and appropriate Federal agen-
35 cies.

36 (f) BORDER INTELLIGENCE PRIORITY.—

37 (1) IN GENERAL.—The Secretary shall make it a priority to assign
38 officers and intelligence analysts under this section from U.S. Customs
39 and Border Protection, U.S. Immigration and Customs Enforcement,
40 and the Coast Guard to participating State, local, and regional fusion
41 centers located in jurisdictions along land or maritime borders of the

1 United States in order to enhance the integrity of and security at the
2 borders by helping Federal, State, local, and tribal law enforcement au-
3 thorities to identify, investigate, and otherwise interdict persons, weap-
4 ons, and related contraband that pose a threat to homeland security.

5 (2) BORDER INTELLIGENCE PRODUCTS.—When performing the re-
6 sponsibilities described in subsection (e), officers and intelligence ana-
7 lysts assigned to participating State, local, and regional fusion centers
8 under this section shall have, as a primary responsibility, the creation
9 of border intelligence products that—

10 (A) assist State, local, and tribal law enforcement agencies in
11 deploying their resources most efficiently to help detect and inter-
12 dict terrorists, weapons of mass destruction, and related contra-
13 band at land or maritime borders of the United States;

14 (B) promote more consistent and timely sharing of border secu-
15 rity-relevant information among jurisdictions along land or mari-
16 time borders of the United States; and

17 (C) enhance the Department’s situational awareness of the
18 threat of acts of terrorism at or involving the land or maritime
19 borders of the United States.

20 (g) DATABASE ACCESS.—To fulfill the objectives described under sub-
21 section (e), each officer or intelligence analyst assigned to a fusion center
22 under this section shall have appropriate access to all relevant Federal data-
23 bases and information systems, consistent with policies, guidelines, proce-
24 dures, instructions, or standards established by the President or, as appro-
25 priate, the program manager of the information sharing environment for the
26 implementation and management of that environment.

27 (h) CONSUMER FEEDBACK.—

28 (1) IN GENERAL.—The Secretary shall create a voluntary mechanism
29 for a State, local, or tribal law enforcement officer or other emergency
30 response provider who is a consumer of the intelligence or other infor-
31 mation products referred to in subsection (e) to provide feedback to the
32 Department on the quality and utility of the intelligence products.

33 (2) REPORT.—The Secretary shall submit annually to the Committee
34 on Homeland Security and Governmental Affairs of the Senate and the
35 Committee on Homeland Security of the House of Representatives a
36 report that includes a description of the consumer feedback obtained
37 under paragraph (1) and, if applicable, how the Department has ad-
38 justed its production of intelligence products in response to that con-
39 sumer feedback.

40 (i) RULE OF CONSTRUCTION.—

1 (1) IN GENERAL.—The authorities granted under this section shall
2 supplement the authorities granted under section 10501(b) of this title,
3 and nothing in this section shall be construed to abrogate the authori-
4 ties granted under section 10501(b).

5 (2) PARTICIPATION.—Nothing in this section shall be construed to
6 require a State, local, or regional government or entity to accept the
7 assignment of officers or intelligence analysts of the Department into
8 the fusion center of that State, locality, or region.

9 (j) GUIDELINES.—The Secretary, in consultation with the Attorney Gen-
10 eral, shall establish guidelines for fusion centers created and operated by
11 State and local governments, to include standards that a fusion center
12 shall—

13 (1) collaboratively develop a mission statement, identify expectations
14 and goals, measure performance, and determine effectiveness for that
15 fusion center;

16 (2) create a representative governance structure that includes law
17 enforcement officers and other emergency response providers and, as
18 appropriate, the private sector;

19 (3) create a collaborative environment for the sharing of intelligence
20 and information among Federal, State, local, and tribal government
21 agencies (including law enforcement officers and other emergency re-
22 sponse providers), the private sector, and the public, consistent with
23 policies, guidelines, procedures, instructions, or standards established
24 by the President or, as appropriate, the program manager of the infor-
25 mation sharing environment;

26 (4) leverage the databases, systems, and networks available from
27 public- and private-sector entities, in accordance with all applicable
28 laws, to maximize information sharing;

29 (5) develop, publish, and adhere to a privacy and civil liberties policy
30 consistent with Federal, State, and local law;

31 (6) provide, in coordination with the Privacy Officer of the Depart-
32 ment and the Officer for Civil Rights and Civil Liberties of the Depart-
33 ment, appropriate privacy and civil liberties training for all State, local,
34 tribal, and private-sector representatives at the fusion center;

35 (7) ensure appropriate security measures are in place for the facility,
36 data, and personnel;

37 (8) select and train personnel based on the needs, mission, goals, and
38 functions of that fusion center;

39 (9) offer a variety of intelligence and information services and prod-
40 ucts to recipients of fusion center intelligence and information; and

1 (10) incorporate law enforcement officers, other emergency response
2 providers, and, as appropriate, the private sector, into all relevant
3 phases of the intelligence and fusion process, consistent with the mis-
4 sion statement developed under paragraph (1), either through full time
5 representatives or liaison relationships with the fusion center to enable
6 the receipt and sharing of information and intelligence.

7 **§ 10513. Homeland Security Information Sharing Fellows**
8 **Program**

9 (a) ESTABLISHMENT.—The Secretary, acting through the Under Sec-
10 retary for Intelligence and Analysis, and in consultation with the Chief
11 Human Capital Officer, shall establish the Homeland Security Information
12 Sharing Fellows Program for the purpose of—

13 (1) detailing State, local, and tribal law enforcement officers and in-
14 telligence analysts to the Department in accordance with subchapter VI
15 of chapter 33 of title 5, to participate in the work of the Office of Intel-
16 ligence and Analysis in order to become familiar with—

17 (A) the relevant missions and capabilities of the Department
18 and other Federal agencies; and

19 (B) the role, programs, products, and personnel of the Office of
20 Intelligence and Analysis; and

21 (2) promoting information sharing between the Department and
22 State, local, and tribal law enforcement officers and intelligence ana-
23 lysts by assigning the officers and analysts to—

24 (A) serve as a point of contact in the Department to assist in
25 the representation of State, local, and tribal information require-
26 ments;

27 (B) identify information within the scope of the information
28 sharing environment, including homeland security information, ter-
29 rorism information, and weapons of mass destruction information,
30 that is of interest to State, local, and tribal law enforcement offi-
31 cers, intelligence analysts, and other emergency response pro-
32 viders;

33 (C) assist Department analysts in preparing and disseminating
34 products derived from information within the scope of the informa-
35 tion sharing environment, including homeland security informa-
36 tion, terrorism information, and weapons of mass destruction in-
37 formation, that are tailored to State, local, and tribal law enforce-
38 ment officers and intelligence analysts and designed to prepare for
39 and thwart acts of terrorism; and

40 (D) assist Department analysts in preparing products derived
41 from information within the scope of the information sharing envi-

1 ronment, including homeland security information, terrorism infor-
2 mation, and weapons of mass destruction information, that are
3 tailored to State, local, and tribal emergency response providers
4 and assist in the dissemination of the products through appro-
5 priate Department channels.

6 (b) ELIGIBILITY.—To be eligible for selection as an Information Sharing
7 Fellow under the program under the Homeland Security Information Shar-
8 ing Fellows Program, an individual shall—

- 9 (1) have homeland security-related responsibilities;
10 (2) be eligible for an appropriate security clearance;
11 (3) possess a valid need for access to classified information, as deter-
12 mined by the Under Secretary for Intelligence and Analysis;
13 (4) be an employee of—
14 (A) a State, local, or regional fusion center;
15 (B) a State or local law enforcement or other government entity
16 that serves a major metropolitan area, suburban area, or rural
17 area, as determined by the Secretary;
18 (C) a State or local law enforcement or other government entity
19 with port, border, or agricultural responsibilities, as determined by
20 the Secretary;
21 (D) a tribal law enforcement or other authority; or
22 (E) another entity the Secretary determines is appropriate; and
23 (5) have undergone appropriate privacy and civil liberties training
24 that is developed, supported, or sponsored by the Privacy Officer and
25 the Officer for Civil Rights and Civil Liberties, in consultation with the
26 Privacy and Civil Liberties Oversight Board established under section
27 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004
28 (42 U.S.C. 2000ee).

29 (c) OPTIONAL PARTICIPATION.—A State, local, or tribal law enforcement
30 or other government entity shall not be required to participate in the Home-
31 land Security Information Sharing Fellows Program.

32 (d) PROCEDURES FOR NOMINATION AND SELECTION.—

33 (1) IN GENERAL.—The Under Secretary for Intelligence and Anal-
34 ysis shall establish procedures to provide for the nomination and selec-
35 tion of individuals to participate in the Homeland Security Information
36 Sharing Fellows Program.

37 (2) LIMITATIONS.—The Under Secretary for Intelligence and Anal-
38 ysis shall—

- 39 (A) select law enforcement officers and intelligence analysts rep-
40 resenting a broad cross-section of State, local, and tribal agencies;
41 and

1 (B) ensure that the number of Information Sharing Fellows se-
2 lected does not impede the activities of the Office of Intelligence
3 and Analysis.

4 **§ 10514. Rural Policing Institute**

5 (a) DEFINITION OF RURAL.—In this section, the term “rural” means an
6 area—

7 (1) that is not located in a metropolitan statistical area, as defined
8 by the Office of Management and Budget; or

9 (2) that is located in a metropolitan statistical area and a county,
10 borough, parish, or area under the jurisdiction of an Indian tribe with
11 a population of not more than 50,000.

12 (b) IN GENERAL.—The Secretary shall establish a Rural Policing Insti-
13 tute, which shall be administered by the Federal Law Enforcement Training
14 Center, to target training to law enforcement agencies and other emergency
15 response providers located in rural areas. The Secretary, through the Rural
16 Policing Institute, shall—

17 (1) evaluate the needs of law enforcement agencies and other emer-
18 gency response providers in rural areas;

19 (2) develop expert training programs designed to address the needs
20 of law enforcement agencies and other emergency response providers in
21 rural areas as identified in the evaluation conducted under paragraph
22 (1), including training programs about intelligence-led policing and pro-
23 tections for privacy, civil rights, and civil liberties;

24 (3) provide the training programs developed under paragraph (2) to
25 law enforcement agencies and other emergency response providers in
26 rural areas; and

27 (4) conduct outreach efforts to ensure that local and tribal govern-
28 ments in rural areas are aware of the training programs developed
29 under paragraph (2) so they can avail themselves of the programs.

30 (c) CURRICULA.—The training at the Rural Policing Institute established
31 under subsection (a) shall—

32 (1) be configured in a manner so as not to duplicate or displace a
33 law enforcement or emergency response program of the Federal Law
34 Enforcement Training Center or a local or tribal government entity in
35 existence on August 3, 2007; and

36 (2) to the maximum extent practicable, be delivered in a cost-effec-
37 tive manner at facilities of the Department, on closed military installa-
38 tions with adequate training facilities, or at facilities operated by the
39 participants.

1 **§ 10515. Interagency Threat Assessment and Coordination**
2 **Group**

3 (a) IN GENERAL.—To improve the sharing of information within the
4 scope of the information sharing environment established under section
5 11708 of this title with State, local, tribal, and private-sector officials, the
6 Director of National Intelligence, through the program manager for the in-
7 formation sharing environment, in coordination with the Secretary, shall co-
8 ordinate and oversee the creation of an Interagency Threat Assessment and
9 Coordination Group (in this section referred to as “ITACG”).

10 (b) COMPOSITION OF ITACG.—The ITACG shall consist of—

11 (1) an ITACG Advisory Council to set policy and develop processes
12 for the integration, analysis, and dissemination of federally coordinated
13 information within the scope of the information sharing environment,
14 including homeland security information, terrorism information, and
15 weapons of mass destruction information; and

16 (2) an ITACG Detail comprised of State, local, and tribal homeland
17 security and law enforcement officers and intelligence analysts detailed
18 to work in the National Counterterrorism Center with Federal intel-
19 ligence analysts for the purpose of integrating, analyzing, and assisting
20 in the dissemination of federally coordinated information within the
21 scope of the information sharing environment, including homeland se-
22 curity information, terrorism information, and weapons of mass de-
23 struction information, through appropriate channels identified by the
24 ITACG Advisory Council.

25 (c) RESPONSIBILITIES OF PROGRAM MANAGER.—The program manager
26 shall—

27 (1) monitor and assess the efficacy of the ITACG;

28 (2) submit annually to the Secretary, the Attorney General, the Di-
29 rector of National Intelligence, the Committee on Homeland Security
30 and Governmental Affairs of the Senate, and the Committee on Home-
31 land Security of the House of Representatives a report on the progress
32 of the ITACG; and

33 (3) in each report required by paragraph (2), include an assessment
34 of whether the detailees under subsection (d)(5) have appropriate ac-
35 cess to all relevant information, as required by subsection (g)(2)(C).

36 (d) RESPONSIBILITIES OF SECRETARY.—The Secretary, or the Sec-
37 retary’s designee, in coordination with the Director of the National Counter-
38 terrorism Center and the ITACG Advisory Council, shall—

39 (1) create policies and standards for the creation of information
40 products derived from information within the scope of the information
41 sharing environment, including homeland security information, ter-

1 rorism information, and weapons of mass destruction information, that
2 are suitable for dissemination to State, local, and tribal governments
3 and the private sector;

4 (2) evaluate and develop processes for the timely dissemination of
5 federally coordinated information within the scope of the information
6 sharing environment, including homeland security information, ter-
7 rorism information, and weapons of mass destruction information, to
8 State, local, and tribal governments and the private sector;

9 (3) establish criteria and a methodology for indicating to State, local,
10 and tribal governments and the private sector the reliability of informa-
11 tion within the scope of the information sharing environment, including
12 homeland security information, terrorism information, and weapons of
13 mass destruction information, disseminated to them;

14 (4) educate the intelligence community about the requirements of the
15 State, local, and tribal homeland security, law enforcement, and other
16 emergency response providers regarding information within the scope
17 of the information sharing environment, including homeland security
18 information, terrorism information, and weapons of mass destruction
19 information;

20 (5) establish and maintain the ITACG Detail, which shall assign an
21 appropriate number of State, local, and tribal homeland security and
22 law enforcement officers and intelligence analysts to work in the Na-
23 tional Counterterrorism Center who shall—

24 (A) educate and advise National Counterterrorism Center intel-
25 ligence analysts about the requirements of the State, local, and
26 tribal homeland security and law enforcement officers, and other
27 emergency response providers regarding information within the
28 scope of the information sharing environment, including homeland
29 security information, terrorism information, and weapons of mass
30 destruction information;

31 (B) assist National Counterterrorism Center intelligence ana-
32 lysts in integrating, analyzing, and otherwise preparing versions of
33 products derived from information within the scope of the informa-
34 tion sharing environment, including homeland security informa-
35 tion, terrorism information, and weapons of mass destruction in-
36 formation that are unclassified or classified at the lowest possible
37 level and suitable for dissemination to State, local, and tribal
38 homeland security and law enforcement agencies in order to help
39 deter and prevent terrorist attacks;

40 (C) implement, in coordination with National Counterterrorism
41 Center intelligence analysts, the policies, processes, procedures,

1 standards, and guidelines developed by the ITACG Advisory Coun-
2 cil;

3 (D) assist in the dissemination of products derived from infor-
4 mation within the scope of the information sharing environment,
5 including homeland security information, terrorism information,
6 and weapons of mass destruction information, to State, local, and
7 tribal jurisdictions only through appropriate channels identified by
8 the ITACG Advisory Council;

9 (E) make recommendations, as appropriate, to the Secretary or
10 the Secretary's designee, for the further dissemination of intel-
11 ligence products that could likely inform or improve the security
12 of a State, local, or tribal government (including a State, local, or
13 tribal law enforcement agency), or a private-sector entity; and

14 (F) report directly to the senior intelligence official from the
15 Department under paragraph (6);

16 (6) detail a senior intelligence official from the Department to the
17 National Counterterrorism Center, who shall—

18 (A) manage the day-to-day operations of the ITACG Detail;

19 (B) report directly to the Director of the National Counterter-
20 rorism Center or the Director's designee; and

21 (C) in coordination with the Director of the Federal Bureau of
22 Investigation, and subject to the approval of the Director of the
23 National Counterterrorism Center, select a deputy from the pool
24 of available detailees from the Federal Bureau of Investigation in
25 the National Counterterrorism Center;

26 (7) establish, in the ITACG Advisory Council, a mechanism to select
27 law enforcement officers and intelligence analysts for placement in the
28 National Counterterrorism Center consistent with paragraph (5), using
29 criteria developed by the ITACG Advisory Council that shall encourage
30 participation from a broadly representative group of State, local, and
31 tribal homeland security and law enforcement agencies;

32 (8) compile an annual assessment of the ITACG Detail's perform-
33 ance, including summaries of customer feedback, in preparing, dissemi-
34 nating, and requesting the dissemination of intelligence products in-
35 tended for State, local and tribal government (including State, local,
36 and tribal law enforcement agencies), and private-sector entities; and

37 (9) provide the assessment developed under paragraph (8) to the
38 program manager for use in the annual reports required by subsection
39 (c)(2).

40 (e) MEMBERSHIP.—The Secretary, or the Secretary's designee, shall serve
41 as the chair of the ITACG Advisory Council, which shall include—

1 (1) representatives of—

2 (A) the Department;

3 (B) the Federal Bureau of Investigation;

4 (C) the National Counterterrorism Center;

5 (D) the Department of Defense;

6 (E) the Department of Energy;

7 (F) the Department of State; and

8 (G) other Federal entities as appropriate;

9 (2) the program manager of the information sharing environment,
10 designated under section 11708(d) of this title, or the program man-
11 ager's designee; and

12 (3) executive level law enforcement and intelligence officials from
13 State, local, and tribal governments.

14 (f) CRITERIA.—The Secretary, in consultation with the Director of Na-
15 tional Intelligence, the Attorney General, and the program manager of the
16 information sharing environment established under section 11708 of this
17 title, shall—

18 (1) establish procedures for selecting members of the ITACG Advi-
19 sory Council and for the proper handling and safeguarding of products
20 derived from information within the scope of the information sharing
21 environment, including homeland security information, terrorism infor-
22 mation, and weapons of mass destruction information, by those mem-
23 bers; and

24 (2) ensure that at least 50 percent of the members of the ITACG
25 Advisory Council are from State, local, and tribal governments.

26 (g) OPERATIONS.—

27 (1) IN GENERAL.—The ITACG Advisory Council shall meet regu-
28 larly, but not less than quarterly, at the facilities of the National
29 Counterterrorism Center of the Office of the Director of National Intel-
30 ligence.

31 (2) MANAGEMENT.—Pursuant to section 119(f)(1)(E) of the Na-
32 tional Security Act of 1947 (50 U.S.C. 3056(f)(1)(E)), the Director of
33 the National Counterterrorism Center, acting through the senior intel-
34 ligence official from the Department of Homeland Security detailed
35 pursuant to subsection (d)(6), shall ensure that—

36 (A) the products derived from information within the scope of
37 the information sharing environment, including homeland security
38 information, terrorism information, and weapons of mass destruc-
39 tion information, prepared by the National Counterterrorism Cen-
40 ter and the ITACG Detail for distribution to State, local, and trib-
41 al homeland security and law enforcement agencies, reflect the re-

1 quirements of the agencies and are produced consistently with the
2 policies, processes, procedures, standards, and guidelines estab-
3 lished by the ITACG Advisory Council;

4 (B) in consultation with the ITACG Advisory Council and con-
5 sistent with sections 102A(f)(1)(B)(iii) and 119(f)(1)(E) of the
6 National Security Act of 1947 (50 U.S.C. 3024(f)(1)(B)(iii),
7 3056(f)(1)(E)), all products described in subparagraph (A) are
8 disseminated through existing channels of the Department and the
9 Department of Justice and other appropriate channels to State,
10 local, and tribal government officials and other entities;

11 (C) all detailees under subsection (d)(5) have appropriate access
12 to all relevant information within the scope of the information
13 sharing environment, including homeland security information, ter-
14 rorism information, and weapons of mass destruction information,
15 available at the National Counterterrorism Center in order to ac-
16 complish the objectives under subsection (d)(5);

17 (D) all detailees under subsection (d)(5) have the appropriate
18 security clearances and are trained in the procedures for handling,
19 processing, storing, and disseminating classified products derived
20 from information within the scope of the information sharing envi-
21 ronment, including homeland security information, terrorism infor-
22 mation, and weapons of mass destruction information; and

23 (E) all detailees under subsection (d)(5) complete appropriate
24 privacy and civil liberties training.

25 (h) INAPPLICABILITY OF THE FEDERAL ADVISORY COMMITTEE ACT.—
26 The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the
27 ITACG or any subsidiary groups of the ITACG.

28 **§ 10516. National asset database**

29 (a) ESTABLISHMENT.—

30 (1) NATIONAL ASSET DATABASE.—The Secretary shall establish and
31 maintain a national database of each system or asset that—

32 (A) the Secretary, in consultation with appropriate homeland se-
33 curity officials of the States, determines to be vital and the loss,
34 interruption, incapacity, or destruction of which would have a neg-
35 ative or debilitating effect on the economic security, public health,
36 or safety of the United States, a State, or a local government; or

37 (B) the Secretary determines is appropriate for inclusion in the
38 database.

39 (2) PRIORITIZED CRITICAL INFRASTRUCTURE LIST.—In accordance
40 with Homeland Security Presidential Directive–7, as in effect on Janu-
41 ary 1, 2007, the Secretary shall establish and maintain a single classi-

1 fied prioritized list of systems and assets included in the database
2 under paragraph (1) that the Secretary determines would, if destroyed
3 or disrupted, cause national or regional catastrophic effects.

4 (b) USE OF DATABASE.—The Secretary shall use the database estab-
5 lished under subsection (a)(1) in the development and implementation of
6 Department plans and programs as appropriate.

7 (c) MAINTENANCE OF DATABASE.—

8 (1) IN GENERAL.—The Secretary shall maintain and annually up-
9 date the database established under subsection (a)(1) and the list es-
10 tablished under subsection (a)(2), including—

11 (A) establishing data collection guidelines and providing the
12 guidelines to the appropriate homeland security official of each
13 State;

14 (B) regularly reviewing the guidelines established under sub-
15 paragraph (A), including by consulting with the appropriate home-
16 land security officials of States, to solicit feedback about the
17 guidelines, as appropriate;

18 (C) after providing the homeland security official of a State
19 with the guidelines under subparagraph (A), allowing the official
20 a reasonable amount of time to submit to the Secretary data sub-
21 missions recommended by the official for inclusion in the database
22 established under subsection (a)(1);

23 (D) examining the contents and identifying submissions made
24 by the official that are described incorrectly or that do not meet
25 the guidelines established under subparagraph (A); and

26 (E) providing to the appropriate homeland security official of
27 each relevant State a list of submissions identified under subpara-
28 graph (D) for review and possible correction before the Secretary
29 finalizes the decision of which submissions will be included in the
30 database established under subsection (a)(1).

31 (2) ORGANIZATION OF INFORMATION IN DATABASE.—The Secretary
32 shall organize the contents of the database established under subsection
33 (a)(1) and the list established under subsection (a)(2) as the Secretary
34 determines is appropriate. Any organizational structure of the contents
35 shall include the categorization of the contents—

36 (A) according to the sectors listed in the National Infrastruc-
37 ture Protection Plan developed pursuant to Homeland Security
38 Presidential Directive–7; and

39 (B) by the State and county of their location.

40 (3) PRIVATE-SECTOR INTEGRATION.—The Secretary shall identify
41 and evaluate methods, including the Department’s Protected Critical

1 Infrastructure Information Program, to acquire relevant private-sector
2 information for the purpose of using that information to generate a
3 database or list, including the database established under subsection
4 (a)(1) and the list established under subsection (a)(2).

5 (4) RETENTION OF CLASSIFICATION.—The classification of informa-
6 tion required to be provided to Congress, the Department, or another
7 department or agency under this section by a sector-specific agency, in-
8 cluding the assignment of a level of classification of the information,
9 shall be binding on Congress, the Department, and that other Federal
10 agency.

11 (d) REPORTS.—

12 (1) ANNUAL REPORT REQUIRED.—The Secretary shall submit annu-
13 ally to the Committee on Homeland Security and Governmental Affairs
14 of the Senate and the Committee on Homeland Security of the House
15 of Representatives a report on the database established under sub-
16 section (a)(1) and the list established under subsection (a)(2).

17 (2) CONTENTS.—Each report shall include the following:

18 (A) The name, location, and sector classification of each of the
19 systems and assets on the list established under subsection (a)(2).

20 (B) The name, location, and sector classification of each of the
21 systems and assets on the list that are determined by the Sec-
22 retary to be most at risk to terrorism.

23 (C) Any significant challenges in compiling the list of the sys-
24 tems and assets included on the list or in the database established
25 under subsection (a)(1).

26 (D) Any significant changes from the preceding report in the
27 systems and assets included on the list or in the database.

28 (E) If appropriate, the extent to which the database and the list
29 have been used, individually or jointly, for allocating funds by the
30 Federal Government to prevent, reduce, mitigate, or respond to
31 acts of terrorism.

32 (F) The amount of coordination between the Department and
33 the private sector, through an entity of the Department that meets
34 with representatives of private-sector industries for purposes of co-
35 ordination, for the purpose of ensuring the accuracy of the data-
36 base and list.

37 (G) Other information the Secretary deems relevant.

38 (3) CLASSIFIED INFORMATION.—The report shall be submitted in
39 unclassified form but may contain a classified annex.

40 (e) NATIONAL INFRASTRUCTURE PROTECTION CONSORTIUM.—The Sec-
41 retary may establish the National Infrastructure Protection Consortium.

1 The National Infrastructure Protection Consortium may advise the Sec-
 2 retary on the best way to identify, generate, organize, and maintain a data-
 3 base or list of systems and assets established by the Secretary, including
 4 the database established under subsection (a)(1) and the list established
 5 under subsection (a)(2). If the Secretary establishes the National Infra-
 6 structure Protection Consortium, the Consortium may—

7 (1) be composed of national laboratories, Federal agencies, State and
 8 local homeland security organizations, academic institutions, or na-
 9 tional Centers of Excellence that have demonstrated experience working
 10 with and identifying critical infrastructure and key resources; and

11 (2) provide input to the Secretary on any request pertaining to the
 12 contents of the database or the list.

13 **§ 10517. Classified Information Advisory Officer**

14 (a) DESIGNATION.—The Secretary shall identify and designate in the De-
 15 partment a Classified Information Advisory Officer.

16 (b) RESPONSIBILITIES.—The responsibilities of the Classified Information
 17 Advisory Officer are as follows:

18 (1) To develop and disseminate educational materials and to develop
 19 and administer training programs to assist State, local, and tribal gov-
 20 ernments (including State, local, and tribal law enforcement agencies),
 21 and private-sector entities—

22 (A) in developing plans and policies to respond to requests re-
 23 lated to classified information without communicating the informa-
 24 tion to individuals who lack appropriate security clearances;

25 (B) regarding the appropriate procedures for challenging classi-
 26 fication designations of information received by personnel of the
 27 entities; and

28 (C) on the means by which personnel may apply for security
 29 clearances.

30 (2) To inform the Under Secretary for Intelligence and Analysis on
 31 policies and procedures that could facilitate the sharing of classified in-
 32 formation with the personnel, as appropriate.

33 **§ 10518. Annual report on intelligence activities of the De-**
 34 **partment**

35 (a) IN GENERAL.—For each fiscal year and along with the budget mate-
 36 rials submitted in support of the budget of the Department pursuant to sec-
 37 tion 1105(a) of title 31, the Under Secretary for Intelligence and Analysis
 38 shall submit to the congressional intelligence committees a report for that
 39 fiscal year on each intelligence activity of each intelligence component of the
 40 Department, as designated by the Under Secretary, that includes the fol-
 41 lowing:

1 (1) The amount of funding requested for each intelligence activity.

2 (2) The number of full-time employees funded to perform each intel-
3 ligence activity.

4 (3) The number of full-time contractor employees (or the equivalent
5 of full-time in the case of part-time contractor employees) funded to
6 perform, or in support of, each intelligence activity.

7 (4) A determination as to whether each intelligence activity is pre-
8 dominantly in support of national intelligence or departmental mission.

9 (5) The total number of analysts of the Intelligence Enterprise of the
10 Department who perform—

11 (A) strategic analysis; or

12 (B) operational analysis.

13 (b) FEASIBILITY AND ADVISABILITY REPORT.—Not later than 120 days
14 after December 19, 2014, the Secretary, acting through the Under Sec-
15 retary for Intelligence and Analysis, shall submit to the congressional intel-
16 ligence committees a report that—

17 (1) examines the feasibility and advisability of including the budget
18 request for all intelligence activities of each intelligence component of
19 the Department that predominantly support departmental missions, as
20 designed by the Under Secretary for Intelligence and Analysis, in the
21 Homeland Security Intelligence Program; and

22 (2) includes a plan to enhance the coordination of department-wide
23 intelligence activities to achieve greater efficiencies in the performance
24 of the intelligence functions of the Department.

25 **Subchapter II—Critical Infrastructure** 26 **Information**

27 **§ 10531. Definitions**

28 In this subchapter:

29 (1) AGENCY.—The term “agency” has the meaning given the term
30 in section 551 of title 5.

31 (2) COVERED FEDERAL AGENCY.—The term “covered Federal agen-
32 cy” means the Department.

33 (3) CRITICAL INFRASTRUCTURE INFORMATION.—The term “critical
34 infrastructure information” means information not customarily in the
35 public domain and related to the security of critical infrastructure or
36 protected systems, including—

37 (A) actual, potential, or threatened interference with, attack on,
38 compromise of, or incapacitation of critical infrastructure or pro-
39 tected systems by either physical or computer-based attack or
40 other similar conduct (including the misuse of or unauthorized ac-
41 cess to all types of communications and data transmission sys-

1 tems) that violates Federal, State, or local law, harms interstate
2 commerce of the United States, or threatens public health or safe-
3 ty;

4 (B) the ability of critical infrastructure or a protected system
5 to resist interference, compromise, or incapacitation, including any
6 planned or past assessment, projection, or estimate of the vulner-
7 ability of critical infrastructure or a protected system, including
8 security testing, risk evaluation, risk management planning, or
9 risk audit; and

10 (C) a planned or past operational problem or solution regarding
11 critical infrastructure or a protected system, including repair, re-
12 covery, reconstruction, insurance, or continuity, to the extent it is
13 related to interference, compromise, or incapacitation.

14 (4) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.—The term
15 “critical infrastructure protection program” means a component or bu-
16 reau of a covered Federal agency that has been designated by the
17 President or an agency head to receive critical infrastructure informa-
18 tion.

19 (5) CYBERSECURITY RISK; INCIDENT.—The terms “cybersecurity
20 risk” and “incident” have the meanings given the terms in section
21 10545 of this title.

22 (6) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The
23 term “information sharing and analysis organization” means a formal
24 or informal entity or collaboration created or employed by public- or
25 private-sector organizations, for purposes of—

26 (A) gathering and analyzing critical infrastructure information,
27 including information relating to cybersecurity risks and incidents,
28 to better understand security problems and interdependencies re-
29 lating to critical infrastructure, including cybersecurity risks and
30 incidents, and protected systems, so as to ensure the availability,
31 integrity, and reliability of the infrastructure and systems;

32 (B) communicating or disclosing critical infrastructure informa-
33 tion, including cybersecurity risks and incidents, to help prevent,
34 detect, mitigate, or recover from the effects of an interference,
35 compromise, or incapacitation problem relating to critical infra-
36 structure, including cybersecurity risks and incidents, or protected
37 systems; and

38 (C) voluntarily disseminating critical infrastructure information,
39 including cybersecurity risks and incidents, to its members, the
40 Federal Government, State and local governments, or other enti-

1 ties that may be of assistance in carrying out the purposes speci-
2 fied in subparagraphs (A) and (B).

3 (7) PROTECTED SYSTEM.—The term “protected system”—

4 (A) means a service, physical or computer-based system, proc-
5 ess, or procedure that directly or indirectly affects the viability of
6 a facility of critical infrastructure; and

7 (B) includes a physical or computer-based system, including a
8 computer, computer system, computer or communications network,
9 or any component hardware or element thereof, software program,
10 processing instructions, or information or data in transmission or
11 storage therein, irrespective of the medium of transmission or
12 storage.

13 (8) VOLUNTARY.—

14 (A) IN GENERAL.—The term “voluntary”, in the case of a sub-
15 mittal of critical infrastructure information to a covered Federal
16 agency, means the submittal of the information in the absence of
17 the agency’s exercise of legal authority to compel access to, or sub-
18 mission of, the information and may be accomplished by a single
19 entity or an information sharing and analysis organization on be-
20 half of itself or its members.

21 (B) EXCLUSIONS.—The term “voluntary”—

22 (i) in the case of an action brought under the securities
23 laws as is defined in section 3(a) of the Securities Exchange
24 Act of 1934 (15 U.S.C. 78c(a))—

25 (I) does not include information or statements con-
26 tained in documents or materials filed with the Securities
27 and Exchange Commission, or with Federal banking reg-
28 ulators, under section 12(i) of the Securities Exchange
29 Act of 1934 (15 U.S.C. 78l(i)); and

30 (II) with respect to the submittal of critical infrastruc-
31 ture information, does not include a disclosure or writing
32 that when made accompanied the solicitation of an offer
33 or a sale of securities; and

34 (ii) does not include information or statements submitted
35 or relied upon as a basis for making licensing or permitting
36 determinations, or during regulatory proceedings.

37 **§ 10532. Designation of critical infrastructure protection**
38 **program**

39 A critical infrastructure protection program may be designated as such
40 by one of the following:

41 (1) The President.

1 (2) The Secretary.

2 **§ 10533. Protection of voluntarily shared critical infrastruc-**
 3 **ture information**

4 (a) PROTECTION.—

5 (1) IN GENERAL.—Critical infrastructure information (including the
 6 identity of the submitting person or entity) that is voluntarily sub-
 7 mitted to a covered Federal agency for use by that agency regarding
 8 the security of critical infrastructure and protected systems, analysis,
 9 warning, interdependency study, recovery, reconstitution, or other in-
 10 formational purpose, when accompanied by an express statement speci-
 11 fied in paragraph (2)—

12 (A) shall be exempt from disclosure under section 552 of title
 13 5 (known as the Freedom of Information Act);

14 (B) shall not be subject to agency rules or judicial doctrine re-
 15 garding ex parte communications with a decision-making official;

16 (C) shall not, without the written consent of the person or enti-
 17 ty submitting the information, be used directly by the agency, an-
 18 other Federal, State, or local authority, or a third party, in a civil
 19 action arising under Federal or State law if the information is
 20 submitted in good faith;

21 (D) shall not, without the written consent of the person or enti-
 22 ty submitting the information, be used or disclosed by an officer
 23 or employee of the United States for purposes other than the pur-
 24 poses of this subchapter, except—

25 (i) in furtherance of an investigation or the prosecution of
 26 a criminal act; or

27 (ii) when disclosure of the information would be—

28 (I) to either House of Congress, or to the extent of
 29 matter within its jurisdiction, a committee or sub-
 30 committee of Congress (including a joint committee or
 31 subcommittee); or

32 (II) to the Comptroller General, or an authorized rep-
 33 resentative of the Comptroller General, in the course of
 34 the performance of the duties of the Government Ac-
 35 countability Office;

36 (E) shall not, if provided to a State or local government or gov-
 37 ernment agency—

38 (i) be made available pursuant to State or local law requir-
 39 ing disclosure of information or records;

40 (ii) otherwise be disclosed or distributed to a party by the
 41 State or local government or government agency without the

1 written consent of the person or entity submitting the infor-
2 mation; or

3 (iii) be used other than for the purpose of protecting crit-
4 ical infrastructure or protected systems, or in furtherance of
5 an investigation or the prosecution of a criminal act; and

6 (F) does not constitute a waiver of an applicable privilege or
7 protection provided under law, such as trade secret protection.

8 (2) EXPRESS STATEMENT.—For purposes of paragraph (1), the term
9 “express statement”, with respect to information or records, means—

10 (A) in the case of written information or records, a written
11 marking on the information or records substantially similar to the
12 following: “This information is voluntarily submitted to the Fed-
13 eral Government in expectation of protection from disclosure as
14 provided by the provisions of the Critical Infrastructure Informa-
15 tion Act of 2002.”; or

16 (B) in the case of oral information, a similar written statement
17 submitted within a reasonable period following the oral commu-
18 nication.

19 (b) LIMITATION.—A communication of critical infrastructure information
20 to a covered Federal agency made pursuant to this subchapter shall not be
21 considered to be an action subject to the requirements of the Federal Advi-
22 sory Committee Act (5 U.S.C. App.).

23 (c) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section
24 shall be construed to limit or otherwise affect the ability of a State, local,
25 or Federal Government entity, agency, or authority, or a third party, under
26 applicable law, to obtain critical infrastructure information in a manner not
27 covered by subsection (a), including information lawfully and properly dis-
28 closed generally or broadly to the public and to use the information in any
29 manner permitted by law. For purposes of this section, a permissible use
30 of independently obtained information includes the disclosure of the infor-
31 mation under section 2302(b)(8) of title 5.

32 (d) TREATMENT OF VOLUNTARY SUBMITTAL OF INFORMATION.—The
33 voluntary submittal to the Government of information or records that are
34 protected from disclosure by this subchapter shall not be construed to con-
35 stitute compliance with a requirement to submit the information to a Fed-
36 eral agency under any other provision of law.

37 (e) PROCEDURES.—

38 (1) IN GENERAL.—The Secretary shall, in consultation with appro-
39 priate representatives of the National Security Council and the Office
40 of Science and Technology Policy, establish uniform procedures for the

1 receipt, care, and storage by Federal agencies of critical infrastructure
2 information that is voluntarily submitted to the Government.

3 (2) ELEMENTS.—The procedures established under paragraph (1)
4 shall include mechanisms regarding—

5 (A) the acknowledgement of receipt by Federal agencies of crit-
6 ical infrastructure information that is voluntarily submitted to the
7 Government;

8 (B) the maintenance of the identification of the information as
9 voluntarily submitted to the Government for purposes of, and sub-
10 ject to, the provisions of this subchapter;

11 (C) the care and storage of the information; and

12 (D) the protection and maintenance of the confidentiality of the
13 information so as to permit the sharing of the information within
14 the Federal Government and with State and local governments,
15 and the issuance of notices and warnings related to the protection
16 of critical infrastructure and protected systems, in a manner to
17 protect from public disclosure the identity of the submitting per-
18 son or entity, or information that is proprietary, business sensitive,
19 relates specifically to the submitting person or entity, and is other-
20 wise not appropriately in the public domain.

21 (f) PENALTIES.—Whoever, being an officer or employee of the United
22 States or of any department or agency thereof, knowingly publishes, di-
23 vulges, discloses, or makes known in any manner or to any extent not au-
24 thorized by law, any critical infrastructure information protected from dis-
25 closure by this subchapter coming to him or her in the course of this em-
26 ployment or official duties or by reason of any examination or investigation
27 made by, or return, report, or record made to or filed with, the department
28 or agency or officer or employee thereof, shall be fined under title 18, im-
29 prisoned not more than 1 year, or both, and shall be removed from office
30 or employment.

31 (g) AUTHORITY TO ISSUE WARNINGS.—The Federal Government may
32 provide advisories, alerts, and warnings to relevant companies, targeted sec-
33 tors, other governmental entities, or the general public regarding potential
34 threats to critical infrastructure as appropriate. In issuing a warning, the
35 Federal Government shall take appropriate actions to protect from disclo-
36 sure—

37 (1) the source of voluntarily submitted critical infrastructure infor-
38 mation that forms the basis for the warning; or

39 (2) information that is proprietary, business sensitive, relates specifi-
40 cally to the submitting person or entity, or is otherwise not appro-
41 priately in the public domain.

1 (h) AUTHORITY TO DELEGATE.—The President may delegate authority
 2 to a critical infrastructure protection program, designated under section
 3 10532 of this title, to enter into a voluntary agreement to promote critical
 4 infrastructure security, including with an information sharing and analysis
 5 organization, or a plan of action as otherwise defined in section 708 of the
 6 Defense Production Act of 1950 (50 U.S.C. 4558).

7 **§ 10534. No private right of action**

8 Nothing in this subchapter may be construed to create a private right of
 9 action for enforcement of a provision of this subtitle.

10 **Subchapter III—Information Security**
 11 **Part A—Department Duties and Powers**

12 **§ 10541. Procedures for sharing information**

13 The Secretary shall establish procedures on the use of information shared
 14 under this chapter that—

- 15 (1) limit the re-dissemination of the information to ensure that it is
 16 not used for an unauthorized purpose;
- 17 (2) ensure the security and confidentiality of the information;
- 18 (3) protect the constitutional and statutory rights of individuals who
 19 are subjects of the information; and
- 20 (4) provide data integrity through the timely removal and destruc-
 21 tion of obsolete or erroneous names and information.

22 **§ 10542. Cybersecurity collaboration between the Depart-**
 23 **ment and the Department of Defense**

24 (a) INTERDEPARTMENTAL COLLABORATION.—

25 (1) IN GENERAL.—The Secretary and the Secretary of Defense shall
 26 provide personnel, equipment, and facilities to increase interdepart-
 27 mental collaboration with respect to—

- 28 (A) strategic planning for the cybersecurity of the United
 29 States;
- 30 (B) mutual support for cybersecurity capabilities development;
 31 and
- 32 (C) synchronization of current operational cybersecurity mission
 33 activities.

34 (2) EFFICIENCIES.—The collaboration provided for under paragraph
 35 (1) shall be designed—

- 36 (A) to improve the efficiency and effectiveness of requirements
 37 formulation and requests for products, services, and technical as-
 38 sistance for, and coordination and performance assessment of, cy-
 39 bersecurity missions executed across a variety of elements of the
 40 Department and the Department of Defense; and

1 (B) to leverage the expertise of the Department and the Depart-
 2 ment of Defense and to avoid duplicating, replicating, or aggreg-
 3 ating unnecessarily the diverse line organizations across tech-
 4 nology developments, operations, and customer support that collec-
 5 tively execute the cybersecurity mission of the Department and the
 6 Department of Defense.

7 (b) RESPONSIBILITIES.—

8 (1) SECRETARY.—The Secretary shall identify and assign, in coordi-
 9 nation with the Secretary of Defense, a Director of Cybersecurity Co-
 10 ordination in the Department to undertake collaborative activities with
 11 the Department of Defense.

12 (2) SECRETARY OF DEFENSE.—The Secretary of Defense shall iden-
 13 tify and assign, in coordination with the Secretary, one or more offi-
 14 cials in the Department of Defense to coordinate, oversee, and execute
 15 collaborative activities and the provision of cybersecurity support to the
 16 Department.

17 **§ 10543. Privacy officer**

18 (a) APPOINTMENT AND RESPONSIBILITIES.—The Secretary shall appoint
 19 a senior official in the Department, who shall report directly to the Sec-
 20 retary, to assume primary responsibility for privacy policy, including—

21 (1) assuring that the use of technologies sustain, and do not erode,
 22 privacy protections relating to the use, collection, and disclosure of per-
 23 sonal information;

24 (2) assuring that personal information contained in Privacy Act sys-
 25 tems of records is handled in full compliance with fair information
 26 practices as set out in section 552a of title 5 (known as the “Privacy
 27 Act of 1974”);

28 (3) evaluating legislative and regulatory proposals involving collec-
 29 tion, use, and disclosure of personal information by the Federal Gov-
 30 ernment;

31 (4) conducting a privacy impact assessment of proposed rules of the
 32 Department or that of the Department on the privacy of personal in-
 33 formation, including the type of personal information collected and the
 34 number of people affected;

35 (5) coordinating with the Officer for Civil Rights and Civil Liberties
 36 to ensure that—

37 (A) programs, policies, and procedures involving civil rights,
 38 civil liberties, and privacy considerations are addressed in an inte-
 39 grated and comprehensive manner; and

40 (B) Congress receives appropriate reports on the programs, poli-
 41 cies, and procedures; and

1 (6) preparing a report to Congress on an annual basis on activities
 2 of the Department that affect privacy, including complaints of privacy
 3 violations, implementation of section 552a of title 5 (known as the
 4 “Privacy Act of 1974”), internal controls, and other matters.

5 (b) AUTHORITY TO INVESTIGATE.—

6 (1) IN GENERAL.—The senior official appointed under subsection (a)
 7 may—

8 (A) have access to all records, reports, audits, reviews, docu-
 9 ments, papers, recommendations, and other materials available to
 10 the Department that relate to programs and operations with re-
 11 spect to the responsibilities of the senior official under this section;

12 (B) make investigations and reports relating to the administra-
 13 tion of the programs and operations of the Department that are,
 14 in the senior official’s judgment, necessary or desirable;

15 (C) subject to the approval of the Secretary, require by sub-
 16 poena the production, by any person other than a Federal agency,
 17 of all information, documents, reports, answers, records, accounts,
 18 papers, and other data and documentary evidence necessary to the
 19 performance of the responsibilities of the senior official under this
 20 section; and

21 (D) administer to, or take from, a person an oath, affirmation,
 22 or affidavit, whenever necessary to the performance of the respon-
 23 sibilities of the senior official under this section.

24 (2) ENFORCEMENT OF SUBPOENAS.—A subpoena issued under para-
 25 graph (1)(C) shall, in the case of contumacy or refusal to obey, be en-
 26 forceable by order of an appropriate United States district court.

27 (3) EFFECT OF OATHS.—An oath, affirmation, or affidavit adminis-
 28 tered or taken under paragraph (1)(D) by or before an employee of the
 29 Privacy Office designated for that purpose by the senior official ap-
 30 pointed under subsection (a) shall have the same force and effect as
 31 if administered or taken by or before an officer having a seal of office.

32 (c) SUPERVISION AND COORDINATION.—

33 (1) IN GENERAL.—The senior official appointed under subsection (a)
 34 shall—

35 (A) report to, and be under the general supervision of, the Sec-
 36 retary; and

37 (B) coordinate activities with the Inspector General of the De-
 38 partment in order to avoid duplication of effort.

39 (2) COORDINATION WITH INSPECTOR GENERAL.—

40 (A) IN GENERAL.—Except as provided in subparagraph (B), the
 41 senior official appointed under subsection (a) may investigate a

1 matter relating to possible violations or abuse concerning the ad-
2 ministration of a program or operation of the Department relevant
3 to the purposes under this section.

4 (B) COORDINATION.—

5 (i) REFERRAL TO INSPECTOR GENERAL.—Before initiating
6 an investigation described under subparagraph (A), the senior
7 official shall refer the matter and all related complaints, alle-
8 gations, and information to the Inspector General of the De-
9 partment.

10 (ii) DETERMINATION.—Not later than 30 days after the re-
11 ceipt of a matter referred under clause (i), the Inspector Gen-
12 eral shall—

13 (I) make a determination regarding whether the In-
14 spector General intends to initiate an audit or investiga-
15 tion of the matter referred under clause (i); and

16 (II) notify the senior official of that determination.

17 (iii) NOTIFICATION THAT AUDIT NOT INITIATED.—If the
18 Inspector General notifies the senior official that the Inspec-
19 tor General intends to initiate an audit or investigation, but
20 does not initiate that audit or investigation within 90 days
21 after providing that notification, the Inspector General shall
22 further notify the senior official that an audit or investigation
23 was not initiated. The further notification under this clause
24 shall be made not later than 3 days after the end of that 90-
25 day period.

26 (iv) INVESTIGATION BY SENIOR OFFICIAL.—The senior offi-
27 cial may investigate a matter referred under clause (i) if—

28 (I) the Inspector General notifies the senior official
29 under clause (ii) that the Inspector General does not in-
30 tend to initiate an audit or investigation relating to that
31 matter; or

32 (II) the Inspector General provides a further notifica-
33 tion under clause (iii) relating to that matter.

34 (v) TRAINING.—An employee of the Office of Inspector
35 General who audits or investigates a matter referred under
36 clause (i) shall be required to receive adequate training on
37 privacy laws, rules, and regulations, to be provided by an en-
38 tity approved by the Inspector General in consultation with
39 the senior official appointed under subsection (a).

40 (d) NOTIFICATION TO CONGRESS ON REMOVAL.—If the Secretary re-
41 moves the senior official appointed under subsection (a) or transfers that

1 senior official to another position or location within the Department, the
2 Secretary shall—

3 (1) promptly submit a written notification of the removal or transfer
4 to both Houses of Congress; and

5 (2) include in a notification the reasons for the removal or transfer.

6 (e) REPORTS BY SENIOR OFFICIAL TO CONGRESS.—The senior official
7 appointed under subsection (a) shall—

8 (1) submit reports directly to Congress regarding performance of the
9 responsibilities of the senior official under this section, without prior
10 comment or amendment by the Secretary, Deputy Secretary of Home-
11 land Security, or any other officer or employee of the Department or
12 the Office of Management and Budget; and

13 (2) inform the Committee on Homeland Security and Governmental
14 Affairs of the Senate and the Committee on Homeland Security of the
15 House of Representatives not later than—

16 (A) 30 days after the Secretary disapproves the senior official's
17 request for a subpoena under subsection (b)(1)(C) or the Sec-
18 retary substantively modifies the requested subpoena; or

19 (B) 45 days after the senior official's request for a subpoena
20 under subsection (b)(1)(C), if that subpoena has not either been
21 approved or disapproved by the Secretary.

22 **§ 10544. Enhancement of Federal and non-Federal cyberse-**
23 **curity**

24 In carrying out the responsibilities under section 10501 of this title, the
25 Under Secretary appointed under section 10302(b)(1)(H) of this title
26 shall—

27 (1) as appropriate, provide to State and local government entities,
28 and upon request to private entities that own or operate critical infor-
29 mation 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, upon 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.

1 **§ 10545. National Cybersecurity and Communications Inte-**
 2 **gration Center**

3 (a) DEFINITIONS.—In this section—

4 (1) CYBERSECURITY RISK.—The term “cybersecurity risk”—

5 (A) means threats to and vulnerabilities of information or infor-
 6 mation systems and any related consequences caused by or result-
 7 ing from unauthorized access, use, disclosure, degradation, disrup-
 8 tion, modification, or destruction of the information or information
 9 systems, including related consequences caused by an act of ter-
 10 rorism; and

11 (B) does not include an action that solely involves a violation
 12 of a consumer term of service or a consumer licensing agreement.

13 (2) CYBER THREAT INDICATOR; DEFENSIVE MEASURE.—The terms
 14 “cyber threat indicator” and “defensive measure” have the meanings
 15 given the terms in section 10561 of this title.

16 (3) INCIDENT.—The term “incident” means an occurrence that actu-
 17 ally or imminently jeopardizes, without lawful authority —

18 (A) the integrity, confidentiality, or availability of information
 19 on an information system; or

20 (B) an information system.

21 (4) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The
 22 term “information sharing and analysis organization” has the meaning
 23 given that term in section 10531 of this title.

24 (5) INFORMATION SYSTEM.—The term “information system” has the
 25 meaning given that term in section 3502(8) of title 44.

26 (6) SHARING.—The term “sharing” means providing, receiving, and
 27 disseminating.

28 (b) NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION
 29 CENTER.—There is in the Department the National Cybersecurity and
 30 Communications Integration Center (referred to in this section as the “Cen-
 31 ter”) to carry out certain responsibilities of the Under Secretary appointed
 32 under section 10302(b)(1)(H) of this title.

33 (c) FUNCTIONS.—The cybersecurity functions of the Center shall in-
 34 clude—

35 (1) being a Federal civilian interface for the multi-directional and
 36 cross-sector sharing of information relating to cyber threat indicators,
 37 defensive measures, cybersecurity risks, incidents, analysis, and warn-
 38 ings for Federal and non-Federal entities, including the implementation
 39 of part B of this subchapter;

40 (2) providing shared situational awareness to enable real-time, inte-
 41 grated, and operational actions across the Federal Government and

1 non-Federal entities to address cybersecurity risks and incidents to
2 Federal and non-Federal entities;

3 (3) coordinating the sharing of information relating to cyber threat
4 indicators, defensive measures, cybersecurity risks, and incidents across
5 the Federal Government;

6 (4) facilitating cross-sector coordination to address cybersecurity
7 risks and incidents, including cybersecurity risks and incidents that
8 may be related or could have consequential impacts across multiple sec-
9 tors;

10 (5)(A) conducting integration and analysis, including cross-sector in-
11 tegration and analysis, of cyber threat indicators, defensive measures,
12 cybersecurity risks, and incidents; and

13 (B) sharing the analysis conducted under subparagraph (A) with
14 Federal and non-Federal entities;

15 (6) on request, providing timely technical assistance, risk manage-
16 ment support, and incident response capabilities to Federal and non-
17 Federal entities with respect to cyber threat indicators, defensive meas-
18 ures, cybersecurity risks, and incidents, which may include attribution,
19 mitigation, and remediation;

20 (7) providing information and recommendations on security and re-
21 siliance measures to Federal and non-Federal entities, including infor-
22 mation and recommendations to—

23 (A) facilitate information security;

24 (B) strengthen information systems against cybersecurity risks
25 and incidents; and

26 (C) share cyber threat indicators and defensive measures;

27 (8) engaging with international partners, in consultation with other
28 appropriate agencies, to—

29 (A) collaborate on cyber threat indicators, defensive measures,
30 and information relating to cybersecurity risks and incidents; and

31 (B) enhance the security and resilience of global cybersecurity;

32 (9) sharing cyber threat indicators, defensive measures, and other in-
33 formation relating to cybersecurity risks and incidents with Federal
34 and non-Federal entities, including across sectors of critical infrastruc-
35 ture, and with State and major urban area fusion centers, as appro-
36 priate;

37 (10) participating, as appropriate, in national exercises run by the
38 Department; and

39 (11) in coordination with the Office of Emergency Communications
40 of the Department, assessing and evaluating consequence, vulnerability,
41 and threat information regarding cyber incidents to public safety com-

1 munications to help facilitate continuous improvements to the security
2 and resiliency of the communications.

3 (d) COMPOSITION.—

4 (1) IN GENERAL.—The Center is composed of—

5 (A) appropriate representatives of Federal entities, such as—

6 (i) sector-specific agencies;

7 (ii) civilian and law enforcement agencies; and

8 (iii) elements of the intelligence community, as that term
9 is defined under section 3 of the National Security Act of
10 1947 (50 U.S.C. 3003);

11 (B) appropriate representatives of non-Federal entities, such
12 as—

13 (i) State and local governments;

14 (ii) information sharing and analysis organizations; and

15 (iii) owners and operators of critical information systems;

16 (C) components in the Center that carry out cybersecurity and
17 communications activities;

18 (D) a designated Federal official for operational coordination
19 with and across each sector; and

20 (E) other appropriate representatives or entities, as determined
21 by the Secretary.

22 (2) INCIDENTS.—In the event of an incident, during exigent cir-
23 cumstances the Secretary may grant a Federal or non-Federal entity
24 immediate temporary access to the Center.

25 (e) PRINCIPLES.—In carrying out the functions under subsection (c), the
26 Center shall ensure—

27 (1) to the extent practicable, that—

28 (A) timely, actionable, and relevant information related to cy-
29 bersecurity risks, incidents, and analysis is shared;

30 (B) when appropriate, information related to cybersecurity
31 risks, incidents, and analysis is integrated with other relevant in-
32 formation and tailored to the specific characteristics of a sector;

33 (C) activities are prioritized and conducted based on the level
34 of risk;

35 (D) industry sector-specific, academic, and national laboratory
36 expertise is sought and receives appropriate consideration;

37 (E) continuous, collaborative, and inclusive coordination oc-
38 curs—

39 (i) across sectors; and

40 (ii) with—

41 (I) sector coordinating councils;

1 (II) information sharing and analysis organizations;
2 and

3 (III) other appropriate non-Federal partners;

4 (F) as appropriate, the Center works to develop and use mecha-
5 nisms for sharing information related to cybersecurity risks and
6 incidents that are technology-neutral, interoperable, real-time,
7 cost-effective, and resilient; and

8 (G) the Center works with other agencies to reduce unneces-
9 sarily duplicative sharing of information related to cybersecurity
10 risks and incidents;

11 (2) that information related to cybersecurity risks and incidents is
12 appropriately safeguarded against unauthorized access; and

13 (3) that activities conducted by the Center comply with all policies,
14 regulations, and laws that protect the privacy and civil liberties of
15 United States persons.

16 (f) NO RIGHT OR BENEFIT.—

17 (1) IN GENERAL.—The provision of assistance or information to, and
18 inclusion in the Center of, governmental or private entities under this
19 section shall be at the sole and unreviewable discretion of the Under
20 Secretary appointed under section 10302(b)(1)(H) of this title.

21 (2) CERTAIN ASSISTANCE OR INFORMATION.—The provision of cer-
22 tain assistance or information to, or inclusion in the Center of, one gov-
23 ernmental or private entity pursuant to this section shall not create a
24 right or benefit, substantive or procedural, to similar assistance or in-
25 formation for any other governmental or private entity.

26 (g) AUTOMATED INFORMATION SHARING.—

27 (1) IN GENERAL.—The Under Secretary appointed under section
28 10302(b)(1)(H) of this title, in coordination with industry and other
29 stakeholders, shall develop capabilities making use of existing informa-
30 tion technology industry standards and best practices, as appropriate,
31 that support and rapidly advance the development, adoption, and im-
32 plementation of automated mechanisms for the sharing of cyber threat
33 indicators and defensive measures in accordance with part B of this
34 subchapter.

35 (2) ANNUAL REPORT.—The Under Secretary appointed under sec-
36 tion 10302(b)(1)(H) of this title shall submit to the Committee on
37 Homeland Security and Governmental Affairs of the Senate and the
38 Committee on Homeland Security of the House of Representatives an
39 annual report on the status and progress of the development of the ca-
40 pabilities described in paragraph (1). The reports shall be required
41 until the capabilities are fully implemented.

1 (h) VOLUNTARY INFORMATION SHARING PROCEDURES AND RELATION-
2 SHIPS.—

3 (1) PROCEDURES.—

4 (A) IN GENERAL.—The Center may enter into a voluntary in-
5 formation sharing relationship with any consenting non-Federal
6 entity for the sharing of cyber threat indicators and defensive
7 measures for cybersecurity purposes in accordance with this sec-
8 tion. Nothing in this subsection may be construed to require any
9 non-Federal entity to enter into an information sharing relation-
10 ship with the Center or any other entity. The Center may termi-
11 nate a voluntary information sharing relationship under this sub-
12 section, at the sole and unreviewable discretion of the Secretary,
13 acting through the Under Secretary appointed under section
14 10302(b)(1)(H) of this title, for any reason, including if the Cen-
15 ter determines that the non-Federal entity with which the Center
16 has entered into the relationship has violated the terms of this
17 subsection.

18 (B) NATIONAL SECURITY.—The Secretary may decline to enter
19 into a voluntary information sharing relationship under this sub-
20 section, at the sole and unreviewable discretion of the Secretary,
21 acting through the Under Secretary appointed under section
22 10302(b)(1)(H) of this title, for any reason, including if the Sec-
23 retary determines that declining to enter into the relationship is
24 appropriate for national security.

25 (2) RELATIONSHIPS.—A voluntary information sharing relationship
26 under this subsection may be characterized as an agreement described
27 as follows:

28 (A) For the use of a non-Federal entity, the Center shall make
29 available a standard agreement, consistent with this section, on
30 the Department's website.

31 (B) At the request of a non-Federal entity, and if determined
32 appropriate by the Center, at the sole and unreviewable discretion
33 of the Secretary, acting through the Under Secretary appointed
34 under section 10302(b)(1)(H) of this title, the Department shall
35 negotiate a non-standard agreement, consistent with this section.

36 (C) An agreement between the Center and a non-Federal entity
37 that was entered into, or that was in effect, before December 18,
38 2015, shall be deemed in compliance with the requirements of this
39 subsection. An agreement under this subsection shall include the
40 relevant privacy protections as in effect under the Cooperative Re-
41 search and Development Agreement for Cybersecurity Information

1 Sharing and Collaboration, as of December 31, 2014. Nothing in
2 this subsection may be construed to require a non-Federal entity
3 to enter into either a standard or negotiated agreement to be in
4 compliance with this subsection.

5 (i) **DIRECT REPORTING.**—The Secretary shall develop policies and proce-
6 dures for direct reporting to the Secretary by the Director of the Center
7 regarding significant cybersecurity risks and incidents.

8 (j) **REPORTS ON INTERNATIONAL COOPERATION.**—The Secretary periodi-
9 cally shall submit to the Committee on Homeland Security and Govern-
10 mental Affairs of the Senate and the Committee on Homeland Security of
11 the House of Representatives a report on the range of efforts underway to
12 bolster cybersecurity collaboration with relevant international partners in ac-
13 cordance with subsection (e)(8).

14 (k) **OUTREACH.**—The Secretary, acting through the Under Secretary ap-
15 pointed under section 10302(b)(1)(H) of this title, shall—

16 (1) disseminate to the public information about how to voluntarily
17 share cyber threat indicators and defensive measures with the Center;
18 and

19 (2) enhance outreach to critical infrastructure owners and operators
20 for purposes of sharing cyber threat indicators and defensive measures
21 with the Center.

22 (l) **CYBERSECURITY OUTREACH.**—

23 (1) **DEFINITIONS.**—For purposes of this subsection, the terms
24 “small business concern” and “small business development center”
25 have the meanings given the terms in section 3 of the Small Business
26 Act (15 U.S.C. 632).

27 (2) **PROVIDE ASSISTANCE.**—The Secretary may leverage small busi-
28 ness development centers to provide assistance to small business con-
29 cerns by disseminating information on cyber threat indicators, defense
30 measures, cybersecurity risks, incidents, analyses, and warnings to help
31 small business concerns in developing or enhancing cybersecurity infra-
32 structure, awareness of cyber threat indicators, and cyber training pro-
33 grams for employees.

34 (m) **COORDINATED VULNERABILITY DISCLOSURE.**—The Secretary, in co-
35 ordination with industry and other stakeholders, may develop and adhere to
36 Department policies and procedures for coordinating vulnerability disclo-
37 sures.

38 **§ 10546. Cybersecurity plans**

39 (a) **DEFINITIONS.**—In this section:

1 (1) AGENCY INFORMATION SYSTEM.—The term “agency information
2 system” means an information system used or operated by an agency
3 or by another entity on behalf of an agency.

4 (2) CYBERSECURITY RISK; INFORMATION SYSTEM.—The terms “cy-
5 bersecurity risk” and “information system” have the meanings given
6 the terms in section 10545 of this title.

7 (3) INTELLIGENCE COMMUNITY.—The term “intelligence commu-
8 nity” has the meaning given the term in section 3 of the National Se-
9 curity Act of 1947 (50 U.S.C. 3003).

10 (4) NATIONAL SECURITY SYSTEM.—The term “national security sys-
11 tem” has the meaning given the term in section 11103 of title 40.

12 (b) INTRUSION ASSESSMENT PLAN.—

13 (1) REQUIREMENT.—The Secretary, in coordination with the Direc-
14 tor of the Office of Management and Budget, shall—

15 (A) develop and implement an intrusion assessment plan to
16 proactively detect, identify, and remove intruders in agency infor-
17 mation systems on a routine basis; and

18 (B) update the plan as necessary.

19 (2) EXCEPTION.—The intrusion assessment plan required under
20 paragraph (1) shall not apply to the Department of Defense, a national
21 security system, or an element of the intelligence community.

22 (c) CYBER INCIDENT RESPONSE PLANS.—The Under Secretary ap-
23 pointed under section 10302(b)(1)(H) of this title shall, in coordination with
24 appropriate Federal departments and agencies, State and local governments,
25 sector coordinating councils, information sharing and analysis organizations
26 (as defined in section 10531 of this title), owners and operators of critical
27 infrastructure, and other appropriate entities and individuals, develop, regu-
28 larly update, maintain, and exercise adaptable cyber incident response plans
29 to address cybersecurity risks (as defined in section 10545 of this title) to
30 critical infrastructure.

31 (d) NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination
32 with the heads of other appropriate Federal departments and agencies, and
33 in accordance with the National Cybersecurity Incident Response Plan re-
34 quired under subsection (c), shall regularly update, maintain, and exercise
35 the Cyber Incident Annex to the National Response Framework of the De-
36 partment.

37 **§ 10547. NET Guard**

38 The Assistant Secretary for Infrastructure Protection may establish a na-
39 tional technology guard, to be known as “NET Guard”, comprised of local
40 teams of volunteers with expertise in relevant areas of science and tech-

1 nology, to assist local communities to respond and recover from attacks on
2 information systems and communications networks.

3 **§ 10548. Prohibition on new regulatory authority**

4 (a) IN GENERAL.—Nothing in the National Cybersecurity Protection Act
5 of 2014 (Public Law 113–282, 128 Stat. 3066) or the amendments made
6 by the Act shall be construed to grant the Secretary any authority to pro-
7 mulgate regulations or set standards relating to the cybersecurity of private-
8 sector critical infrastructure that was not in effect on December 17, 2014.

9 (b) PRIVATE ENTITIES.—Nothing in the National Cybersecurity Protec-
10 tion Act of 2014 (Public Law 113–282, 128 Stat. 3066) or the amendments
11 made by the Act shall be construed to require any private entity—

12 (1) to request assistance from the Secretary; or

13 (2) that requested assistance from the Secretary to implement any
14 measure or recommendation suggested by the Secretary.

15 **§ 10549. Federal intrusion detection and prevention system**

16 (a) DEFINITIONS.—In subsections (a) through (f) of this section:

17 (1) AGENCY.—The term “agency” has the meaning given the term
18 in section 3502 of title 44.

19 (2) AGENCY INFORMATION.—The term “agency information” means
20 information collected or maintained by or on behalf of an agency.

21 (3) AGENCY INFORMATION SYSTEM.—The term “agency information
22 system” has the meaning given the term in section 10546 of this title.

23 (4) CYBERSECURITY RISK, INFORMATION SYSTEM.—The terms “cy-
24 bersecurity risk” and “information system” have the meanings given
25 the terms in section 10545 of this title.

26 (b) DEPLOYMENT, OPERATION, AND MAINTENANCE OF CAPABILITIES.—

27 (1) IN GENERAL.—Not later than December 18, 2016, the Secretary
28 shall deploy, operate, and maintain, to make available for use by any
29 agency, with or without reimbursement—

30 (A) a capability to detect cybersecurity risks in network traffic
31 transiting or traveling to or from an agency information system;
32 and

33 (B) a capability to—

34 (i) prevent network traffic associated with those cybersecur-
35 ity risks from transiting or traveling to or from an agency
36 information system; or

37 (ii) modify the network traffic to remove the cybersecurity
38 risk.

39 (2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy
40 new technologies and modify existing technologies to the intrusion de-

1 tection and prevention capabilities described in paragraph (1) as appro-
2 priate to improve the intrusion detection and prevention capabilities.

3 (c) ACTIVITIES.—In carrying out subsection (b), the Secretary—

4 (1) may access, and the head of an agency may disclose to the Sec-
5 retary or a private entity providing assistance to the Secretary under
6 paragraph (2), information transiting or traveling to or from an agency
7 information system, regardless of the location from which the Secretary
8 or a private entity providing assistance to the Secretary under para-
9 graph (2) accesses the information, notwithstanding any other provi-
10 sion of law that would otherwise restrict or prevent the head of an
11 agency from disclosing the information to the Secretary or a private
12 entity providing assistance to the Secretary under paragraph (2);

13 (2) may enter into contracts or other agreements with, or otherwise
14 request and obtain the assistance of, private entities to deploy, operate,
15 and maintain technologies in accordance with subsection (b);

16 (3) may retain, use, and disclose information obtained through the
17 conduct of activities authorized under this section only to protect infor-
18 mation and information systems from cybersecurity risks;

19 (4) shall regularly assess, through operational test and evaluation in
20 real world or simulated environments, available advanced protective
21 technologies to improve detection and prevention capabilities, including
22 commercial and noncommercial technologies and detection technologies
23 beyond signature-based detection, and acquire, test, and deploy the
24 technologies when appropriate;

25 (5) shall establish a pilot through which the Secretary may acquire,
26 test, and deploy, as rapidly as possible, technologies described in para-
27 graph (4); and

28 (6) shall periodically update the privacy impact assessment required
29 under section 208(b) of the E-Government Act of 2002 (44 U.S.C.
30 3501 note).

31 (d) PRINCIPLES.—In carrying out subsection (b), the Secretary shall en-
32 sure that—

33 (1) activities carried out under this section are reasonably necessary
34 for the purpose of protecting agency information and agency informa-
35 tion systems from a cybersecurity risk;

36 (2) information accessed by the Secretary will be retained no longer
37 than reasonably necessary for the purpose of protecting agency infor-
38 mation and agency information systems from a cybersecurity risk;

39 (3) notice has been provided to users of an agency information sys-
40 tem concerning access to communications of users of the agency infor-

1 information system for the purpose of protecting agency information and
2 the agency information system; and

3 (4) the activities are implemented pursuant to policies and proce-
4 dures governing the operation of the intrusion detection and prevention
5 capabilities.

6 (e) PRIVATE ENTITIES.—

7 (1) CONDITIONS.—A private entity described in subsection (c)(2)
8 may not—

9 (A) disclose any network traffic transiting or traveling to or
10 from an agency information system to any entity other than the
11 Department or the agency that disclosed the information under
12 subsection (c)(1), including personal information of a specific indi-
13 vidual or information that identifies a specific individual not di-
14 rectly related to a cybersecurity risk; or

15 (B) use any network traffic transiting or traveling to or from
16 an agency information system to which the private entity gains ac-
17 cess in accordance with this section for any purpose other than to
18 protect agency information and agency information systems
19 against cybersecurity risks or to administer a contract or other
20 agreement entered into pursuant to subsection (c)(2) or as part
21 of another contract with the Secretary.

22 (2) LIMITATION ON LIABILITY.—No cause of action shall lie in any
23 court against a private entity for assistance provided to the Secretary
24 in accordance with this section and any contract or agreement entered
25 into pursuant to subsection (c)(2).

26 (3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be
27 construed to authorize an Internet service provider to break a user
28 agreement with a customer without the consent of the customer.

29 (f) PRIVACY OFFICER REVIEW.—Not later than December 18, 2016, the
30 Privacy Officer appointed under section 10543 of this title, in consultation
31 with the Attorney General, shall review the policies and guidelines for the
32 program carried out under this section to ensure that the policies and guide-
33 lines are consistent with applicable privacy laws, including those governing
34 the acquisition, interception, retention, use, and disclosure of communica-
35 tions.

36 (g) AGENCY RESPONSIBILITIES.—

37 (1) DEFINITION OF AGENCY INFORMATION SYSTEM.—In this sub-
38 section, the term “agency information system” means an information
39 system owned or operated by an agency.

40 (2) IN GENERAL.—Except as provided in paragraph (3)—

1 (A) not later than December 18, 2016, or 2 months after the
2 date on which the Secretary makes available the intrusion detec-
3 tion and prevention capabilities under subsection (b)(1), whichever
4 is later, the head of each agency shall apply and continue to utilize
5 the capabilities to all information traveling between an agency in-
6 formation system and another information system; and

7 (B) not later than 6 months after the date on which the Sec-
8 retary makes available improvements to the intrusion detection
9 and prevention capabilities pursuant to subsection (b)(2), the head
10 of each agency shall apply and continue to utilize the improved in-
11 trusion detection and prevention capabilities.

12 (3) EXCEPTION.—The requirements under paragraph (2) shall not
13 apply to the Department of Defense, a national security system, or an
14 element of the intelligence community.

15 (4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be
16 construed to limit an agency from applying the intrusion detection and
17 prevention capabilities to an information system other than an agency
18 information system under subsection (b)(1) at the discretion of the
19 head of the agency or as provided in relevant policies, directives, and
20 guidelines.

21 (h) RULE OF CONSTRUCTION.—Nothing in subsection (i) shall be con-
22 strued to affect the limitation of liability of a private entity for assistance
23 provided to the Secretary under subsection (d)(2) if the assistance was ren-
24 dered before the termination date under subsection (i) or otherwise during
25 a period in which the assistance was authorized.

26 (i) TERMINATION.—The requirements under subsections (a) through (f)
27 of this section terminate on December 18, 2022.

28 **§ 10550. Cybersecurity strategy**

29 (a) DEFINITION OF HOMELAND SECURITY ENTERPRISE.—In this section,
30 the term “Homeland Security Enterprise” means relevant governmental and
31 nongovernmental entities involved in homeland security, including Federal,
32 State, local, and tribal government officials, private-sector representatives,
33 academics, and other policy experts.

34 (b) DEVELOPMENT OF STRATEGY.—The Secretary shall develop a depart-
35 mental strategy to carry out cybersecurity responsibilities as set forth by
36 law.

37 (c) CONTENTS.—The strategy required under subsection (b) shall include
38 the following:

39 (1) Strategic and operational goals and priorities to successfully exe-
40 cute the full range of the Secretary’s cybersecurity responsibilities.

1 (2) Information on the programs, policies, and activities that are re-
2 quired to successfully execute the full range of the Secretary's cyberse-
3 curity responsibilities, including programs, policies, and activities in
4 furtherance of the following:

5 (A) Cybersecurity functions set forth in section 10545 of this
6 title.

7 (B) Cybersecurity investigation capabilities.

8 (C) Cybersecurity research and development.

9 (D) Engagement with international cybersecurity partners.

10 (d) CONSIDERATIONS.—In developing the strategy required under sub-
11 section (b), the Secretary shall—

12 (1) consider—

13 (A) the cybersecurity strategy for the Homeland Security Enter-
14 prise published by the Secretary in November 2011;

15 (B) the Department of Homeland Security Fiscal Years 2014–
16 2018 Strategic Plan; and

17 (C) the most recent Quadrennial Homeland Security Review
18 issued pursuant to section 11506 of this title; and

19 (2) include information on the roles and responsibilities of compo-
20 nents and offices of the Department, to the extent practicable, to carry
21 out the strategy.

22 (e) IMPLEMENTATION PLAN.—Not later than 90 days after the develop-
23 ment of the strategy required under subsection (b), the Secretary shall issue
24 an implementation plan for the strategy that includes the following:

25 (1) Strategic objectives and corresponding tasks.

26 (2) Projected timelines and costs for the tasks.

27 (3) Metrics to evaluate performance of the tasks.

28 (f) CONGRESSIONAL OVERSIGHT.—The Secretary shall submit to Con-
29 gress for assessment the following:

30 (1) A copy of the strategy required under subsection (b) on issuance.

31 (2) A copy of the implementation plan required under subsection (e),
32 on issuance, together with detailed information on any associated legis-
33 lative or budgetary proposals.

34 (g) CLASSIFIED INFORMATION.—The strategy required under subsection
35 (b) shall be in an unclassified form but may contain a classified annex.

36 (h) RULE OF CONSTRUCTION.—Nothing in this section may be construed
37 as permitting the Department to engage in monitoring, surveillance,
38 exfiltration, or other collection activities for the purpose of tracking an indi-
39 vidual's personally identifiable information.

Part B—Cybersecurity Information Sharing

§ 10561. Definitions

In this part:

(1) AGENCY.—The term “agency” has the meaning given the term in section 3502 of title 44.

(2) ANTITRUST LAWS.—The term “antitrust laws”—

(A) has the meaning given the term in the 1st section of the Clayton Act (15 U.S.C. 12);

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair competition; and

(C) includes any State antitrust law, but only to the extent that the law is consistent with the law referred to in subparagraph (A) or (B).

(3) APPROPRIATE FEDERAL ENTITIES.—The term “appropriate federal entities” means the following:

(A) The Department of Commerce.

(B) The Department of Defense.

(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

(4) CYBERSECURITY PURPOSE.—The term “cybersecurity purpose” means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(5) CYBERSECURITY THREAT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term “cybersecurity threat” means an action, not protected by the 1st amendment of the Constitution, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed in, or transiting an information system.

(B) EXCLUSION.—The term “cybersecurity threat” does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(6) CYBER THREAT INDICATOR.—The term “cyber threat indicator” means information that is necessary to describe or identify—

1 (A) malicious reconnaissance, including anomalous patterns of
 2 communication that appear to be transmitted for the purpose of
 3 gathering technical information relating to a cybersecurity threat
 4 or security vulnerability;

5 (B) a method of defeating a security control or exploitation of
 6 a security vulnerability;

7 (C) a security vulnerability, including anomalous activity that
 8 appears to indicate the existence of a security vulnerability;

9 (D) a method of causing a user with legitimate access to an in-
 10 formation system or information that is stored on, processed by,
 11 or transiting an information system to unwittingly enable the de-
 12 feat of a security control or exploitation of a security vulnerability;

13 (E) malicious cyber command and control;

14 (F) the actual or potential harm caused by an incident, includ-
 15 ing a description of the information exfiltrated as a result of a
 16 particular cybersecurity threat;

17 (G) any other attribute of a cybersecurity threat, if disclosure
 18 of the attribute is not otherwise prohibited by law; or

19 (H) any combination of subparagraphs (A) through (G).

20 (7) DEFENSIVE MEASURE.—

21 (A) IN GENERAL.—Except as provided in subparagraph (B), the
 22 term “defensive measure” means an action, device, procedure, sig-
 23 nature, technique, or other measure applied to an information sys-
 24 tem or information that is stored on, processed by, or transiting
 25 an information system that detects, prevents, or mitigates a known
 26 or suspected cybersecurity threat or security vulnerability.

27 (B) EXCLUSION.—The term “defensive measure” does not in-
 28 clude a measure that destroys, renders unusable, provides unau-
 29 thorized access to, or substantially harms an information system
 30 or information stored on, processed by, or transiting the informa-
 31 tion system not owned by—

32 (i) the private entity operating the measure; or

33 (ii) another entity or Federal entity that may provide con-
 34 sent and has provided consent to that private entity for oper-
 35 ation of the measure.

36 (8) FEDERAL ENTITY.—The term “Federal entity” means a depart-
 37 ment or agency of the United States or any component of the depart-
 38 ment or agency.

39 (9) INFORMATION SYSTEM.—The term “information system”—

40 (A) has the meaning given the term in section 3502 of title 44;
 41 and

1 (B) includes industrial control systems such as supervisory con-
2 trol and data acquisition systems, distributed control systems, and
3 programmable logic controllers.

4 (10) LOCAL GOVERNMENT.—The term “local government” means
5 any borough, city, county, parish, town, township, village or other polit-
6 ical subdivision of a State.

7 (11) MALICIOUS CYBER COMMAND AND CONTROL.—The term “mali-
8 cious cyber command and control” means a method for unauthorized
9 remote identification of, access to, or use of, an information system or
10 information that is stored on, processed by, or transiting an informa-
11 tion system.

12 (12) MALICIOUS RECONNAISSANCE.—The term “malicious reconnais-
13 sance” means a method for actively probing or passively monitoring an
14 information system for the purpose of discerning security vulnerabilities
15 of the information system, if the method is associated with a known
16 or suspected cybersecurity threat.

17 (13) 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 (14) NON-FEDERAL ENTITY.—

21 (A) IN GENERAL.—Except as provided in this paragraph, the
22 term “non-Federal entity” means any private entity, non-Federal
23 Government agency or department, or State, tribal, or local gov-
24 ernment (including a political subdivision, department, or compo-
25 nent of the government).

26 (B) INCLUSIONS.—The term “non-Federal entity” includes a
27 government agency or department of the District of Columbia,
28 Puerto Rico, the Virgin Islands, Guam, American Samoa, the
29 Northern Mariana Islands, and any other territory or possession
30 of the United States.

31 (C) EXCLUSIONS.—The term “non-Federal entity” does not in-
32 clude a foreign power as defined in section 101 of the Foreign In-
33 telligence Surveillance Act of 1978 (50 U.S.C. 1801).

34 (15) PRIVATE ENTITY.—

35 (A) IN GENERAL.—Except as provided in this paragraph, the
36 term “private entity” means any person or private group, organi-
37 zation, proprietorship, partnership, trust, cooperative organization,
38 or other commercial or nonprofit entity, including an officer, em-
39 ployee, or agent.

1 (B) INCLUSION.—The term “private entity” includes a State,
2 tribal, or local government performing utility services, such as
3 electric, natural gas, or water services.

4 (C) EXCLUSION.—The term “private entity” does not include a
5 foreign power as defined in section 101 of the Foreign Intelligence
6 Surveillance Act of 1978 (50 U.S.C. 1801).

7 (16) SECURITY CONTROL.—The term “security control” means the
8 management, operational, and technical controls used to protect
9 against an unauthorized effort to adversely affect the confidentiality,
10 integrity, and availability of an information system or its information.

11 (17) SECURITY VULNERABILITY.—The term “security vulnerability”
12 means any attribute of hardware, software, process, or procedure that
13 could enable or facilitate the defeat of a security control.

14 (18) TRIBAL.—The term “tribal” has the meaning given the term
15 “Indian tribe” in section 4 of the Indian Self-Determination and Edu-
16 cation Assistance Act (25 U.S.C. 450b).

17 **§ 10562. Procedures for sharing information by Federal Gov-**
18 **ernment**

19 (a) IN GENERAL.—Consistent with the protection of classified informa-
20 tion, intelligence sources and methods, and privacy and civil liberties, the
21 Director of National Intelligence, the Secretary of Homeland Security, the
22 Secretary of Defense, and the Attorney General, in consultation with the
23 heads of the appropriate Federal entities, shall jointly develop and issue pro-
24 cedures to facilitate and promote—

25 (1) timely sharing of classified cyber threat indicators and defensive
26 measures the Federal Government possesses with representatives of rel-
27 evant Federal entities and non-Federal entities that have appropriate
28 security clearances;

29 (2) timely sharing with relevant Federal entities and non-Federal en-
30 tities of cyber threat indicators, defensive measures, and information
31 relating to cybersecurity threats or authorized uses under this part, in
32 the possession of the Federal Government, that may be declassified and
33 shared at an unclassified level;

34 (3) timely sharing with relevant Federal entities and non-Federal en-
35 tities, or the public if appropriate, of unclassified, including controlled
36 unclassified, cyber threat indicators and defensive measures the Fed-
37 eral Government possesses;

38 (4) timely sharing with Federal entities and non-Federal entities, if
39 appropriate, of information relating to cybersecurity threats or author-
40 ized uses under this part that the Federal Government possesses about

1 cybersecurity threats to those entities to prevent or mitigate adverse ef-
2 fects from the threats; and

3 (5) periodic sharing, through publication and targeted outreach, of
4 cybersecurity best practices that are developed based on ongoing anal-
5 yses of cyber threat indicators, defensive measures, and information re-
6 lating to cybersecurity threats or authorized uses under this part, in
7 the possession of the Federal Government with attention to accessibility
8 and implementation challenges faced by small business concerns (as de-
9 fined in section 3 of the Small Business Act (15 U.S.C. 632)).

10 (b) CONTENT.—The procedures developed under subsection (a) shall—

11 (1) ensure the Federal Government has and maintains the capability
12 to share cyber threat indicators and defensive measures in real time
13 consistent with the protection of classified information;

14 (2) incorporate to the greatest extent practicable existing processes
15 and existing roles and responsibilities of Federal entities and non-Fed-
16 eral entities for information sharing by the Federal Government, in-
17 cluding sector specific information sharing and analysis centers;

18 (3) include procedures for notifying, in a timely manner, Federal en-
19 tities and non-Federal entities that have received a cyber threat indi-
20 cator or defensive measure from a Federal entity under this part that
21 is known or determined to be in error or in contravention of the re-
22 quirements of this part or another provision of Federal law or policy
23 of the error or contravention;

24 (4) include requirements for Federal entities sharing cyber threat in-
25 dicators or defensive measures to implement and utilize security con-
26 trols to protect against unauthorized access to, or acquisition of, the
27 indicators or measures;

28 (5) include procedures that require a Federal entity, prior to the
29 sharing of a cyber threat indicator—

30 (A) to—

31 (i) review the indicator to assess whether the indicator con-
32 tains any information not directly related to a cybersecurity
33 threat that the Federal entity knows at the time of sharing
34 to be personal information of a specific individual or informa-
35 tion that identifies a specific individual; and

36 (ii) remove the information; or

37 (B) to implement and utilize a technical capability configured to
38 remove information not directly related to a cybersecurity threat
39 that the Federal entity knows at the time of sharing to be per-
40 sonal information of a specific individual or information that iden-
41 tifies a specific individual; and

1 (6) include procedures for notifying, in a timely manner, any United
2 States person whose personal information is known or determined to
3 have been shared by a Federal entity in violation of this part.

4 (e) CONSULTATION.—In developing the procedures required under this
5 section, the Director of National Intelligence, the Secretary, the Secretary
6 of Defense, and the Attorney General shall consult with appropriate Federal
7 entities, including the Small Business Administration and the National Labora-
8 tories (as defined in section 2 of the Energy Policy Act of 2005 (42
9 U.S.C. 15801)), to ensure that effective protocols are implemented that will
10 facilitate and promote the sharing of cyber threat indicators by the Federal
11 Government in a timely manner.

12 (d) SUBMITTAL TO CONGRESS.—The Director of National Intelligence, in
13 consultation with the heads of the appropriate Federal entities, shall submit
14 to Congress the procedures required by subsection (a).

15 **§ 10563. Authorization for preventing, detecting, analyzing,**
16 **and mitigating cybersecurity threats.**

17 (a) AUTHORIZATION FOR MONITORING.—

18 (1) IN GENERAL.—A private entity may, for cybersecurity purposes,
19 monitor—

20 (A) an information system of the private entity;

21 (B) an information system of another non-Federal entity, on the
22 authorization and written consent of the other entity;

23 (C) an information system of a Federal entity, on the authoriza-
24 tion and written consent of an authorized representative of the
25 Federal entity; and

26 (D) information that is stored on, processed by, or transiting an
27 information system monitored by the private entity under this
28 paragraph.

29 (2) CONSTRUCTION.—Nothing in paragraph (1) shall be construed
30 to—

31 (A) authorize the monitoring of an information system, or the
32 use of information obtained through the monitoring, other than as
33 provided in this part; or

34 (B) limit otherwise lawful activity.

35 (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

36 (1) IN GENERAL.—A private entity may, for cybersecurity purposes,
37 operate a defensive measure that is applied to—

38 (A) an information system of the private entity to protect the
39 rights or property of the entity;

1 (B) an information system of another non-Federal entity, on
 2 written consent of the other entity for operation of the defensive
 3 measure to protect the rights or property of the entity;

4 (C) an information system of a Federal entity on written con-
 5 sent of an authorized representative of the Federal entity for oper-
 6 ation of the defensive measure to protect the rights or property
 7 of the Federal Government.

8 (2) CONSTRUCTION.—Nothing in paragraph (1) shall be construed
 9 to—

10 (A) authorize the use of a defensive measure other than as pro-
 11 vided in paragraph (1); or

12 (B) limit otherwise lawful activity.

13 (e) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDI-
 14 CATORS OR DEFENSIVE MEASURES.—

15 (1) IN GENERAL.—Except as provided in paragraph (2), a non-Fed-
 16 eral entity may, for a cybersecurity purpose and consistent with the
 17 protection of classified information, share with, or receive, from, any
 18 other non-Federal entity or the Federal Government a cyber threat indi-
 19 cator or defensive measure.

20 (2) COMPLIANCE WITH LAWFUL RESTRICTION.—A non-Federal enti-
 21 ty receiving a cyber threat indicator or defensive measure from another
 22 non-Federal entity or a Federal entity shall comply with otherwise law-
 23 ful restrictions placed on the sharing or use of the indicator or defen-
 24 sive measure by the sharing non-Federal entity or Federal entity.

25 (3) CONSTRUCTION.—Nothing in paragraph (1) shall be construed
 26 to—

27 (A) authorize the sharing or receiving of a cyber threat indi-
 28 cator or defensive measure other than as provided in paragraph

29 (1); or

30 (B) limit otherwise lawful activity.

31 (d) PROTECTION AND USE OF INFORMATION.—

32 (1) SECURITY OF INFORMATION.—A non-Federal entity monitoring
 33 an information system, operating a defensive measure, or providing or
 34 receiving a cyber threat indicator or defensive measure under this sec-
 35 tion shall implement and utilize a security control to protect against
 36 unauthorized access to or acquisition of the cyber threat indicator or
 37 defensive measure.

38 (2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—A non-Fed-
 39 eral entity sharing a cyber threat indicator pursuant to this part shall,
 40 prior to sharing—

1 (A) review the cyber threat indicator to assess whether the indi-
 2 cator contains any information not directly related to a cybersecu-
 3 rity threat that the non-Federal entity knows at the time of shar-
 4 ing to be personal information of a specific individual or informa-
 5 tion that identifies a specific individual and remove the informa-
 6 tion; or

7 (B) implement and utilize a technical capability configured to
 8 remove any information not directly related to a cybersecurity
 9 threat that the non-Federal entity knows at the time of sharing
 10 to be personal information of a specific individual or information
 11 that identifies a specific individual.

12 (3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES
 13 BY NON-FEDERAL ENTITIES.—

14 (A) IN GENERAL.—Consistent with this part, a cyber threat indi-
 15 cator or defensive measure shared or received under this section
 16 may, for cybersecurity purposes—

17 (i) be used by a non-Federal entity to monitor or operate
 18 a defensive measure that is applied to—

19 (I) an information system of the non-Federal entity;

20 or

21 (II) an information system of another non-Federal en-
 22 tity or a Federal entity on the written consent of the
 23 other non-Federal entity or that Federal entity; and

24 (ii) be otherwise used, retained, and further shared by a
 25 non-Federal entity subject to—

26 (I) an otherwise lawful restriction placed by the shar-
 27 ing non-Federal entity or Federal entity on the cyber
 28 threat indicator or defensive measure; or

29 (II) an otherwise applicable provision of law.

30 (B) CONSTRUCTION.—Nothing in subparagraph (A) shall be
 31 construed to authorize the use of a cyber threat indicator or defen-
 32 sive measure other than as provided in this section.

33 (4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR
 34 LOCAL GOVERNMENT.—

35 (A) LAW ENFORCEMENT USE.—A State, tribal, or local govern-
 36 ment that receives a cyber threat indicator or defensive measure
 37 under this part may use the cyber threat indicator or defensive
 38 measure for the purposes described in section 10564(e)(5)(A) of
 39 this title.

40 (B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator
 41 or defensive measure shared by or with a State, tribal, or local

1 government, including a component of a State, tribal, or local gov-
 2 ernment that is a private entity, under this section shall be—

3 (i) considered voluntarily shared information; and

4 (ii) exempt from disclosure under any provision of State,
 5 tribal, or local freedom of information law, open government
 6 law, open meetings law, open records law, sunshine law, or
 7 similar law requiring disclosure of information or records.

8 (C) STATE, TRIBAL, AND LOCAL REGULATORY AUTHORITY.—

9 (i) IN GENERAL.—Except as provided in clause (ii), a cyber
 10 threat indicator or defensive measure shared with a State,
 11 tribal, or local government under this part shall not be used
 12 by any State, tribal, or local government to regulate, includ-
 13 ing an enforcement action, the lawful activity of any non-Fed-
 14 eral entity or any activity taken by a non-Federal entity pur-
 15 suant to mandatory standards, including an activity relating
 16 to monitoring, operating a defensive measure, or sharing a
 17 cyber threat indicator.

18 (ii) REGULATORY AUTHORITY SPECIFICALLY RELATING TO
 19 PREVENTION OR MITIGATION OF CYBERSECURITY
 20 THREATS.—A cyber threat indicator or defensive measure
 21 shared as described in clause (i) may, consistent with a State,
 22 tribal, or local government regulatory authority specifically re-
 23 lating to the prevention or mitigation of cybersecurity threats
 24 to information systems, inform the development or implemen-
 25 tation of a regulation relating to the information systems.

26 (e) ANTITRUST EXEMPTION.—

27 (1) IN GENERAL.—Except as provided in section 10569(e) of this
 28 title, it shall not be considered a violation of any provision of antitrust
 29 laws for 2 or more private entities to exchange or provide a cyber
 30 threat indicator or defensive measure, or assistance, relating to the pre-
 31 vention, investigation, or mitigation of a cybersecurity threat, for cyber-
 32 security purposes under this part.

33 (2) APPLICABILITY.—Paragraph (1) shall apply only to information
 34 that is exchanged or assistance provided to assist with—

35 (A) facilitating the prevention, investigation, or mitigation of a
 36 cybersecurity threat to an information system or information that
 37 is stored on, processed by, or transiting an information system; or

38 (B) communicating or disclosing a cyber threat indicator to help
 39 prevent, investigate, or mitigate the effect of a cybersecurity threat
 40 to an information system or information that is stored on, pro-
 41 cessed by, or transiting an information system.

1 (f) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator or
 2 defensive measure with a non-Federal entity under this part shall not create
 3 a right or benefit to similar information by the non-Federal entity or any
 4 other non-Federal entity.

5 **§ 10564. Sharing of cyber threat indicators and defensive**
 6 **measures with Federal Government**

7 (a) DEVELOPMENT OF POLICIES AND PROCEDURES.—The Attorney Gen-
 8 eral and the Secretary shall, in consultation with the heads of the appro-
 9 priate Federal entities, jointly issue and make publicly available policies and
 10 procedures relating to the receipt of cyber threat indicators and defensive
 11 measures by the Federal Government. Consistent with the guidelines re-
 12 quired by subsection (d), the policies and procedures shall ensure—

13 (1) that cyber threat indicators shared with the Federal Government
 14 by any non-Federal entity pursuant to section 10563(c) of this title
 15 through the real-time process described in subsection (d)—

16 (A) are shared in an automated manner with all appropriate
 17 Federal entities;

18 (B) are only subject to a delay, modification, or other action due
 19 to controls established for the real-time process that could impede
 20 real-time receipt by all appropriate Federal entities when the
 21 delay, modification, or other action is due to controls—

22 (i) agreed on unanimously by all of the heads of the appro-
 23 priate Federal entities;

24 (ii) carried out before any appropriate Federal entity re-
 25 tains or uses the cyber threat indicators or defensive meas-
 26 ures; and

27 (iii) uniformly applied so that each appropriate Federal en-
 28 tity is subject to the same delay, modification, or other ac-
 29 tion; and

30 (C) may be provided to other Federal entities;

31 (2) that cyber threat indicators shared with the Federal Government
 32 by any non-Federal entity pursuant to section 10563 of this title in a
 33 manner other than the real-time process described in subsection (d)—

34 (A) are shared as quickly as operationally practicable with all
 35 appropriate Federal entities;

36 (B) are not subject to any unnecessary delay, interference, or
 37 any other action that could impede receipt by all appropriate Fed-
 38 eral entities; and

39 (C) may be provided to other Federal entities; and

40 (3) there are—

41 (A) audit capabilities; and

1 (B) appropriate sanctions in place for officers, employees, or
2 agents of a Federal entity who knowingly and willfully conduct ac-
3 tivities under this part in an unauthorized manner.

4 (b) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS
5 WITH FEDERAL GOVERNMENT.—The Attorney General and the Secretary
6 jointly shall develop and make publicly available guidance to assist entities
7 and promote sharing of cyber threat indicators with Federal entities under
8 this part. The guidelines shall include guidance on the following:

9 (1) Identification of types of information that would qualify as a
10 cyber threat indicator under this part that would be unlikely to include
11 information that—

12 (A) is not directly related to a cybersecurity threat; and

13 (B) is personal information of a specific individual or informa-
14 tion that identifies a specific individual.

15 (2) Identification of types of information protected under otherwise
16 applicable privacy laws that are unlikely to be directly related to a cy-
17 bersecurity threat.

18 (3) Such other matters as the Attorney General and the Secretary
19 consider appropriate for entities sharing cyber threat indicators with
20 Federal entities under this part.

21 (c) PRIVACY AND CIVIL LIBERTIES.—

22 (1) ISSUANCE AND AVAILABILITY OF GUIDELINES.—The Attorney
23 General and the Secretary shall, in coordination with the heads of the
24 appropriate Federal entities and in consultation with officers des-
25 ignated under section 1062 of the Intelligence Reform and Terrorism
26 Prevention Act of 2004 (42 U.S.C. 2000ee–1) and such private entities
27 with industry expertise as the Attorney General and the Secretary con-
28 sider relevant, jointly issue and make publicly available final guidelines
29 relating to privacy and civil liberties that shall govern the receipt, re-
30 tention, use, and dissemination of cyber threat indicators by a Federal
31 entity obtained in connection with activities authorized in this part.

32 (2) CONTENT.—The guidelines shall, consistent with the need to pro-
33 tect information systems from cybersecurity threats and mitigate cyber-
34 security threats—

35 (A) limit the effect on privacy and civil liberties of activities by
36 the Federal Government under this part;

37 (B) limit the receipt, retention, use, and dissemination of cyber
38 threat indicators containing personal information of specific indi-
39 viduals or information that identifies specific individuals, including
40 by establishing—

1 (i) a process for the timely destruction of the information
2 that is known not to be directly related to uses authorized
3 under this part; and

4 (ii) specific limitations on the length of any period in which
5 a cyber threat indicator may be retained;

6 (C) include requirements to safeguard cyber threat indicators
7 containing personal information of specific individuals or informa-
8 tion that identifies specific individuals from unauthorized access or
9 acquisition, including appropriate sanctions for activities by offi-
10 cers, employees, or agents of the Federal Government in con-
11 travention of the guidelines;

12 (D) consistent with this part, any other applicable provisions of
13 law, and the fair information practice principles set forth in ap-
14 pendix A of the document entitled “National Strategy for Trusted
15 Identities in Cyberspace” and published by the President in April
16 2011, govern the retention, use, and dissemination by the Federal
17 Government of cyber threat indicators shared with the Federal
18 Government under this part, including the extent to which the
19 cyber threat indicators may be used by the Federal Government;

20 (E) include procedures for notifying entities and Federal enti-
21 ties if information received pursuant to this section is known or
22 determined by a Federal entity receiving the information not to
23 constitute a cyber threat indicator;

24 (F) protect the confidentiality of cyber threat indicators con-
25 taining personal information of specific individuals or information
26 that identifies specific individuals to the greatest extent practicable
27 and require recipients to be informed that the indicators may only
28 be used for purposes authorized under this part; and

29 (G) include steps that may be needed so that dissemination of
30 cyber threat indicators is consistent with the protection of classi-
31 fied and other sensitive national security information.

32 (3) PERIODIC REVIEW.—The Attorney General and the Secretary
33 shall, in coordination with the heads of the appropriate Federal entities
34 and in consultation with officers and private entities described in para-
35 graph (1), periodically, but not less frequently than once every 2 years,
36 jointly review the guidelines issued under paragraph (1).

37 (d) CAPABILITY AND PROCESS IN THE DEPARTMENT.—

38 (1) IN GENERAL.—The Secretary, in coordination with the heads of
39 the appropriate Federal entities, shall develop and implement a capa-
40 bility and process in the Department that—

1 (A) shall accept from any non-Federal entity in real time cyber
2 threat indicators and defensive measures, pursuant to this section;

3 (B) on submittal of the certification under paragraph (2) that
4 the capability and process fully and effectively operates as de-
5 scribed in paragraph (2), shall be the process by which the Fed-
6 eral Government receives cyber threat indicators and +defensive
7 measures under this part that are shared by a non-Federal entity
8 with the Federal Government through electronic mail or media, an
9 interactive form on an Internet website, or a real time, automated
10 process between information systems, except—

11 (i) consistent with section 10563 of this title, communica-
12 tions between a Federal entity and a non-Federal entity re-
13 garding a previously shared cyber threat indicator to—

14 (I) describe the relevant cybersecurity threat; or

15 (II) develop a defensive measure based on the cyber
16 threat indicator; and

17 (ii) communications by a regulated non-Federal entity with
18 the entity's Federal regulatory authority regarding a cyberse-
19 curity threat;

20 (C) ensures that all of the appropriate Federal entities receive
21 in an automated manner cyber threat indicators and defensive
22 measures shared through the real-time process in the Department;

23 (D) is in compliance with the policies, procedures, and guide-
24 lines required by this section; and

25 (E) does not limit or prohibit otherwise lawful disclosures of
26 communications, records, or other information, including—

27 (i) reporting known or suspected criminal activity, by a
28 non-Federal entity to any other non-Federal entity or a Fed-
29 eral entity, including cyber threat indicators or defensive
30 measures shared with a Federal entity in furtherance of open-
31 ing a Federal law enforcement investigation;

32 (ii) voluntary or legally compelled participation in a Fed-
33 eral investigation; and

34 (iii) providing cyber threat indicators or defensive measures
35 as part of a statutory or authorized contractual requirement.

36 (2) CERTIFICATION AND DESIGNATION.—

37 (A) CERTIFICATION OF CAPABILITY AND PROCESS.—The Sec-
38 retary shall, in consultation with the heads of the appropriate Fed-
39 eral entities, submit to Congress a certification as to whether the
40 capability and process required by paragraph (1) fully and effec-
41 tively operates—

1 (i) as the process by which the Federal Government re-
2 ceives from any non-Federal entity a cyber threat indicator
3 or defensive measure under this part; and

4 (ii) in accordance with the interim policies, procedures, and
5 guidelines developed under this part.

6 (B) DESIGNATION.—

7 (i) IN GENERAL.—At any time after certification is sub-
8 mitted under subparagraph (A), the President may designate
9 an appropriate Federal entity, other than the Department of
10 Defense (including the National Security Agency), to develop
11 and implement a capability and process as described in para-
12 graph (1) in addition to the capability and process developed
13 under paragraph (1) by the Secretary, if, not fewer than 30
14 days before making the designation, the President submits to
15 Congress a certification and explanation that—

16 (I) the designation is necessary to ensure full, effec-
17 tive, and secure operation of a capability and process for
18 the Federal Government to receive from any non-Federal
19 entity cyber threat indicators or defensive measures
20 under this part;

21 (II) the designated appropriate Federal entity will re-
22 ceive and share cyber threat indicators and defensive
23 measures in accordance with the policies, procedures,
24 and guidelines developed under this part, including sub-
25 section (a)(1); and

26 (III) the designation is consistent with the mission of
27 the appropriate Federal entity and improves the ability
28 of the Federal Government to receive, share, and use
29 cyber threat indicators and defensive measures as au-
30 thorized under this part.

31 (ii) APPLICATION TO ADDITIONAL CAPABILITY AND PROC-
32 ESS.—If the President designates an appropriate Federal en-
33 tity to develop and implement a capability and process under
34 clause (i), the provisions of this part that apply to the capa-
35 bility and process required by paragraph (1) apply to the ca-
36 pability and process developed and implemented under clause
37 (i).

38 (3) PUBLIC NOTICE AND ACCESS.—The Secretary shall ensure there
39 is public notice of, and access to, the capability and process developed
40 and implemented under paragraph (1) so that—

1 (A) any non-Federal entity may share cyber threat indicators
2 and defensive measures through the process with the Federal Gov-
3 ernment; and

4 (B) all of the appropriate Federal entities receive the cyber
5 threat indicators and defensive measures in real time with receipt
6 through the process in the Department consistent with the policies
7 and procedures issued under subsection (a).

8 (4) OTHER FEDERAL ENTITIES.—The process developed and imple-
9 mented under paragraph (1) shall ensure that other Federal entities re-
10 ceive in a timely manner any cyber threat indicators and defensive
11 measures shared with the Federal Government through the process.

12 (e) INFORMATION SHARED WITH OR PROVIDED TO FEDERAL GOVERN-
13 MENT.—

14 (1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of
15 cyber threat indicators and defensive measures to the Federal Govern-
16 ment under this part shall not constitute a waiver of any applicable
17 privilege or protection provided by law, including trade secret protec-
18 tion.

19 (2) PROPRIETARY INFORMATION.—Consistent with section
20 10563(e)(2) of this title and any other applicable provision of law, a
21 cyber threat indicator or defensive measure provided by a non-Federal
22 entity to the Federal Government under this part shall be considered
23 the commercial, financial, and proprietary information of the non-Fed-
24 eral entity when so designated by the originating non-Federal entity or
25 a 3d party acting in accordance with the written authorization of the
26 originating non-Federal entity.

27 (3) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator or de-
28 fensive measure shared with the Federal Government under this part
29 shall be—

30 (A) deemed voluntarily shared information and exempt from dis-
31 closure under section 552 of title 5 and any State, tribal, or local
32 provision of law requiring disclosure of information or records; and

33 (B) withheld, without discretion, from the public under section
34 552(b)(3)(B) of title 5 and any State, tribal, or local provision of
35 law requiring disclosure of information or records.

36 (4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat
37 indicator or defensive measure to the Federal Government under this
38 part shall not be subject to a rule of any Federal agency or department
39 or any judicial doctrine regarding ex parte communications with a deci-
40 sion-making official.

41 (5) DISCLOSURE, RETENTION, AND USE.—

1 (A) AUTHORIZED ACTIVITIES.—Cyber threat indicators and de-
2 fensive measures provided to the Federal Government under this
3 part may, consistent with otherwise applicable provisions of Fed-
4 eral law, be disclosed to, retained by, and used by any Federal
5 agency or department, component, officer, employee, or agent of
6 the Federal Government solely for—

7 (i) a cybersecurity purpose;

8 (ii) the purpose of identifying—

9 (I) a cybersecurity threat, including the source of the
10 cybersecurity threat; or

11 (II) a security vulnerability;

12 (iii) the purpose of responding to, or otherwise preventing
13 or mitigating, a specific threat of death, a specific threat of
14 serious bodily harm, or a specific threat of serious economic
15 harm, including a terrorist act or a use of a weapon of mass
16 destruction;

17 (iv) the purpose of responding to, investigating, prosec-
18 cuting, or otherwise preventing or mitigating, a serious
19 threat to a minor, including sexual exploitation and threats
20 to physical safety; or

21 (v) the purpose of preventing, investigating, disrupting, or
22 prosecuting an offense arising out of a threat described in
23 clause (iii) or any of the offenses listed in sections 1028
24 through 1030 and chapters 37 and 90 of title 18.

25 (B) PROHIBITED ACTIVITIES.—Cyber threat indicators and de-
26 fensive measures provided to the Federal Government under this
27 part shall not be disclosed to, retained by, or used by any Federal
28 agency or department for any use not permitted under subpara-
29 graph (A).

30 (C) PRIVACY AND CIVIL LIBERTIES.—Cyber threat indicators
31 and defensive measures provided to the Federal Government under
32 this part shall be retained, used, and disseminated by the Federal
33 Government—

34 (i) in accordance with the policies, procedures, and guide-
35 lines required by subsections (a) through (c);

36 (ii) in a manner that protects from unauthorized use or
37 disclosure any cyber threat indicators that may contain—

38 (I) personal information of a specific individual; or

39 (II) information that identifies a specific individual;

40 and

1 (iii) in a manner that protects the confidentiality of cyber
2 threat indicators containing—

3 (I) personal information of a specific individual; or

4 (II) information that identifies a specific individual.

5 (D) FEDERAL REGULATORY AUTHORITY.—

6 (i) IN GENERAL.—Except as provided in clause (ii), cyber
7 threat indicators and defensive measures provided to the Fed-
8 eral Government under this part shall not be used by any
9 Federal, State, tribal, or local government to regulate, includ-
10 ing an enforcement action, the lawful activities of any non-
11 Federal entity or any activities taken by a non-Federal entity
12 pursuant to mandatory standards, including activities relating
13 to monitoring, operating defensive measures, or sharing cyber
14 threat indicators.

15 (ii) EXCEPTIONS.—

16 (I) REGULATORY AUTHORITY SPECIFICALLY RELATING
17 TO PREVENTION OR MITIGATION OF CYBERSECURITY
18 THREATS.—Cyber threat indicators and defensive meas-
19 ures provided to the Federal Government under this part
20 may, consistent with Federal or State regulatory author-
21 ity specifically relating to the prevention or mitigation of
22 cybersecurity threats to information systems, inform the
23 development or implementation of regulations relating to
24 the information systems.

25 (II) PROCEDURES DEVELOPED AND IMPLEMENTED
26 UNDER THIS PART.—Clause (i) shall not apply to proce-
27 dures developed and implemented under this part.

28 **§ 10565. Protection from liability**

29 (a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall
30 be brought in any court against any private entity, and the action shall be
31 promptly dismissed, for the monitoring of an information system and infor-
32 mation under section 10563(a) of this title that is conducted in accordance
33 with this part.

34 (b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of
35 action shall be brought in any court against any private entity, and the ac-
36 tion shall be promptly dismissed, for the sharing or receipt of a cyber threat
37 indicator or defensive measure under section 10563(e) of this title if—

38 (1) the sharing or receipt is conducted in accordance with this part;

39 and

40 (2) in a case in which a cyber threat indicator or defensive measure
41 is shared with the Federal Government, the cyber threat indicator or

1 defensive measure is shared in a manner that is consistent with section
2 10564(d)(1)(B) of this title.

3 (c) CONSTRUCTION.—Nothing in this part shall be construed—

4 (1) to create—

5 (A) a duty to share a cyber threat indicator or defensive meas-
6 ure; or

7 (B) a duty to warn or act based on the receipt of a cyber threat
8 indicator or defensive measure; or

9 (2) to undermine or limit the availability of otherwise applicable com-
10 mon law or statutory defenses.

11 **§ 10566. Oversight of Government activities**

12 (a) REPORT ON IMPLEMENTATION.—Not later than December 18, 2016,
13 the heads of the appropriate Federal entities shall jointly submit to Con-
14 gress a detailed report concerning the implementation of this part. The re-
15 port may include such recommendations as the heads of the appropriate
16 Federal entities may have for improvements or modifications to the authori-
17 ties, policies, procedures, and guidelines under this part and shall include
18 the following:

19 (1) An evaluation of the effectiveness of real-time information shar-
20 ing through the capability and process developed under section
21 10564(d) of this title, including any impediments to real-time sharing.

22 (2) An assessment of whether cyber threat indicators or defensive
23 measures have been properly classified and an accounting of the num-
24 ber of security clearances authorized by the Federal Government for
25 sharing cyber threat indicators or defensive measures with the private
26 sector.

27 (3) The number of cyber threat indicators or defensive measures re-
28 ceived through the capability and process developed under section
29 10564(d) of this title.

30 (4) A list of Federal entities that have received cyber threat indica-
31 tors or defensive measures under this part.

32 (b) BIENNIAL REPORT ON COMPLIANCE.—

33 (1) WHEN REPORT SHALL BE SUBMITTED.—Not later than Decem-
34 ber 18, 2017, and not less frequently than once every 2 years there-
35 after, the inspectors general of the appropriate Federal entities, in con-
36 sultation with the Inspector General of the Intelligence Community and
37 the Council of Inspectors General on Financial Oversight, shall jointly
38 submit to Congress an interagency report on the actions of the execu-
39 tive branch of the Federal Government to carry out this part during
40 the most recent 2-year period.

1 (2) CONTENTS.—Each report shall include, for the period covered by
2 the report, the following:

3 (A) An assessment of the sufficiency of the policies, procedures,
4 and guidelines relating to the sharing of cyber threat indicators in
5 the Federal Government, including those policies, procedures, and
6 guidelines relating to the removal of information not directly re-
7 lated to a cybersecurity threat that is personal information of a
8 specific individual or information that identifies a specific indi-
9 vidual.

10 (B) An assessment of whether cyber threat indicators or defen-
11 sive measures have been properly classified and an accounting of
12 the number of security clearances authorized by the Federal Gov-
13 ernment for the purpose of sharing cyber threat indicators or de-
14 fensive measures with the private sector.

15 (C) A review of the actions taken by the Federal Government
16 based on cyber threat indicators or defensive measures shared with
17 the Federal Government under this part, including a review of the
18 following:

19 (i) The appropriateness of subsequent uses and dissemina-
20 tions of cyber threat indicators or defensive measures.

21 (ii) Whether cyber threat indicators or defensive measures
22 were shared in a timely and adequate manner with appro-
23 priate entities, or, if appropriate, were made publicly avail-
24 able.

25 (D) An assessment of the cyber threat indicators or defensive
26 measures shared with the appropriate Federal entities under this
27 part, including the following:

28 (i) The number of cyber threat indicators or defensive
29 measures shared through the capability and process developed
30 under section 10564(d) of this title.

31 (ii) An assessment of any information not directly related
32 to a cybersecurity threat that is personal information of a
33 specific individual or information identifying a specific indi-
34 vidual and was shared by a non-Federal government entity
35 with the Federal Government in contravention of this part, or
36 was shared in the Federal Government in contravention of
37 the guidelines required by this part, including a description
38 of any significant violation of this part.

39 (iii) The number of times, according to the Attorney Gen-
40 eral, that information shared under this part was used by a

1 Federal entity to prosecute an offense listed in section
2 10564(e)(5)(A) of this title.

3 (iv) A quantitative and qualitative assessment of the effect
4 of the sharing of cyber threat indicators or defensive meas-
5 ures with the Federal Government on the privacy and civil
6 liberties of specific individuals, including the number of no-
7 tices that were issued with respect to a failure to remove in-
8 formation not directly related to a cybersecurity threat that
9 was personal information of a specific individual or informa-
10 tion that identified a specific individual in accordance with
11 the procedures required by section 10564(c)(2)(E) of this
12 title.

13 (v) The adequacy of any steps taken by the Federal Gov-
14 ernment to reduce any adverse effect from activities carried
15 out under this part on the privacy and civil liberties of United
16 States persons.

17 (E) An assessment of the sharing of cyber threat indicators or
18 defensive measures among Federal entities to identify inappro-
19 priate barriers to sharing information.

20 (3) RECOMMENDATIONS.—Each report may include such rec-
21 ommendations as the inspectors general may have for improvements or
22 modifications to the authorities and processes under this part.

23 (c) INDEPENDENT REPORT ON REMOVAL OF PERSONAL INFORMATION.—
24 Not later than December 18, 2018, the Comptroller General shall submit
25 to Congress a report on the actions taken by the Federal Government to
26 remove personal information from cyber threat indicators or defensive meas-
27 ures pursuant to this part. The report shall include an assessment of the
28 sufficiency of the policies, procedures, and guidelines established under this
29 part in addressing concerns relating to privacy and civil liberties.

30 (d) FORM OF REPORTS.—Each report required under this section shall
31 be submitted in an unclassified form, but may include a classified annex.

32 (e) PUBLIC AVAILABILITY OF REPORTS.—The unclassified portions of the
33 reports required under this section shall be made available to the public.

34 **§ 10567. Report on cybersecurity threats**

35 (a) DEFINITION OF INTELLIGENCE COMMUNITY.—In this section, the
36 term “intelligence community” has the meaning given that term in section
37 3 of the National Security Act of 1947 (50 U.S.C. 3003).

38 (b) WHEN REPORT SHALL BE SUBMITTED.—Not later than 180 days
39 after December 18, 2015, the Director of National Intelligence, in coordina-
40 tion with the heads of other appropriate elements of the intelligence commu-
41 nity, shall submit to the Select Committee on Intelligence of the Senate and

1 the Permanent Select Committee on Intelligence of the House of Represent-
2 atives a report on cybersecurity threats, including cyberattacks, theft, and
3 data breaches.

4 (e) CONTENTS.—The report shall include the following:

5 (1) An assessment of the current intelligence sharing and coopera-
6 tion relationships of the United States with other countries regarding
7 cybersecurity threats, including cyberattacks, theft, and data breaches,
8 directed against the United States that threaten the United States' na-
9 tional security interests, economy, and intellectual property, specifically
10 identifying the relative utility of the relationships, which elements of
11 the intelligence community participate in the relationships, and whether
12 and how the relationships could be improved.

13 (2) A list and an assessment of the countries and nonstate actors
14 that are the primary threats of carrying out a cybersecurity threat, in-
15 cluding a cyberattack, theft, or data breach, against the United States
16 that threatens the United States' national security, economy, and intel-
17 lectual property.

18 (3) A description of the extent to which the capabilities of the United
19 States Government to respond to or prevent cybersecurity threats, in-
20 cluding cyberattacks, theft, or data breaches, directed against the
21 United States private sector are degraded by a delay in the prompt no-
22 tification by private entities of those threats or cyberattacks, theft, and
23 data breaches.

24 (4) An assessment of additional technologies or capabilities that
25 would enhance the ability of the United States to prevent and to re-
26 spond to cybersecurity threats, including cyberattacks, theft, and data
27 breaches.

28 (5) An assessment of any technologies or practices utilized by the
29 private sector that could be rapidly fielded to assist the intelligence
30 community in preventing and responding to cybersecurity threats.

31 (d) FORM OF REPORT.—The report required by subsection (b) shall be
32 made available in classified and unclassified forms.

33 **§ 10568. Exception to limitation on authority of Secretary of**
34 **Defense to disseminate information**

35 Notwithstanding section 393(c)(3) of title 10, the Secretary of Defense
36 may authorize the sharing of cyber threat indicators and defensive measures
37 pursuant to the policies, procedures, and guidelines developed or issued
38 under this part.

39 **§ 10569. Construction and preemption**

40 (a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this part shall be
41 construed—

1 (1) to limit or prohibit otherwise lawful disclosures of communica-
2 tions, records, or other information, including reporting of known or
3 suspected criminal activity, by a non-Federal entity to any other non-
4 Federal entity or the Federal Government under this part; or

5 (2) to limit or prohibit otherwise lawful use of the disclosures by any
6 Federal entity, even when the otherwise lawful disclosures duplicate or
7 replicate disclosures made under this part.

8 (b) WHISTLE BLOWER PROTECTIONS.—Nothing in this part shall be con-
9 strued to prohibit or limit the disclosure of information protected under sec-
10 tion 2302(b)(8) or 7211 of title 5, section 1034 of title 10, section 1104
11 of the National Security Act of 1947 (50 U.S.C. 3234), or any similar pro-
12 vision of Federal or State law.

13 (c) PROTECTION OF SOURCES AND METHODS.—Nothing in this part shall
14 be construed—

15 (1) as creating any immunity against, or otherwise affecting, any ac-
16 tion brought by the Federal Government, or any agency or department
17 of the Government, to enforce any law, executive order, or procedure
18 governing the appropriate handling, disclosure, or use of classified in-
19 formation;

20 (2) to affect the conduct of authorized law enforcement or intel-
21 ligence activities; or

22 (3) to modify the authority of a department or agency of the Federal
23 Government to protect classified information and sources and methods
24 and the national security of the United States.

25 (d) RELATIONSHIP TO OTHER LAWS.—Nothing in this part shall be con-
26 strued to affect any requirement under any other provision of law for a non-
27 Federal entity to provide information to the Federal Government.

28 (e) PROHIBITED CONDUCT.—Nothing in this part shall be construed to
29 permit price-fixing, allocating a market between competitors, monopolizing
30 or attempting to monopolize a market, boycotting, or exchanging price or
31 cost information, customer lists, or information regarding future competitive
32 planning.

33 (f) INFORMATION SHARING RELATIONSHIPS.—Nothing in this part shall
34 be construed—

35 (1) to limit or modify an existing information sharing relationship;

36 (2) to prohibit a new information sharing relationship;

37 (3) to require a new information sharing relationship between any
38 non-Federal entity and a Federal entity or another non-Federal entity;
39 or

40 (4) to require the use of the capability and process in the Depart-
41 ment developed under section 10564(d) of this title.

1 (g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—

2 Nothing in this part shall be construed—

3 (1) to amend, repeal, or supersede any current or future contractual
4 agreement, terms of service agreement, or other contractual relation-
5 ship between non-Federal entities, or between a non-Federal entity and
6 a Federal entity; or

7 (2) to abrogate trade secret or intellectual property rights of a non-
8 Federal entity or Federal entity.

9 (h) ANTI-TASKING RESTRICTION.—Nothing in this part shall be con-
10 strued to permit a Federal entity—

11 (1) to require a non-Federal entity to provide information to a Fed-
12 eral entity or another non-Federal entity;

13 (2) to condition the sharing of cyber threat indicators with a non-
14 Federal entity on the entity's provision of cyber threat indicators to a
15 Federal entity or another non-Federal entity; or

16 (3) to condition the award of a Federal grant, contract, or purchase
17 on the provision of a cyber threat indicator to a Federal entity or an-
18 other non-Federal entity.

19 (i) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this part shall
20 be construed to subject any entity to liability for choosing not to engage
21 in the voluntary activities authorized in this part.

22 (j) USE AND RETENTION OF INFORMATION.—Nothing in this part shall
23 be construed to authorize, or to modify any existing authority of, a depart-
24 ment or agency of the Federal Government to retain or use any information
25 shared under this part for any use other than permitted in this part.

26 (k) FEDERAL PREEMPTION.—

27 (1) IN GENERAL.—This part supersedes any statute or other provi-
28 sion of law of a State or political subdivision of a State that restricts
29 or otherwise expressly regulates an activity authorized under this part.

30 (2) STATE LAW ENFORCEMENT.—Nothing in this part shall be con-
31 strued to supersede any statute or other provision of law of a State
32 or political subdivision of a State concerning the use of authorized law
33 enforcement practices and procedures.

34 (l) REGULATORY AUTHORITY.—Nothing in this part shall be construed—

35 (1) to authorize the prescribing of any regulations not specifically
36 authorized to be issued under this part;

37 (2) to establish or limit any regulatory authority not specifically es-
38 tablished or limited under this part; or

39 (3) to authorize regulatory actions that would duplicate or conflict
40 with regulatory requirements, mandatory standards, or related proce-
41 sses under another provision of Federal law.

1 (m) AUTHORITY OF SECRETARY OF DEFENSE TO RESPOND TO MALI-
 2 CIOUS CYBER ACTIVITY CARRIED OUT BY FOREIGN POWERS.—Nothing in
 3 this part shall be construed to limit the authority of the Secretary of De-
 4 fense under section 130g of title 10.

5 (n) DISCLOSURE IN CRIMINAL PROSECUTION.—Nothing in this part shall
 6 be construed to prevent the disclosure of a cyber threat indicator or defen-
 7 sive measure shared under this part in a criminal prosecution when an ap-
 8 plicable provision of Federal, State, tribal, or local law requires disclosure
 9 in the case.

10 **§ 10570. Effective period**

11 (a) IN GENERAL.—Except as provided in subsection (b), this part and
 12 the amendments made by the Cybersecurity Information Sharing Act of
 13 2015 (Public Law 114–113, div. N, title I, 129 Stat. 2936) are effective
 14 during the period ending on September 30, 2025.

15 (b) EXCEPTION.—With respect to any action authorized by this part or
 16 information obtained pursuant to an action authorized by this part that oc-
 17 curs before the date on which the provisions referred to in subsection (a)
 18 cease to have effect, the provisions of this part shall continue in effect.

19 **Part C—Federal Cybersecurity** 20 **Enhancement**

21 **§ 10581. Definitions**

22 In this part:

23 (1) AGENCY.—The term “agency” has the meaning given the term
 24 in section 3502 of title 44.

25 (2) AGENCY INFORMATION SYSTEM.—The term “agency information
 26 system” has the meaning given the term in section 10546 of this title.

27 (3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
 28 priate congressional committees” means—

29 (A) the Committee on Homeland Security and Governmental
 30 Affairs of the Senate; and

31 (B) the Committee on Homeland Security of the House of Rep-
 32 resentatives.

33 (4) CYBERSECURITY RISK.—The term “cybersecurity risk” has the
 34 meaning given the term in section 10545 of this title.

35 (5) DIRECTOR.—The term “Director” means the Director of the Of-
 36 fice of Management and Budget.

37 (6) INFORMATION SYSTEM.—The term “information system” has the
 38 meaning given the term in section 10545 of this title.

39 (7) INTELLIGENCE COMMUNITY.—The term “intelligence commu-
 40 nity” has the meaning given the term in section 3 of the National Se-
 41 curity Act of 1947 (50 U.S.C. 3003).

1 (8) NATIONAL SECURITY SYSTEM.—The term “national security sys-
2 tem” has the meaning given the term in section 11103 of title 40.

3 **§ 10582. Advanced internal defenses**

4 (a) ADVANCED NETWORK SECURITY TOOLS.—

5 (1) IN GENERAL.—The Secretary shall include, in the efforts of the
6 Department to continuously diagnose and mitigate cybersecurity risks,
7 advanced network security tools to improve visibility of network activ-
8 ity, including through the use of commercial and free or open source
9 tools, and to detect and mitigate intrusions and anomalous activity.

10 (2) DEVELOPMENT OF PLAN.—The Director shall develop, and the
11 Secretary shall implement, a plan to ensure that each agency utilizes
12 advanced network security tools, including those described in paragraph
13 (1), to detect and mitigate intrusions and anomalous activity.

14 (b) PRIORITIZING ADVANCED SECURITY TOOLS.—The Director and the
15 Secretary, in consultation with appropriate agencies, shall—

16 (1) review and update Government-wide policies and programs to en-
17 sure appropriate prioritization and use of network security monitoring
18 tools in agency networks; and

19 (2) brief appropriate congressional committees on the prioritization
20 and use.

21 (c) IMPROVED METRICS.—The Secretary, in collaboration with the Direc-
22 tor, shall review and update the metrics used to measure security under sec-
23 tion 3554 of title 44 to include measures of intrusion and incident detection
24 and response times.

25 (d) TRANSPARENCY AND ACCOUNTABILITY.—The Director, in consulta-
26 tion with the Secretary, shall increase transparency to the public on agency
27 cybersecurity posture, including by increasing the number of metrics avail-
28 able on Federal Government performance websites and, to the greatest ex-
29 tent practicable, displaying metrics for department components, small agen-
30 cies, and micro-agencies.

31 (e) EXCEPTION.—The requirements under this section shall not apply to
32 the Department of Defense, a national security system, or an element of
33 the intelligence community.

34 **§ 10583. Federal cybersecurity requirements**

35 (a) IMPLEMENTATION OF FEDERAL CYBERSECURITY STANDARDS.—Con-
36 sistent with section 3553 of title 44, the Secretary, in consultation with the
37 Director, shall exercise the authority to issue binding operational directives
38 to assist the Director in ensuring timely agency adoption of, and compliance
39 with, policies and standards promulgated under section 11331 of title 40
40 for securing agency information systems.

41 (b) CYBERSECURITY REQUIREMENTS AT AGENCIES.—

1 (1) IN GENERAL.—Consistent with policies, standards, guidelines,
2 and directives on information security under subchapter II of chapter
3 35 of title 44 and the standards and guidelines promulgated under sec-
4 tion 11331 of title 40 and except as provided in paragraph (2), not
5 later than December 18, 2016, the head of each agency shall—

6 (A) identify sensitive and mission critical data stored by the
7 agency consistent with the inventory required under the first sub-
8 section (e) (relating to the inventory of major information sys-
9 tems) and the second subsection (e) (relating to the inventory of
10 information systems) of section 3505 of title 44;

11 (B) assess access controls to the data described in subparagraph
12 (A), the need for readily accessible storage of the data, and indi-
13 viduals' need to access the data;

14 (C) encrypt or otherwise render indecipherable to unauthorized
15 users the data described in subparagraph (A) that is stored on or
16 transiting agency information systems;

17 (D) implement a single sign-on trusted identity platform for in-
18 dividuals accessing each public website of the agency that requires
19 user authentication, as developed by the Administrator of General
20 Services in collaboration with the Secretary; and

21 (E) implement identity management consistent with section 504
22 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7464),
23 including multi-factor authentication, for—

24 (i) remote access to an agency information system; and

25 (ii) each user account with elevated privileges on an agency
26 information system.

27 (2) EXCEPTION.—The requirements under paragraph (1) shall not
28 apply to an agency information system for which—

29 (A) the head of the agency has personally certified to the Direc-
30 tor with particularity that—

31 (i) operational requirements articulated in the certification
32 and related to the agency information system would make it
33 excessively burdensome to implement the cybersecurity re-
34 quirement;

35 (ii) the cybersecurity requirement is not necessary to secure
36 the agency information system or agency information stored
37 on or transiting it; and

38 (iii) the agency has taken all necessary steps to secure the
39 agency information system and agency information stored on
40 or transiting it; and

1 (B) the head of the agency or the designee of the head of the
 2 agency has submitted the certification described in subparagraph
 3 (A) to the appropriate congressional committees and the agency’s
 4 authorizing committees.

5 (3) CONSTRUCTION.—

6 (A) AUTHORITY OF OFFICIALS NOT ALTERED.—Nothing in this
 7 section shall be construed to alter the authority of the Secretary,
 8 the Director, or the Director of the National Institute of Stand-
 9 ards and Technology in implementing subchapter II of chapter 35
 10 of title 44.

11 (B) DEVELOPMENT OF TECHNOLOGY, STANDARDS, POLICIES,
 12 AND GUIDELINES NOT AFFECTED.—Nothing in this section shall
 13 be construed to affect the National Institute of Standards and
 14 Technology standards process or the requirement under section
 15 3553(a)(4) of title 44 or to discourage continued improvements
 16 and advancements in the technology, standards, policies, and
 17 guidelines used to promote Federal information security.

18 (c) EXCEPTION.—The requirements under this section do not apply to the
 19 Department of Defense, a national security system, or an element of the
 20 intelligence community.

21 **§ 10584. Assessment; reports**

22 (a) DEFINITIONS.—In this section:

23 (1) AGENCY INFORMATION.—The term “agency information” has the
 24 meaning given the term in section 10549 of this title.

25 (2) CYBER THREAT INDICATOR; DEFENSIVE MEASURE.—The terms
 26 “cyber threat indicator” and “defensive measure” have the meanings
 27 given the terms in section 10561 of this title.

28 (3) INTRUSION ASSESSMENTS.—The term “intrusion assessments”
 29 means actions taken under the intrusion assessment plan to identify
 30 and remove intruders in agency information systems.

31 (4) INTRUSION ASSESSMENT PLAN.—The term “intrusion assess-
 32 ment plan” means the plan required under section 10546(b) of this
 33 title.

34 (5) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—The
 35 term “intrusion detection and prevention capabilities” means the capa-
 36 bilities required under section 10549(b) of this title.

37 (b) THIRD-PARTY ASSESSMENT.—Not later than December 18, 2018, the
 38 Comptroller General shall conduct a study and publish a report on the effec-
 39 tiveness of the approach and strategy of the Federal Government to secur-
 40 ing agency information systems, including the intrusion detection and pre-
 41 vention capabilities and the intrusion assessment plan.

1 (c) REPORTS TO CONGRESS.—

2 (1) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—

3 (A) SECRETARY.—The Secretary not later than June 18 each
4 year shall submit to the appropriate congressional committees a
5 report on the status of the implementation of the intrusion detec-
6 tion and prevention capabilities, including—

7 (i) a description of privacy controls;

8 (ii) a description of the technologies and capabilities uti-
9 lized to detect cybersecurity risks in network traffic, including
10 the extent to which those technologies and capabilities include
11 existing commercial and noncommercial technologies;

12 (iii) a description of the technologies and capabilities uti-
13 lized to prevent network traffic associated with cybersecurity
14 risks from transiting or traveling to or from agency informa-
15 tion systems, including the extent to which those technologies
16 and capabilities include existing commercial and noncommer-
17 cial technologies;

18 (iv) a list of the types of indicators or other identifiers or
19 techniques used to detect cybersecurity risks in network traf-
20 fic transiting or traveling to or from agency information sys-
21 tems on each iteration of the intrusion detection and preven-
22 tion capabilities, and the number of each type of indicator,
23 identifier, and technique;

24 (v) the number of instances in which the intrusion detec-
25 tion and prevention capabilities detected a cybersecurity risk
26 in network traffic transiting or traveling to or from agency
27 information systems and the number of times the intrusion
28 detection and prevention capabilities blocked network traffic
29 associated with cybersecurity risk; and

30 (vi) a description of the pilot established under section
31 10549(e)(5) of this title, including the number of new tech-
32 nologies tested and the number of participating agencies.

33 (B) DIRECTOR.—Not later than June 18, 2017, and annually
34 thereafter, the Director shall submit to Congress, as part of the
35 report required under section 3553(c) of title 44, an analysis of
36 agency application of the intrusion detection and prevention capa-
37 bilities, including—

38 (i) a list of each agency and the degree to which each agen-
39 cy has applied the intrusion detection and prevention capabili-
40 ties to an agency information system; and

41 (ii) a list by agency of—

1 (I) the number of instances in which the intrusion de-
2 tection and prevention capabilities detected a cybersecu-
3 rity risk in network traffic transiting or traveling to or
4 from an agency information system and the types of in-
5 dicators, identifiers, and techniques used to detect the
6 cybersecurity risks; and

7 (II) the number of instances in which the intrusion de-
8 tection and prevention capabilities prevented network
9 traffic associated with a cybersecurity risk from
10 transiting or traveling to or from an agency information
11 system and the types of indicators, identifiers, and tech-
12 niques used to detect the agency information systems.

13 (C) CHIEF INFORMATION OFFICER.—Not earlier than June 18,
14 2017, and not later than December 18, 2017, the Federal Chief
15 Information Officer shall review and submit to the appropriate
16 congressional committees a report assessing the intrusion detection
17 and intrusion prevention capabilities, including—

18 (i) the effectiveness of the system in detecting, disrupting,
19 and preventing cyber-threat actors, including advanced per-
20 sistent threats, from accessing agency information and agency
21 information systems;

22 (ii) whether the intrusion detection and prevention capabili-
23 ties, continuous diagnostics and mitigation, and other systems
24 deployed under subtitle C of title II of the Homeland Security
25 Act of 2002 (Public Law 107–296, 116 Stat. 2155) are effec-
26 tive in securing Federal information systems;

27 (iii) the costs and benefits of the intrusion detection and
28 prevention capabilities, including as compared to commercial
29 technologies and tools and including the value of classified
30 cyber threat indicators; and

31 (iv) the capability of agencies to protect sensitive cyber
32 threat indicators and defensive measures if they were shared
33 through unclassified mechanisms for use in commercial tech-
34 nologies and tools.

35 (2) DEVELOPMENT AND IMPLEMENTATION OF INTRUSION ASSESS-
36 MENT PLAN, ADVANCED INTERNAL DEFENSES, AND FEDERAL CYBER-
37 SECURITY REQUIREMENTS.—The Director—

38 (A) 30 days after any update to the intrusion assessment plan,
39 shall submit the intrusion assessment plan to the appropriate con-
40 gressional committees;

1 (B) not later than December 18, 2016, and annually thereafter,
 2 shall submit to Congress, as part of the report required under sec-
 3 tion 3553(c) of title 44—

4 (i) a description of the implementation of the intrusion as-
 5 sessment plan;

6 (ii) the findings of the intrusion assessments conducted
 7 pursuant to the intrusion assessment plan;

8 (iii) a description of the advanced network security tools in-
 9 cluded in the efforts to continuously diagnose and mitigate
 10 cybersecurity risks pursuant to section 10582(a)(1) of this
 11 title; and

12 (iv) a list by agency of compliance with the requirements
 13 of section 10583(b) of this title; and

14 (C) not later than December 18, 2016, submit to the appro-
 15 priate congressional committees—

16 (i) a copy of the plan developed pursuant to section
 17 10582(a)(2) of this title; and

18 (ii) the improved metrics developed pursuant to section
 19 10582(e) of this title.

20 (3) TERMINATION.—The requirements under this subsection termi-
 21 nate on December 18, 2022.

22 (d) FORM.—Each report required under this section shall be submitted
 23 in unclassified form, but may include a classified annex.

24 **Part D—Other Cyber Matters**

25 **§ 10591. Apprehension and prosecution of international** 26 **cyber criminals**

27 (a) DEFINITION OF INTERNATIONAL CYBER CRIMINAL.—In this section,
 28 the term “international cyber criminal” means an individual—

29 (1) who is believed to have committed a cybercrime or intellectual
 30 property crime against the interests of the United States or the citizens
 31 of the United States; and

32 (2) for whom—

33 (A) an arrest warrant has been issued by a judge in the United
 34 States; or

35 (B) an international wanted notice (commonly referred to as a
 36 “Red Notice”) has been circulated by Interpol.

37 (b) CONSULTATIONS FOR NONCOOPERATION.—The Secretary of State
 38 shall consult with the appropriate government official of each country from
 39 which extradition is not likely due to the lack of an extradition treaty with
 40 the United States or other reasons, in which 1 or more international cyber

1 criminals are physically present, to determine what actions the government
2 of the country has taken—

3 (1) to apprehend and prosecute the criminals; and

4 (2) to prevent the criminals from carrying out cybercrimes or intel-
5 lectual property crimes against the interests of the United States or its
6 citizens.

7 (c) ANNUAL REPORT.—

8 (1) DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEES.—

9 For purposes of this subsection, the term “appropriate congressional
10 committees” means—

11 (A) the Committee on Foreign Relations, the Committee on Ap-
12 propriations, the Committee on Homeland Security and Govern-
13 mental Affairs, the Committee on Banking, Housing, and Urban
14 Affairs, the Select Committee on Intelligence, and the Committee
15 on the Judiciary of the Senate; and

16 (B) the Committee on Foreign Affairs, the Committee on Ap-
17 propriations, the Committee on Homeland Security, the Com-
18 mittee on Financial Services, the Permanent Select Committee on
19 Intelligence, and the Committee on the Judiciary of the House of
20 Representatives.

21 (2) CONTENTS.—The Secretary of State shall submit to the appro-
22 priate congressional committees an annual report that includes—

23 (A) the number of international cyber criminals located in other
24 countries, disaggregated by country, and indicating from which
25 countries extradition is not likely due to the lack of an extradition
26 treaty with the United States or other reasons;

27 (B) the nature and number of significant discussions by an offi-
28 cial of the Department of State on ways to thwart or prosecute
29 international cyber criminals with an official of another country,
30 including the name of each country; and

31 (C) for each international cyber criminal who was extradited to
32 the United States during the most recently completed calendar
33 year—

34 (i) his or her name;

35 (ii) the crimes for which he or she was charged;

36 (iii) his or her previous country of residence; and

37 (iv) the country from which he or she was extradited to the
38 United States.

39 (3) FORM.—The report shall be in unclassified form to the maximum
40 extent possible, but may include a classified annex.

1 **§ 10592. Enhancement of emergency services**

2 (a) COLLECTION OF DATA.—The Secretary, acting through the National
3 Cybersecurity and Communications Integration Center, in coordination with
4 appropriate Federal entities and the Director for Emergency Communica-
5 tions, shall establish a process by which a Statewide Interoperability Coordi-
6 nator may report data on any cybersecurity risk or incident involving any
7 information system or network used by emergency response providers in
8 that State.

9 (b) ANALYSIS OF DATA.—Not later than December 18, 2016, the Sec-
10 retary, acting through the Director of the National Cybersecurity and Com-
11 munications Integration Center, in coordination with appropriate entities
12 and the Director for Emergency Communications, and in consultation with
13 the Secretary of Commerce, acting through the Director of the National In-
14 stitute of Standards and Technology, shall conduct integration and analysis
15 of the data reported under subsection (a) to develop information and rec-
16 ommendations on security and resilience measures for any information sys-
17 tem or network used by State emergency response providers.

18 (c) BEST PRACTICES.—

19 (1) IN GENERAL.—Using the results of the integration and analysis
20 conducted under subsection (b), and any other relevant information,
21 the Director of the National Institute of Standards and Technology
22 shall, on an ongoing basis, facilitate and support the development of
23 methods for reducing cybersecurity risks to emergency response pro-
24 viders using the process described in section 2(e) of the National Insti-
25 tute of Standards and Technology Act (15 U.S.C. 272(e)).

26 (2) REPORT.—The Director of the National Institute of Standards
27 and Technology shall submit to Congress a report on the result of the
28 activities of the Director under paragraph (1), including any methods
29 developed by the Director under paragraph (1), and shall make the re-
30 port publicly available on the website of the National Institute of
31 Standards and Technology.

32 (d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed
33 to—

34 (1) require a State to report data under subsection (a); or

35 (2) require a non-Federal entity (as defined in section 10561 of this
36 title) to—

37 (A) adopt a recommended measure developed under subsection
38 (b); or

39 (B) follow the result of the activities carried out under sub-
40 section (c), including any methods developed under subsection (c).

1 **§ 10593. Improving cybersecurity in the health care industry**

2 (a) DEFINITIONS.—In this section:

3 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
4 priate congressional committees” means—

5 (A) the Committee on Health, Education, Labor, and Pensions,
6 the Committee on Homeland Security and Governmental Affairs,
7 and the Select Committee on Intelligence of the Senate; and

8 (B) the Committee on Energy and Commerce, the Committee
9 on Homeland Security, and the Permanent Select Committee on
10 Intelligence of the House of Representatives.

11 (2) BUSINESS ASSOCIATE.—The term “business associate” has the
12 meaning given the term in section 160.103 of title 45, Code of Federal
13 Regulations (as in effect on December 17, 2015).

14 (3) COVERED ENTITY.—The term “covered entity” has the meaning
15 given the term in section 160.103 of title 45, Code of Federal Regula-
16 tions (as in effect on December 17, 2015).

17 (4) CYBERSECURITY THREAT; CYBER THREAT INDICATOR; DEFEN-
18 SIVE MEASURE; FEDERAL ENTITY.—The terms “cybersecurity threat”,
19 “cyber threat indicator”, “defensive measure”, and “Federal entity”
20 have the meanings given the terms in section 10561 of this title.

21 (5) HEALTH CARE CLEARINGHOUSE; HEALTH CARE PROVIDER;
22 HEALTH PLAN.—The terms “health care clearinghouse”, “health care
23 provider”, and “health plan” have the meanings given the terms in sec-
24 tion 160.103 of title 45, Code of Federal Regulations (as in effect on
25 December 17, 2015).

26 (6) HEALTH CARE INDUSTRY STAKEHOLDER.—The term “health
27 care industry stakeholder” means any—

28 (A) health plan, health care clearinghouse, or health care pro-
29 vider;

30 (B) advocate for patients or consumers;

31 (C) pharmacist;

32 (D) developer or vendor of health information technology;

33 (E) laboratory;

34 (F) pharmaceutical or medical device manufacturer; or

35 (G) additional stakeholder the Secretary determines necessary
36 for purposes of subsection (b)(1), (c)(1), (c)(3), or (d)(1).

37 (7) NON-FEDERAL ENTITY; PRIVATE ENTITY.—The terms “non-Fed-
38 eral entity” and “private entity” have the meanings given the terms
39 in section 10561 of this title.

40 (b) REPORT.—

1 (1) IN GENERAL.—Not later than December 18, 2016, the Secretary
2 of Health and Human Services shall submit to the Committee on
3 Health, Education, Labor, and Pensions of the Senate and the Com-
4 mittee on Energy and Commerce of the House of Representatives a re-
5 port on the preparedness of the Department of Health and Human
6 Services and health care industry stakeholders in responding to cyber-
7 security threats.

8 (2) CONTENTS OF REPORT.—With respect to the internal response
9 of the Department of Health and Human Services to emerging cyberse-
10 curity threats, the report under paragraph (1) shall include—

11 (A) a clear statement of the official in the Department of
12 Health and Human Services to be responsible for leading and co-
13 ordinating efforts of the Department of Health and Human Serv-
14 ices regarding cybersecurity threats in the health care industry;
15 and

16 (B) a plan from each relevant operating division and subdivision
17 of the Department of Health and Human Services on how the di-
18 vision or subdivision will address cybersecurity threats in the
19 health care industry, including a clear delineation of how each the
20 division or subdivision will divide responsibility among the per-
21 sonnel of the division or subdivision and communicate with other
22 divisions and subdivisions regarding efforts to address the threats.

23 (c) HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE.—

24 (1) IN GENERAL.—The Secretary of Health and Human Services, in
25 consultation with the Director of the National Institute of Standards
26 and Technology and the Secretary of Homeland Security, shall convene
27 health care industry stakeholders, cybersecurity experts, and any Fed-
28 eral agencies or entities the Secretary of Health and Human Services
29 determines appropriate to establish a task force to—

30 (A) analyze how industries, other than the health care industry,
31 have implemented strategies and safeguards for addressing cyber-
32 security threats in their respective industries;

33 (B) analyze challenges and barriers private entities (excluding
34 any State, tribal, or local government) in the health care industry
35 face securing themselves against cyberattacks;

36 (C) review challenges that covered entities and business associ-
37 ates face in securing networked medical devices and other software
38 or systems that connect to an electronic health record;

39 (D) provide the Secretary of Health and Human Services with
40 information to disseminate to health care industry stakeholders of

1 all sizes for purposes of improving their preparedness for, and re-
2 sponse to, cybersecurity threats affecting the health care industry;

3 (E) establish a plan for implementing part B of this subchapter,
4 so that the Federal Government and health care industry stake-
5 holders may in real time, share actionable cyber threat indicators
6 and defensive measures; and

7 (F) report to the appropriate congressional committees on the
8 findings and recommendations of the task force regarding carrying
9 out subparagraphs (A) through (E).

10 (2) TERMINATION.—The task force established under this subsection
11 shall terminate 1 year after the date on which the task force is estab-
12 lished.

13 (3) DISSEMINATION.—Not later than 60 days after the termination
14 of the task force established under this subsection, the Secretary of
15 Health and Human Services shall disseminate the information de-
16 scribed in paragraph (1)(D) to health care industry stakeholders in ac-
17 cordance with paragraph (1)(D).

18 (d) ALIGNING HEALTH CARE INDUSTRY SECURITY APPROACHES.—

19 (1) IN GENERAL.—The Secretary of Health and Human Services
20 shall establish, through a collaborative process with the Secretary of
21 Homeland Security, health care industry stakeholders, the Director of
22 the National Institute of Standards and Technology, and any Federal
23 entity or non-Federal entity the Secretary of Health and Human Ser-
24 vices determines appropriate, a common set of voluntary, consensus-
25 based, and industry-led guidelines, best practices, methodologies, proce-
26 dures, and processes that—

27 (A) serve as a resource for cost-effectively reducing cybersecu-
28 rity risks for a range of health care organizations;

29 (B) support voluntary adoption and implementation efforts to
30 improve safeguards to address cybersecurity threats;

31 (C) are consistent with—

32 (i) the standards, guidelines, best practices, methodologies,
33 procedures, and processes developed under section 2(e)(15) of
34 the National Institute of Standards and Technology Act (15
35 U.S.C. 272(e)(15));

36 (ii) the security and privacy regulations promulgated under
37 section 264(e) of the Health Insurance Portability and Ac-
38 countability Act of 1996 (42 U.S.C. 1320d–2 note); and

39 (iii) the provisions of the Health Information Technology
40 for Economic and Clinical Health Act (Public Law 111–5,

1 div. A, title XIII, div. B, title IV, 123 Stat. 226, 467), and
 2 the amendments made by the Act; and

3 (D) are updated on a regular basis and applicable to a range
 4 of health care organizations.

5 (2) LIMITATION.—Nothing in this subsection shall be interpreted as
 6 granting the Secretary of Health and Human Services authority to—

7 (A) provide for audits to ensure that health care organizations
 8 are in compliance with this subsection; or

9 (B) mandate, direct, or condition the award of any Federal
 10 grant, contract, or purchase, on compliance with this subsection.

11 (3) NO LIABILITY FOR NONPARTICIPATION.—Nothing in this section
 12 shall be construed to subject a health care industry stakeholder to li-
 13 ability for choosing not to engage in the voluntary activities authorized,
 14 or guidelines developed, under this subsection.

15 (e) INCORPORATING ONGOING ACTIVITIES.—In carrying out the activities
 16 under this section, the Secretary of Health and Human Services may incor-
 17 porate activities that are ongoing as of December 17, 2015, and that are
 18 consistent with the objectives of this section.

19 (f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed
 20 to limit the antitrust exemption under section 10563(e) of this title or the
 21 protection from liability under section 10565 of this title.

22 **Subchapter IV—Supporting Anti-Terrorism** 23 **by Fostering Effective Technologies**

24 **§ 10621. 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-

nership, individual aggregation of individuals, or another legal entity that provides commercial property and casualty insurance, including an affiliate of a commercial insurance carrier.

(3) LIABILITY INSURANCE.—The term “liability insurance” means insurance for legal liabilities incurred by the insured resulting from—

(A) loss of, or damage to, property of others;

(B) ensuing loss of income or extra expense incurred because of loss of, or damage to, property of others;

(C) bodily injury, including to persons other than the insured or its employees; or

(D) loss resulting from debt or default of another.

(4) LOSS.—The term “loss” means death, bodily injury, or loss of, or damage to, property, including business interruption loss.

(5) NON-FEDERAL GOVERNMENT CUSTOMERS.—The term “non-Federal Government customers” means a customer of a Seller that is not an agency or instrumentality of the United States Government with authority under Public Law 85–804 (50 U.S.C. 1431 et seq.) to provide for indemnification under certain circumstances for third-party claims against its contractors, including State and local authorities and commercial entities.

(6) QUALIFIED ANTI-TERRORISM TECHNOLOGY.—The term “qualified anti-terrorism technology” means a product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm the acts might otherwise cause, that is designated as such by the Secretary.

(7) SELLER.—The term “Seller” means a person or entity that sells or otherwise provides a qualified anti-terrorism technology to Federal and non-Federal Government customers.

§ 10622. Administration

(a) IN GENERAL.—The Secretary is responsible for the administration of this subchapter.

(b) DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES.—The Secretary may designate anti-terrorism technologies that qualify for protection under the system of risk management set forth in this subchapter in accordance with criteria that shall include the following:

(1) Prior United States Government use or demonstrated substantial utility and effectiveness.

(2) Availability of the technology for immediate deployment in public 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 (c) 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 **§ 10623. 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) of this subsection, have
28 been deployed in defense against, in response to, or in recovery from
29 the act, and the claims result, or may result, in loss to the Seller, there
30 shall be a rebuttable presumption that the government contractor’s de-
31 fense applies in the lawsuit. This presumption shall only be overcome
32 by evidence showing that the Seller acted fraudulently or with willful
33 misconduct in submitting information to the Secretary during the
34 course of the Secretary’s consideration of the technology under this
35 subsection. This presumption of the government contractor’s defense
36 shall apply regardless of whether the claim against the Seller arises
37 from a sale of the product to Federal Government or non-Federal Gov-
38 ernment customers.

39 (2) EXCLUSIVE RESPONSIBILITY.—The Secretary is exclusively re-
40 sponsible for the review and approval of anti-terrorism technology for
41 purposes of establishing a government contractor’s defense in any prod-

1 uct liability lawsuit for claims arising out of, relating to, or resulting
 2 from, an act of terrorism when qualified anti-terrorism technologies ap-
 3 proved by the Secretary, as provided in this paragraph and paragraph
 4 (3), have been deployed in defense against, in response to, or in recov-
 5 ery from the act, and the claims result, or may result, in loss to the
 6 Seller. Upon the Seller's submission to the Secretary for approval of
 7 anti-terrorism technology, the Secretary shall conduct a comprehensive
 8 review of the design of the technology and determine whether it will
 9 perform as intended, conforms to the Seller's specifications, and is safe
 10 for use as intended. The Seller shall conduct safety and hazard anal-
 11 yses on the technology and shall supply the Secretary with all such in-
 12 formation relating to the analyses.

13 (3) CERTIFICATE.—For anti-terrorism technology reviewed and ap-
 14 proved by the Secretary, the Secretary shall issue a certificate of con-
 15 formance to the Seller and place the anti-terrorism technology on an
 16 Approved Product List for Homeland Security.

17 (e) EXCLUSION.—Nothing in this section shall in any way limit the ability
 18 of any person to seek any form of recovery from any person, government,
 19 or other entity that—

20 (1) attempts to commit, knowingly participates in, aids and abets,
 21 or commits any act of terrorism, or any criminal act related to or re-
 22 sulting from the act of terrorism; or

23 (2) participates in a conspiracy to commit an act of terrorism or a
 24 criminal act.

25 § 10624. Risk management

26 (a) IN GENERAL.—

27 (1) LIABILITY INSURANCE REQUIRED.—The Seller shall obtain liabil-
 28 ity insurance of the types and in the amounts as required under this
 29 section and certified by the Secretary to satisfy otherwise compensable
 30 third-party claims arising out of, relating to, or resulting from, an act
 31 of terrorism when qualified anti-terrorism technologies have been de-
 32 ployed in defense against, in response to, or in recovery from the act.

33 (2) MAXIMUM AMOUNT.—For the total claims related to one act of
 34 terrorism, the Seller is not required to obtain liability insurance of
 35 more than the maximum amount of liability insurance reasonably avail-
 36 able from private sources on the world market at prices and terms that
 37 will not unreasonably distort the sales price of Seller's anti-terrorism
 38 technologies.

39 (3) SCOPE OF COVERAGE.—Liability insurance obtained under this
 40 subsection shall, in addition to the Seller, protect the following, to the
 41 extent of their potential liability for involvement in the manufacture,

1 qualification, sale, use, or operation of qualified anti-terrorism tech-
 2 nologies deployed in defense against, in response to, or in recovery from
 3 an act of terrorism:

4 (A) Contractors, subcontractors, suppliers, vendors and cus-
 5 tomers of the Seller.

6 (B) Contractors, subcontractors, suppliers, and vendors of the
 7 customer.

8 (4) THIRD PARTY CLAIMS.—The liability insurance under this sec-
 9 tion shall provide coverage against third party claims arising out of,
 10 relating to, or resulting from the sale or use of anti-terrorism tech-
 11 nologies.

12 (b) RECIPROCAL WAIVER OF CLAIMS.—The Seller shall enter into a re-
 13 ciprocal waiver of claims with its contractors, subcontractors, suppliers, ven-
 14 dors and customers, and contractors and subcontractors of the customers,
 15 involved in the manufacture, sale, use, or operation of qualified anti-ter-
 16 rorism technologies, under which each party to the waiver agrees to be re-
 17 sponsible for losses, including business interruption losses, that it sustains,
 18 or for losses sustained by its own employees resulting from an activity re-
 19 sulting from an act of terrorism when qualified anti-terrorism technologies
 20 have been deployed in defense against, in response to, or in recovery from
 21 the act.

22 (c) EXTENT OF LIABILITY.—Notwithstanding any other provision of law,
 23 liability for all claims against a Seller arising out of, relating to, or resulting
 24 from, an act of terrorism when qualified anti-terrorism technologies have
 25 been deployed in defense against, in response to, or in recovery from the
 26 act, and the claims result, or may result, in loss to the Seller, whether for
 27 compensatory or punitive damages or for contribution or indemnity, shall
 28 not be in an amount greater than the limits of liability insurance coverage
 29 required to be maintained by the Seller under this section.

30 **Subchapter V—Secure Handling of** 31 **Ammonium Nitrate**

32 **§ 10631. Definitions**

33 In this subchapter:

34 (1) AMMONIUM NITRATE.—The term “ammonium nitrate” means—

35 (A) solid ammonium nitrate that is chiefly the ammonium salt
 36 of nitric acid and contains not less than 33 percent nitrogen by
 37 weight; and

38 (B) a mixture containing a percentage of ammonium nitrate
 39 that is equal to or greater than the percentage determined by the
 40 Secretary under section 10632(b) of this title.

1 (2) AMMONIUM NITRATE FACILITY.—The term “ammonium nitrate
2 facility” means an entity that produces, sells or otherwise transfers
3 ownership of, or provides application services for, ammonium nitrate.

4 (3) AMMONIUM NITRATE PURCHASER.—The term “ammonium ni-
5 trate purchaser” means a person who purchases ammonium nitrate
6 from an ammonium nitrate facility.

7 **§ 10632. Regulation of the sale and transfer of ammonium**
8 **nitrate**

9 (a) IN GENERAL.—The Secretary shall regulate the sale and transfer of
10 ammonium nitrate by an ammonium nitrate facility in accordance with this
11 subchapter to prevent the misappropriation or use of ammonium nitrate in
12 an act of terrorism.

13 (b) AMMONIUM NITRATE MIXTURES.—The Secretary, in consultation
14 with the heads of appropriate Federal departments and agencies (including
15 the Secretary of Agriculture), shall, after notice and an opportunity for
16 comment, establish a threshold percentage for ammonium nitrate in a sub-
17 stance.

18 (c) REGISTRATION OF OWNERS OF AMMONIUM NITRATE FACILITIES.—

19 (1) PROCESS.—The Secretary shall establish a process by which a
20 person that—

21 (A) owns an ammonium nitrate facility is required to register
22 with the Department; and

23 (B) registers under subparagraph (A) is issued a registration
24 number for purposes of this subchapter.

25 (2) INFORMATION.—A person applying to register under paragraph
26 (1) shall submit to the Secretary—

27 (A) the name, address, and telephone number of each ammo-
28 nium nitrate facility owned by that person;

29 (B) the name of the person designated by that person as the
30 point of contact for each facility, for purposes of this subchapter;
31 and

32 (C) other information the Secretary determines is appropriate.

33 (d) REGISTRATION OF AMMONIUM NITRATE PURCHASERS.—

34 (1) PROCESS.—The Secretary shall establish a process by which a
35 person that—

36 (A) intends to be an ammonium nitrate purchaser is required
37 to register with the Department; and

38 (B) registers under subparagraph (A) is issued a registration
39 number for purposes of this subchapter.

40 (2) INFORMATION.—A person applying to register under paragraph
41 (1) as an ammonium nitrate purchaser shall submit to the Secretary—

1 (A) the name, address, and telephone number of the applicant;
2 and

3 (B) the intended use of ammonium nitrate to be purchased by
4 the applicant.

5 (e) RECORDS.—

6 (1) MAINTENANCE OF RECORDS.—The owner of an ammonium ni-
7 trate facility shall—

8 (A) maintain a record of each sale or transfer of ammonium ni-
9 trate, during the 2-year period beginning on the date of that sale
10 or transfer; and

11 (B) include in the record the information described in para-
12 graph (2).

13 (2) SPECIFIC INFORMATION REQUIRED.—For each sale or transfer
14 of ammonium nitrate, the owner of an ammonium nitrate facility
15 shall—

16 (A) record the name, address, telephone number, and registra-
17 tion number issued under subsection (c) or (d) of each person that
18 purchases ammonium nitrate, in a manner prescribed by the Sec-
19 retary;

20 (B) if applicable, record the name, address, and telephone num-
21 ber of an agent acting on behalf of the person described in sub-
22 paragraph (A), at the point of sale;

23 (C) record the date and quantity of ammonium nitrate sold or
24 transferred; and

25 (D) verify the identity of the persons described in subpara-
26 graphs (A) and (B), as applicable, in accordance with a procedure
27 established by the Secretary.

28 (3) PROTECTION OF INFORMATION.—In maintaining records under
29 paragraph (1), the owner of an ammonium nitrate facility shall take
30 reasonable actions to ensure the protection of the information included
31 in the records.

32 (f) EXEMPTION FOR EXPLOSIVE PURPOSES.—The Secretary may exempt
33 from this subchapter a person producing, selling, or purchasing ammonium
34 nitrate exclusively for use in the production of an explosive under a license
35 or permit issued under chapter 40 of title 18.

36 (g) CONSULTATION.—In carrying out this section, the Secretary shall
37 consult with the Secretary of Agriculture, States, and appropriate private-
38 sector entities, to ensure that the access of agricultural producers to ammo-
39 nium nitrate is not unduly burdened.

40 (h) DATA CONFIDENTIALITY.—

1 (1) IN GENERAL.—Notwithstanding section 552 of title 5 or the
2 USA PATRIOT Act (Public Law 107–56, 115 Stat. 272), and except
3 as provided in paragraph (2), the Secretary may not disclose to any
4 person any information obtained under this subchapter.

5 (2) EXCEPTION.—The Secretary may disclose information obtained
6 by the Secretary under this subchapter to—

7 (A) an officer or employee of the United States, or a person
8 that has entered into a contract with the United States, who has
9 a need to know the information to perform the duties of the offi-
10 cer, employee, or person; or

11 (B) to a State agency under section 10634 of this title, under
12 appropriate arrangements to ensure the protection of the informa-
13 tion.

14 (i) REGISTRATION PROCEDURES AND CHECK OF TERRORIST SCREENING
15 DATABASE.—

16 (1) REGISTRATION PROCEDURES.—

17 (A) IN GENERAL.—The Secretary shall establish procedures to
18 efficiently receive applications for registration numbers under this
19 subchapter, conduct the checks required under paragraph (2), and
20 promptly issue or deny a registration number.

21 (B) INITIAL 6-MONTH REGISTRATION PERIOD.—The Secretary
22 shall take steps to maximize the number of registration applica-
23 tions that are submitted and processed during the 6-month period
24 described in section 10636(e) of this title.

25 (2) CHECK OF TERRORIST SCREENING DATABASE.—

26 (A) CHECK REQUIRED.—The Secretary shall conduct a check of
27 appropriate identifying information of a person seeking to register
28 with the Department under subsection (c) or (d) against identi-
29 fying information that appears in the terrorist screening database
30 of the Department.

31 (B) AUTHORITY TO DENY REGISTRATION NUMBER.—If the
32 identifying information of a person seeking to register with the
33 Department under subsection (c) or (d) appears in the terrorist
34 screening database of the Department, the Secretary may deny
35 issuance of a registration number under this subchapter.

36 (3) EXPEDITED REVIEW OF APPLICATIONS.—

37 (A) IN GENERAL.—Following the 6-month period described in
38 section 10636(e) of this title, the Secretary shall, to the extent
39 practicable, issue or deny registration numbers under this sub-
40 chapter not later than 72 hours after the time the Secretary re-
41 ceives a complete registration application, unless the Secretary de-

1 termines, in the interest of national security, that additional time
2 is necessary to review an application.

3 (B) NOTICE OF APPLICATION STATUS.—In all cases, the Sec-
4 retary shall notify a person seeking to register with the Depart-
5 ment under subsection (c) or (d) of the status of the application
6 of that person not later than 72 hours after the time the Secretary
7 receives a complete registration application.

8 (4) EXPEDITED APPEALS PROCESS.—

9 (A) REQUIREMENT.—

10 (i) ESTABLISHMENT.—The Secretary shall establish an ex-
11 pedited appeals process for persons denied a registration
12 number under this subchapter.

13 (ii) TIME FOR RESOLVING APPEALS.—The Secretary shall,
14 to the extent practicable, resolve appeals not later than 72
15 hours after receiving a complete request for appeal unless the
16 Secretary determines, in the interest of national security, that
17 additional time is necessary to resolve an appeal.

18 (B) CONSULTATION.—The Secretary, in developing the appeals
19 process under subparagraph (A), shall consult with appropriate
20 stakeholders.

21 (C) GUIDANCE.—The Secretary shall provide guidance regard-
22 ing the procedures and information required for an appeal under
23 subparagraph (A) to any person denied a registration number
24 under this subchapter.

25 (5) RESTRICTIONS ON USE AND MAINTENANCE OF INFORMATION.—

26 (A) IN GENERAL.—Information constituting grounds for denial
27 of a registration number under this section shall be maintained
28 confidentially by the Secretary and may be used only for making
29 determinations under this section.

30 (B) SHARING OF INFORMATION.—Notwithstanding any other
31 provision of this subchapter, the Secretary may share information
32 with Federal, State, local, and tribal law enforcement agencies, as
33 appropriate.

34 (6) REGISTRATION INFORMATION.—

35 (A) AUTHORITY TO REQUIRE INFORMATION.—The Secretary
36 may require a person applying for a registration number under
37 this subchapter to submit information necessary to carry out the
38 requirements of this section.

39 (B) REQUIREMENT TO UPDATE INFORMATION.—The Secretary
40 may require persons issued a registration under this subchapter to

1 update registration information submitted to the Secretary under
2 this subchapter, as appropriate.

3 (7) RECHECKS AGAINST TERRORIST SCREENING DATABASE.—

4 (A) IN GENERAL.—The Secretary shall, as appropriate, recheck
5 persons provided a registration number pursuant to this sub-
6 chapter against the terrorist screening database of the Depart-
7 ment, and may revoke the registration number if the Secretary de-
8 termines the person may pose a threat to national security.

9 (B) NOTICE OF REVOCATION.—The Secretary shall, as appro-
10 priate, provide prior notice to a person whose registration number
11 is revoked under this section, and the person shall have an oppor-
12 tunity to appeal, as provided in paragraph (4).

13 **§ 10633. Inspection and auditing of records**

14 The Secretary shall establish a process for the periodic inspection and au-
15 diting of the records maintained by owners of ammonium nitrate facilities
16 for the purpose of monitoring compliance with this subchapter or for the
17 purpose of deterring or preventing the misappropriation or use of ammo-
18 nium nitrate in an act of terrorism.

19 **§ 10634. Administrative provisions**

20 (a) COOPERATIVE AGREEMENTS.—The Secretary—

21 (1) may enter into a cooperative agreement with the Secretary of Ag-
22 riculture, or the head of any State department of agriculture or its des-
23 ignee involved in agricultural regulation, in consultation with the State
24 agency responsible for homeland security, to carry out the provisions
25 of this subchapter; and

26 (2) wherever possible, shall seek to cooperate with State agencies or
27 their designees that oversee ammonium nitrate facility operations when
28 seeking cooperative agreements to implement the registration and en-
29 forcement provisions of this subchapter.

30 (b) DELEGATION.—

31 (1) AUTHORITY.—The Secretary may delegate to a State the author-
32 ity to assist the Secretary in the administration and enforcement of
33 this subchapter.

34 (2) DELEGATION REQUIRED.—At the request of a Governor of a
35 State, the Secretary shall delegate to that State the authority to carry
36 out functions under sections 10632 and 10633 of this title, if the Sec-
37 retary determines that the State is capable of satisfactorily carrying
38 out the functions.

39 (3) FUNDING.—Subject to the availability of appropriations, if the
40 Secretary delegates functions to a State under this subsection, the Sec-

1 retary shall provide to that State sufficient funds to carry out the dele-
2 gated functions.

3 (c) PROVISION OF GUIDANCE AND NOTIFICATION MATERIALS TO AMMO-
4 NIUM NITRATE FACILITIES.—

5 (1) GUIDANCE.—The Secretary shall make available to each owner
6 of an ammonium nitrate facility registered under section 10632(c) of
7 this title guidance on—

8 (A) the identification of suspicious ammonium nitrate purchases
9 or transfers or attempted purchases or transfers;

10 (B) the appropriate course of action to be taken by the ammo-
11 nium nitrate facility owner with respect to such a purchase or
12 transfer or attempted purchase or transfer, including—

13 (i) exercising the right of the owner of the ammonium ni-
14 trate facility to decline sale of ammonium nitrate; and

15 (ii) notifying appropriate law enforcement entities; and

16 (C) additional subjects determined appropriate to prevent the
17 misappropriation or use of ammonium nitrate in an act of ter-
18 rorism.

19 (2) USE OF MATERIALS AND PROGRAMS.—In providing guidance
20 under this subsection, the Secretary shall, to the extent practicable, le-
21 verage relevant materials and programs.

22 (3) NOTIFICATION MATERIALS.—

23 (A) IN GENERAL.—The Secretary shall make available materials
24 suitable for posting at locations where ammonium nitrate is sold.

25 (B) DESIGN.—Materials made available under subparagraph
26 (A) shall be designed to notify prospective ammonium nitrate pur-
27 chasers of—

28 (i) the record-keeping requirements under section 10632 of
29 this title; and

30 (ii) the penalties for violating the requirements.

31 **§ 10635. Theft reporting requirement**

32 A person who is required to comply with section 10632(e) of this title
33 who has knowledge of the theft or unexplained loss of ammonium nitrate
34 shall report the theft or loss to the appropriate Federal law enforcement au-
35 thorities not later than 1 calendar day after the date on which the person
36 becomes aware of the theft or loss. On receipt of the report, the relevant
37 Federal authorities shall inform State, local, and tribal law enforcement en-
38 tities, as appropriate.

39 **§ 10636. Prohibitions and penalty**

40 (a) PROHIBITIONS.—

1 (1) TAKING POSSESSION.—A person may not purchase ammonium
2 nitrate from an ammonium nitrate facility unless the person is reg-
3 istered under subsection (c) or (d) of section 10632 of this title, or is
4 an agent of a person registered under subsection (c) or (d) of section
5 10632.

6 (2) TRANSFERRING POSSESSION.—An owner of an ammonium ni-
7 trate facility shall not transfer possession of ammonium nitrate from
8 the ammonium nitrate facility to an ammonium nitrate purchaser who
9 is not registered under subsection (c) or (d) of section 10632 of this
10 title, or to an agent acting on behalf of an ammonium nitrate pur-
11 chaser when the purchaser is not registered under subsection (c) or (d)
12 of section 10632.

13 (3) OTHER PROHIBITIONS.—A person may not—

14 (A) purchase ammonium nitrate without a registration number
15 required under subsection (c) or (d) of section 10632 of this title;

16 (B) own or operate an ammonium nitrate facility without a reg-
17 istration number required under section 10632(c) of this title; or

18 (C) fail to comply with a requirement or violate another prohibi-
19 tion under this subchapter.

20 (b) CIVIL PENALTY.—A person that violates this subchapter may be as-
21 sessed a civil penalty by the Secretary of not more than \$50,000 per viola-
22 tion.

23 (c) PENALTY CONSIDERATIONS.—In determining the amount of a civil
24 penalty under this section, the Secretary shall consider—

25 (1) the nature and circumstances of the violation;

26 (2) with respect to the person who commits the violation, any history
27 of prior violations, the ability to pay the penalty, and any effect the
28 penalty is likely to have on the ability of the person to do business;
29 and

30 (3) any other matter that the Secretary determines that justice re-
31 quires.

32 (d) NOTICE AND OPPORTUNITY FOR A HEARING.—A civil penalty may
33 not be assessed under this subchapter unless the person liable for the pen-
34 alty has been given notice and an opportunity for a hearing on the violation
35 for which the penalty is to be assessed in the county, parish, or incorporated
36 city of residence of that person.

37 (e) DELAY IN APPLICATION OF PROHIBITION.—Paragraphs (1) and (2)
38 of subsection (a) shall apply on and after the date that is 6 months after
39 the date that the Secretary issues a final rule implementing this subchapter.

1 **§ 10637. Protection from civil liability**

2 (a) IN GENERAL.—An owner of an ammonium nitrate facility that in
3 good faith refuses to sell or transfer ammonium nitrate to a person, or that
4 in good faith discloses to the Department or to appropriate law enforcement
5 authorities an actual or attempted purchase or transfer of ammonium ni-
6 trate, based upon a reasonable belief that the person seeking purchase or
7 transfer of ammonium nitrate may use the ammonium nitrate to create an
8 explosive device to be employed in an act of terrorism (as defined in section
9 3077 of title 18), or to use ammonium nitrate for any other unlawful pur-
10 pose, shall not be liable in any civil action relating to that refusal to sell
11 ammonium nitrate or that disclosure.

12 (b) REASONABLE BELIEF.—A reasonable belief that a person may use
13 ammonium nitrate to create an explosive device to be employed in an act
14 of terrorism under subsection (a) may not solely be based on the race, sex,
15 national origin, creed, religion, status as a veteran, or status as a member
16 of the armed forces of the United States of that person.

17 **§ 10638. Preemption of other laws**

18 (a) OTHER FEDERAL REGULATIONS.—Except as provided in section
19 10637 of this title, nothing in this subchapter affects a regulation issued
20 by an agency other than an agency of the Department.

21 (b) STATE LAW.—Subject to section 10637 of this title, this subchapter
22 preempts the laws of a State to the extent that the laws are inconsistent
23 with this subchapter, except that this subchapter shall not preempt any
24 State law that provides additional protection against the acquisition of am-
25 monium nitrate by terrorists or the use of ammonium nitrate in explosives
26 in acts of terrorism or for other illicit purposes, as determined by the Sec-
27 retary.

28 **Subchapter VI—Chemical Facilities**

29 **§ 10651. Definitions**

30 In this subchapter:

31 (1) CFATS REGULATION.—The term “CFATS regulation” means—

32 (A) an existing CFATS regulation; and

33 (B) any regulation or amendment to an existing CFATS regula-
34 tion issued pursuant to the authority under section 10657 of this
35 title.

36 (2) CHEMICAL FACILITY OF INTEREST.—The term “chemical facility
37 of interest” means a facility that—

38 (A) holds, or that the Secretary has a reasonable basis to be-
39 lieve holds, a chemical of interest, as designated under Appendix
40 A to part 27 of title 6, Code of Federal Regulations, or any sue-

1 cessor to the Appendix, at a threshold quantity set pursuant to
2 relevant risk-related security principles; and

3 (B) is not an excluded facility.

4 (3) COVERED CHEMICAL FACILITY.—The term “covered chemical fa-
5 cility” means a facility that—

6 (A) the Secretary—

7 (i) identifies as a chemical facility of interest; and

8 (ii) based on review of the facility’s Top-Screen, determines
9 meets the risk criteria developed under section
10 10652(f)(2)(B) of this title; and

11 (B) is not an excluded facility.

12 (4) EXCLUDED FACILITY.—The term “excluded facility” means—

13 (A) a facility regulated under the Maritime Transportation Se-
14 curity Act of 2002 (Public Law 107–295; 116 Stat. 2064);

15 (B) a public water system, as that term is defined in section
16 1401 of the Public Health Service Act (42 U.S.C. 300f);

17 (C) a treatment works, as that term is defined in section 212
18 of the Federal Water Pollution Control Act (33 U.S.C. 1292);

19 (D) a facility owned or operated by the Department of Defense
20 or the Department of Energy; or

21 (E) a facility subject to regulation by the Nuclear Regulatory
22 Commission, or by a State that has entered into an agreement
23 with the Nuclear Regulatory Commission under section 274(b) of
24 the Atomic Energy Act of 1954 (42 U.S.C. 2021(b)) to protect
25 against unauthorized access of any material, activity, or structure
26 licensed by the Nuclear Regulatory Commission.

27 (5) EXISTING CFATS REGULATION.—The term “existing CFATS reg-
28 ulation” means—

29 (A) a regulation promulgated under section 550 of the Depart-
30 ment of Homeland Security Appropriations Act, 2007 (Public Law
31 109–295), that was in effect on December 17, 2014; and

32 (B) a Federal Register notice or other published guidance relat-
33 ing to section 550 of the Department of Homeland Security Ap-
34 propriations Act, 2007 (Public Law 109–295), that was in effect
35 on December 17, 2014.

36 (6) EXPEDITED APPROVAL FACILITY.—The term “expedited approval
37 facility” means a covered chemical facility for which the owner or oper-
38 ator elects to submit a site security plan in accordance with section
39 10652(d)(4) of this title.

40 (7) FACIALLY DEFICIENT.—The term “facially deficient”, relating to
41 a site security plan, means a site security plan that does not support

1 a certification that the security measures in the plan address the secu-
 2 rity vulnerability assessment and the risk-based performance standards
 3 for security for a facility, based on a review of—

- 4 (A) the facility’s site security plan;
- 5 (B) the facility’s Top-Screen;
- 6 (C) the facility’s security vulnerability assessment; or
- 7 (D) any other information that—
 - 8 (i) the facility submits to the Department; or
 - 9 (ii) the Department obtains from a public source or other
 - 10 source.

11 (8) GUIDANCE FOR EXPEDITED APPROVAL FACILITIES.—The term
 12 “guidance for expedited approval facilities” means the guidance issued
 13 under section 10652(d)(4)(B)(i) of this title.

14 (9) RISK ASSESSMENT.—The term “risk assessment” means the Sec-
 15 retary’s application of relevant risk criteria identified in section
 16 10652(f)(2)(B) of this title.

17 (10) TERRORIST SCREENING DATABASE.—The term “terrorist
 18 screening database” means the terrorist screening database maintained
 19 by the Federal Government Terrorist Screening Center or its successor.

20 (11) TIER.—The term “tier” has the meaning given the term in sec-
 21 tion 27.105 of title 6, Code of Federal Regulations, or any successor
 22 to section 27.105.

23 (12) TIERING; TIERING METHODOLOGY.—The terms “tiering” and
 24 “tiering methodology” mean the procedure by which the Secretary as-
 25 signs a tier to each covered chemical facility based on the risk assess-
 26 ment for that covered chemical facility.

27 (13) TOP-SCREEN.—The term “Top-Screen” has the meaning given
 28 the term in section 27.105 of title 6, Code of Federal Regulations, or
 29 any successor to section 27.105.

30 (14) VULNERABILITY ASSESSMENT.—The term “vulnerability assess-
 31 ment” means the identification of weaknesses in the security of a
 32 chemical facility of interest.

33 **§ 10652. Chemical Facility Anti-Terrorism Standards Pro-**
 34 **gram**

35 (a) ESTABLISHMENT.—There is in the Department a Chemical Facility
 36 Anti-Terrorism Standards Program.

37 (b) DUTIES OF SECRETARY.—In carrying out the Chemical Facility Anti-
 38 Terrorism Standards Program, the Secretary shall—

- 39 (1) identify—
 - 40 (A) chemical facilities of interest; and
 - 41 (B) covered chemical facilities;

1 (2) require each chemical facility of interest to submit a Top-Screen
2 and any other information the Secretary determines necessary to enable
3 the Department to assess the security risks associated with the facility;

4 (3) establish risk-based performance standards designed to address
5 high levels of security risk at covered chemical facilities; and

6 (4) require each covered chemical facility to—

7 (A) submit a security vulnerability assessment; and

8 (B) develop, submit, and implement a site security plan.

9 (c) SECURITY MEASURES.—

10 (1) IN GENERAL.—A facility, in developing a site security plan as
11 required under subsection (b), shall include security measures that, in
12 combination, appropriately address the security vulnerability assess-
13 ment and the risk-based performance standards for security for the fa-
14 cility.

15 (2) EMPLOYEE INPUT.—To the greatest extent practicable, a facili-
16 ty's security vulnerability assessment and site security plan shall in-
17 clude input from at least 1 facility employee and, where applicable, 1
18 employee representative from the bargaining agent at that facility, each
19 of whom possesses, in the determination of the facility's security offi-
20 cer, relevant knowledge, experience, training, or education as pertains
21 to matters of site security.

22 (d) APPROVAL OR DISAPPROVAL OF SITE SECURITY PLANS.—

23 (1) IN GENERAL.—

24 (A) REVIEW.—Except as provided in paragraph (4), the Sec-
25 retary shall review and approve or disapprove each site security
26 plan submitted pursuant to subsection (b).

27 (B) BASES FOR DISAPPROVAL.—The Secretary—

28 (i) may not disapprove a site security plan based on the
29 presence or absence of a particular security measure; and

30 (ii) shall disapprove a site security plan if the plan fails to
31 satisfy the risk-based performance standards established pur-
32 suant to subsection (b)(3).

33 (2) ALTERNATIVE SECURITY PROGRAMS.—

34 (A) AUTHORITY TO APPROVE.—

35 (i) IN GENERAL.—The Secretary may approve an alter-
36 native security program established by a private-sector entity
37 or a Federal, State, or local authority or under other applica-
38 ble laws if the Secretary determines that the requirements of
39 the program meet the requirements under this section.

40 (ii) ADDITIONAL SECURITY MEASURES.—If the require-
41 ments of an alternative security program do not meet the re-

1 requirements under this section, the Secretary may recommend
2 additional security measures to the program that will enable
3 the Secretary to approve the program.

4 (B) SATISFACTION OF SITE SECURITY PLAN REQUIREMENT.—

5 A covered chemical facility may satisfy the site security plan re-
6 quirement under subsection (b)(4) by adopting an alternative secu-
7 rity program that the Secretary has—

8 (i) reviewed and approved under subparagraph (A); and

9 (ii) determined to be appropriate for the operations and se-
10 curity concerns of the covered chemical facility.

11 (3) SITE SECURITY PLAN ASSESSMENTS.—

12 (A) RISK ASSESSMENT POLICIES AND PROCEDURES.—In ap-
13 proving or disapproving a site security plan under this subsection,
14 the Secretary shall employ the risk assessment policies and proce-
15 dures developed under this subchapter.

16 (B) PREVIOUSLY APPROVED PLANS.—In the case of a covered
17 chemical facility for which the Secretary approved a site security
18 plan before December 18, 2014, the Secretary may not require the
19 facility to resubmit the site security plan solely by reason of the
20 enactment of this subchapter.

21 (4) EXPEDITED APPROVAL PROGRAM.—

22 (A) IN GENERAL.—A covered chemical facility assigned to tier
23 3 or 4 may meet the requirement to develop and submit a site se-
24 curity plan under subsection (b)(4) by developing and submitting
25 to the Secretary—

26 (i) a site security plan and the certification described in
27 subparagraph (C); or

28 (ii) a site security plan in conformance with a template au-
29 thorized under subparagraph (H).

30 (B) GUIDANCE FOR EXPEDITED APPROVAL FACILITIES.—

31 (i) IN GENERAL.—The Secretary shall issue guidance for
32 expedited approval facilities that identifies specific security
33 measures that are sufficient to meet the risk-based perform-
34 ance standards.

35 (ii) MATERIAL DEVIATION FROM GUIDANCE.—If a security
36 measure in the site security plan of an expedited approval fa-
37 cility materially deviates from a security measure in the guid-
38 ance for expedited approval facilities, the site security plan
39 shall include an explanation of how the security measure
40 meets the risk-based performance standards.

1 (iii) APPLICABILITY OF OTHER LAWS TO DEVELOPMENT
2 AND ISSUANCE OF INITIAL GUIDANCE.—In developing and
3 issuing, or amending, the guidance for expedited approval fa-
4 cilities under this subparagraph and in collecting information
5 from expedited approval facilities, the Secretary shall not be
6 subject to—

7 (I) section 553 of title 5;

8 (II) subchapter I of chapter 35 of title 44; or

9 (III) section 10657(b) of this title.

10 (C) CERTIFICATION.—The owner or operator of an expedited
11 approval facility shall submit to the Secretary a certification,
12 signed under penalty of perjury, that—

13 (i) the owner or operator is familiar with the requirements
14 of this subchapter and part 27 of title 6, Code of Federal
15 Regulations, or any successor to this subchapter or part 27,
16 and the site security plan being submitted;

17 (ii) the site security plan includes the security measures re-
18 quired by subsection (c);

19 (iii)(I) the security measures in the site security plan do
20 not materially deviate from the guidance for expedited ap-
21 proval facilities except where indicated in the site security
22 plan;

23 (II) any deviations from the guidance for expedited ap-
24 proval facilities in the site security plan meet the risk-based
25 performance standards for the tier to which the facility is as-
26 signed; and

27 (III) the owner or operator has provided an explanation of
28 how the site security plan meets the risk-based performance
29 standards for any material deviation;

30 (iv) the owner or operator has visited, examined, docu-
31 mented, and verified that the expedited approval facility
32 meets the criteria set forth in the site security plan;

33 (v) the expedited approval facility has implemented all of
34 the required performance measures outlined in the site secu-
35 rity plan or set out planned measures that will be imple-
36 mented within a reasonable time period stated in the site se-
37 curity plan;

38 (vi) each individual responsible for implementing the site
39 security plan has been made aware of the requirements rel-
40 evant to the individual's responsibility contained in the site

1 security plan and has demonstrated competency to carry out
2 those requirements;

3 (vii) the owner or operator has committed, or, in the case
4 of planned measures, will commit, the necessary resources to
5 fully implement the site security plan; and

6 (viii) the planned measures include an adequate procedure
7 for addressing events beyond the control of the owner or oper-
8 ator in implementing any planned measures.

9 (D) DEADLINE.—

10 (i) DATE FOR SUBMISSION TO SECRETARY.—The owner or
11 operator of an expedited approval facility shall submit to the
12 Secretary the site security plan and the certification described
13 in subparagraph (C) not later than 120 days after—

14 (I) for an expedited approval facility that was assigned
15 to tier 3 or 4 under existing CFATS regulations before
16 December 18, 2014, the date that is 210 days after De-
17 cember 18, 2014; and

18 (II) for any expedited approval facility not described
19 in subclause (I), the later of—

20 (aa) the date on which the expedited approval fa-
21 cility is assigned to tier 3 or 4 under subsection
22 (e)(2)(A); or

23 (bb) the date that is 210 days after December 18,
24 2014.

25 (ii) NOTICE.—An owner or operator of an expedited ap-
26 proval facility shall notify the Secretary of the intent of the
27 owner or operator to certify the site security plan for the ex-
28 pedited approval facility not later than 30 days before the
29 date on which the owner or operator submits the site security
30 plan and certification described in subparagraph (C).

31 (E) COMPLIANCE.—

32 (i) IN GENERAL.—For an expedited approval facility sub-
33 mitting a site security plan and certification in accordance
34 with subparagraphs (A), (B), (C), and (D)—

35 (I) the expedited approval facility shall comply with all
36 of the requirements of its site security plan; and

37 (II) the Secretary—

38 (aa) except as provided in subparagraph (G), may
39 not disapprove the site security plan; and

1 (bb) may audit and inspect the expedited ap-
2 proval facility under subsection (e) to verify compli-
3 ance with its site security plan.

4 (ii) NONCOMPLIANCE.—If the Secretary determines an ex-
5 pedited approval facility is not in compliance with the require-
6 ments of the site security plan or is otherwise in violation of
7 this subchapter, the Secretary may enforce compliance in ac-
8 cordance with section 10654 of this title.

9 (F) AMENDMENTS TO SITE SECURITY PLAN.—

10 (i) REQUIREMENT.—

11 (I) IN GENERAL.—If the owner or operator of an ex-
12 pedited approval facility amends a site security plan sub-
13 mitted under subparagraph (A), the owner or operator
14 shall submit the amended site security plan and a certifi-
15 cation relating to the amended site security plan that
16 contains the information described in subparagraph (C).

17 (II) TECHNICAL AMENDMENTS.—For purposes of this
18 clause, an amendment to a site security plan includes
19 any technical amendment to the site security plan.

20 (ii) WHEN AMENDMENT REQUIRED.—The owner or oper-
21 ator of an expedited approval facility shall amend the site se-
22 curity plan if—

23 (I) there is a change in the design, construction, oper-
24 ation, or maintenance of the expedited approval facility
25 that affects the site security plan;

26 (II) the Secretary requires additional security meas-
27 ures or suspends a certification and recommends addi-
28 tional security measures under subparagraph (G); or

29 (III) the owner or operator receives notice from the
30 Secretary of a change in tiering under subsection (f)(3).

31 (iii) DEADLINE.—An amended site security plan and cer-
32 tification shall be submitted under clause (i)—

33 (I) in the case of a change in design, construction, op-
34 eration, or maintenance of the expedited approval facility
35 that affects the security plan, not later than 120 days
36 after the date on which the change in design, construc-
37 tion, operation, or maintenance occurred;

38 (II) in the case of the Secretary requiring additional
39 security measures or suspending a certification and rec-
40 ommending additional security measures under subpara-
41 graph (G), not later than 120 days after the date on

1 which the owner or operator receives notice of the re-
2 quirement for additional security measures or suspension
3 of the certification and recommendation of additional se-
4 curity measures; and

5 (III) in the case of a change in tiering, not later than
6 120 days after the date on which the owner or operator
7 receives notice under subsection (f)(3).

8 (G) FACIALLY DEFICIENT SITE SECURITY PLANS.—

9 (i) PROHIBITION.—Notwithstanding subparagraph (A) or
10 (E), the Secretary may suspend the authority of a covered
11 chemical facility to certify a site security plan if the Sec-
12 retary—

13 (I) determines the certified site security plan or an
14 amended site security plan is facially deficient; and

15 (II) not later than 100 days after the date on which
16 the Secretary receives the site security plan and certifi-
17 cation, provides the covered chemical facility with written
18 notification that the site security plan is facially defi-
19 cient, including a clear explanation of each deficiency in
20 the site security plan.

21 (ii) ADDITIONAL SECURITY MEASURES.—

22 (I) IN GENERAL.—If, during or after a compliance in-
23 spection of an expedited approval facility, the Secretary
24 determines that planned or implemented security meas-
25 ures in the site security plan of the facility are insuffi-
26 cient to meet the risk-based performance standards
27 based on misrepresentation, omission, or an inadequate
28 description of the site, the Secretary may—

29 (aa) require additional security measures; or

30 (bb) suspend the certification of the facility.

31 (II) RECOMMENDATION OF ADDITIONAL SECURITY
32 MEASURES.—If the Secretary suspends the certification
33 of an expedited approval facility under subclause (I), the
34 Secretary shall—

35 (aa) recommend specific additional security meas-
36 ures that, if made part of the site security plan by
37 the facility, would enable the Secretary to approve
38 the site security plan; and

39 (bb) provide the facility an opportunity to submit
40 a new or modified site security plan and certifi-
41 cation under subparagraph (A).

1 (III) SUBMISSION; REVIEW.—If an expedited approval
2 facility determines to submit a new or modified site secu-
3 rity plan and certification as authorized under subclause
4 (II)(bb)—

5 (aa) not later than 90 days after the date on
6 which the facility receives recommendations under
7 subclause (II)(aa), the facility shall submit the new
8 or modified plan and certification; and

9 (bb) not later than 45 days after the date on
10 which the Secretary receives the new or modified
11 plan under item (aa), the Secretary shall review the
12 plan and determine whether the plan is facially defi-
13 cient.

14 (IV) DETERMINATION NOT TO INCLUDE ADDITIONAL
15 SECURITY MEASURES.—

16 (aa) REVOCATION OF CERTIFICATION.—If an ex-
17 pedited approval facility does not agree to include in
18 its site security plan specific additional security
19 measures recommended by the Secretary under sub-
20 clause (II)(aa), or does not submit a new or modi-
21 fied site security plan in accordance with subclause
22 (III), the Secretary may revoke the certification of
23 the facility by issuing an order under section
24 10654(a)(1)(B) of this title.

25 (bb) EFFECT OF REVOCATION.—If the Secretary
26 revokes the certification of an expedited approval fa-
27 cility under item (aa) by issuing an order under sec-
28 tion 10654(a)(1)(B) of this title—

29 (AA) the order shall require the owner or op-
30 erator of the facility to submit a site security
31 plan or alternative security program for review
32 by the Secretary under subsection (d)(1) or
33 (2); and

34 (BB) the facility shall no longer be eligible
35 to certify a site security plan under this para-
36 graph.

37 (V) FACIAL DEFICIENCY.—If the Secretary determines
38 that a new or modified site security plan submitted by
39 an expedited approval facility under subclause (III) is
40 facially deficient—

1 (aa) not later than 120 days after the date of the
 2 determination, the owner or operator of the facility
 3 shall submit a site security plan or alternative secu-
 4 rity program for review by the Secretary under sub-
 5 section (d)(1) or (2); and

6 (bb) the facility shall no longer be eligible to cer-
 7 tify a site security plan under this paragraph.

8 (H) TEMPLATES.—

9 (i) IN GENERAL.—The Secretary may develop prescriptive
 10 site security plan templates with specific security measures to
 11 meet the risk-based performance standards under subsection
 12 (b)(3) for adoption and certification by a covered chemical fa-
 13 cility assigned to tier 3 or 4 in lieu of developing and certi-
 14 fying its own plan.

15 (ii) APPLICABILITY OF OTHER LAWS TO DEVELOPING AND
 16 ISSUING INITIAL SITE SECURITY PLAN TEMPLATES AND RE-
 17 LATED GUIDANCE AND TO COLLECTING INFORMATION.—Dur-
 18 ing the period before the Secretary has met the deadline
 19 under subparagraph (B)(i), in developing and issuing, or
 20 amending, the site security plan templates under this sub-
 21 paragraph, in issuing guidance for implementation of the
 22 templates, and in collecting information from expedited ap-
 23 proval facilities, the Secretary shall not be subject to—

24 (I) section 553 of title 5;

25 (II) subchapter I of chapter 35 of title 44; or

26 (III) section 10657(b) of this title.

27 (iii) RULE OF CONSTRUCTION.—Nothing in this subpara-
 28 graph shall be construed to prevent a covered chemical facil-
 29 ity from developing and certifying its own security plan in ac-
 30 cordance with subparagraph (A).

31 (I) EVALUATION.—

32 (i) IN GENERAL.—The Secretary shall take any appropriate
 33 action necessary for a full evaluation of the expedited ap-
 34 proval program authorized under this paragraph, including
 35 conducting an appropriate number of inspections, as author-
 36 ized under subsection (e), of expedited approval facilities.

37 (ii) REPORT.—The Secretary shall submit to the Com-
 38 mittee on Homeland Security and Governmental Affairs of
 39 the Senate and the Committee on Homeland Security and the
 40 Committee on Energy and Commerce of the House of Rep-
 41 resentatives a report that contains—

1 (I)(aa) the number of eligible facilities using the expedited approval program authorized under this paragraph;
 2 and
 3

4 (bb) the number of facilities that are eligible for the expedited approval program but are using the standard process for developing and submitting a site security plan under subsection (b)(4);
 5
 6
 7

8 (II) any costs and efficiencies associated with the expedited approval program;
 9

10 (III) the impact of the expedited approval program on the backlog for site security plan approval and authorization inspections;
 11
 12

13 (IV) an assessment of the ability of expedited approval facilities to submit facially sufficient site security plans;
 14

15 (V) an assessment of any impact of the expedited approval program on the security of chemical facilities; and
 16

17 (VI) a recommendation by the Secretary on the frequency of compliance inspections that may be required for expedited approval facilities.
 18
 19

20 (e) COMPLIANCE.—

21 (1) AUDITS AND INSPECTIONS.—

22 (A) DEFINITIONS.—In this paragraph:

23 (i) NONDEPARTMENTAL.—The term “nondepartmental”—

24 (I) with respect to personnel, means personnel that is not employed by the Department; and
 25

26 (II) with respect to an entity, means an entity that is not a component or other authority of the Department.
 27

28 (ii) NONGOVERNMENTAL.—The term “nongovernmental”—

29 (I) with respect to personnel, means personnel that is not employed by the Federal Government; and
 30

31 (II) with respect to an entity, means an entity that is not an agency, department, or other authority of the Federal Government.
 32
 33

34 (B) AUTHORITY TO CONDUCT AUDITS AND INSPECTIONS.—The Secretary shall conduct audits or inspections under this subchapter using—
 35
 36

37 (i) employees of the Department;

38 (ii) nondepartmental or nongovernmental personnel approved by the Secretary; or
 39

40 (iii) a combination of individuals described in clauses (i) and (ii).
 41

1 (C) SUPPORT PERSONNEL.—The Secretary may use nongovern-
2 mental personnel to provide administrative and logistical services
3 in support of audits and inspections under this subchapter.

4 (D) REPORTING STRUCTURE.—

5 (i) NONDEPARTMENTAL AND NONGOVERNMENTAL AUDITS
6 AND INSPECTIONS.—Any audit or inspection conducted by an
7 individual employed by a nondepartmental or nongovern-
8 mental entity shall be assigned in coordination with a regional
9 supervisor with responsibility for supervising inspectors in the
10 Infrastructure Security Compliance Division of the Depart-
11 ment for the region in which the audit or inspection is to be
12 conducted.

13 (ii) REQUIREMENT TO REPORT.—While an individual em-
14 ployed by a nondepartmental or nongovernmental entity is in
15 the field conducting an audit or inspection under this sub-
16 section, the individual shall report to the regional supervisor
17 with responsibility for supervising inspectors in the Infra-
18 structure Security Compliance Division of the Department for
19 the region in which the individual is operating.

20 (iii) APPROVAL.—The authority to approve a site security
21 plan under subsection (d) or determine if a covered chemical
22 facility is in compliance with an approved site security plan
23 shall be exercised solely by the Secretary or a designee of the
24 Secretary in the Department.

25 (E) STANDARDS FOR AUDITORS AND INSPECTORS.—The Sec-
26 retary shall prescribe standards for the training and retraining of
27 each individual used by the Department as an auditor or inspec-
28 tor, including each individual employed by the Department and all
29 nondepartmental or nongovernmental personnel, including—

30 (i) minimum training requirements for new auditors and
31 inspectors;

32 (ii) retraining requirements;

33 (iii) minimum education and experience levels;

34 (iv) the submission of information as required by the Sec-
35 retary to enable determination of whether the auditor or in-
36 spector has a conflict of interest;

37 (v) the proper certification necessary to handle chemical-
38 terrorism vulnerability information (as defined in section
39 27.105 of title 6, Code of Federal Regulations, or any suc-
40 cessor to section 27.105);

1 (vi) the reporting of any issue of non-compliance with this
2 section to the Secretary within 24 hours; and

3 (vii) any additional qualifications for fitness of duty as the
4 Secretary may require.

5 (F) CONDITIONS FOR NONGOVERNMENTAL AUDITORS AND IN-
6 SPECTORS.—If the Secretary arranges for an audit or inspection
7 under subparagraph (B) to be carried out by a nongovernmental
8 entity, the Secretary shall—

9 (i) prescribe standards for the qualification of the individ-
10 uals who carry out the audits and inspections that are com-
11 mensurate with the standards for similar Government audi-
12 tors or inspectors; and

13 (ii) ensure that any duties carried out by a nongovern-
14 mental entity are not inherently governmental functions.

15 (2) PERSONNEL SURETY PROGRAM.—

16 (A) ESTABLISHMENT.—For purposes of this subchapter, the
17 Secretary shall establish and carry out a Personnel Surety Pro-
18 gram that—

19 (i) does not require an owner or operator of a covered
20 chemical facility that voluntarily participates in the program
21 to submit information about an individual more than 1 time;

22 (ii) provides a participating owner or operator of a covered
23 chemical facility with relevant information about an individual
24 based on vetting the individual against the terrorist screening
25 database, to the extent that the feedback is necessary for the
26 facility to be in compliance with regulations promulgated
27 under this subchapter; and

28 (iii) provides redress to an individual—

29 (I) whose information was vetted against the terrorist
30 screening database under the program; and

31 (II) who believes that the personally identifiable infor-
32 mation submitted to the Department for vetting by a
33 covered chemical facility, or its designated representa-
34 tive, was inaccurate.

35 (B) IMPLEMENTATION.—To the extent that a risk-based per-
36 formance standard established under subsection (b) requires iden-
37 tifying individuals with ties to terrorism—

38 (i) a covered chemical facility—

39 (I) may satisfy its obligation under the standard by
40 using any Federal screening program that periodically
41 vets individuals against the terrorist screening database,

1 or any successor program, including the Personnel Sur-
 2 ety Program established under subparagraph (A); and

3 (II) shall—

4 (aa) accept a credential from a Federal screening
 5 program described in subclause (I) if an individual
 6 who is required to be screened presents the creden-
 7 tial; and

8 (bb) address in its site security plan or alter-
 9 native security program the measures it will take to
 10 verify that a credential or documentation from a
 11 Federal screening program described in subclause
 12 (I) is current;

13 (ii) visual inspection shall be sufficient to meet the require-
 14 ment under clause (i)(II)(bb), but the facility should consider
 15 other means of verification, consistent with the facility's as-
 16 sessment of the threat posed by acceptance of the credentials;
 17 and

18 (iii) the Secretary may not require a covered chemical facil-
 19 ity to submit any information about an individual unless the
 20 individual—

21 (I) is to be vetted under the Personnel Surety Pro-
 22 gram; or

23 (II) has been identified as presenting a terrorism secu-
 24 rity risk.

25 (C) RIGHTS UNAFFECTED.—Nothing in this section shall super-
 26 sede the ability—

27 (i) of a facility to maintain its own policies regarding the
 28 access of individuals to restricted areas or critical assets; or

29 (ii) of an employing facility and a bargaining agent, where
 30 applicable, to negotiate as to how the results of a background
 31 check may be used by the facility with respect to employment
 32 status.

33 (3) AVAILABILITY OF INFORMATION.—The Secretary shall share
 34 with the owner or operator of a covered chemical facility any informa-
 35 tion that the owner or operator needs to comply with this section.

36 (f) RESPONSIBILITIES OF THE SECRETARY.—

37 (1) IDENTIFICATION OF CHEMICAL FACILITIES OF INTEREST.—In
 38 carrying out this subchapter, the Secretary shall consult with the heads
 39 of other Federal agencies, States and political subdivisions thereof, rel-
 40 evant business associations, and public and private labor organizations
 41 to identify all chemical facilities of interest.

1 (2) RISK ASSESSMENT.—

2 (A) IN GENERAL.—For purposes of this subchapter, the Sec-
 3 retary shall develop a security risk assessment approach and cor-
 4 responding tiering methodology for covered chemical facilities that
 5 incorporates the relevant elements of risk, including threat, vulner-
 6 ability, and consequence.

7 (B) CRITERIA FOR DETERMINING SECURITY RISK.—The criteria
 8 for determining the security risk of terrorism associated with a
 9 covered chemical facility shall take into account—

10 (i) relevant threat information;

11 (ii) potential severe economic consequences and the poten-
 12 tial loss of human life in the event of the facility being subject
 13 to attack, compromise, infiltration, or exploitation by terror-
 14 ists; and

15 (iii) vulnerability of the facility to attack, compromise, infil-
 16 tration, or exploitation by terrorists.

17 (3) CHANGES IN TIERING.—

18 (A) MAINTENANCE OF RECORDS.—The Secretary shall docu-
 19 ment the basis for each instance in which—

20 (i) tiering for a covered chemical facility is changed; or

21 (ii) a covered chemical facility is determined to no longer
 22 be subject to the requirements under this subchapter.

23 (B) REQUIRED INFORMATION.—The records maintained under
 24 subparagraph (A) shall include information on whether and how
 25 the Secretary confirmed the information that was the basis for the
 26 change or determination described in subparagraph (A).

27 (4) SEMIANNUAL PERFORMANCE REPORTING.—Not later than 6
 28 months after December 18, 2014, and not less frequently than once
 29 every 6 months after that date, the Secretary shall submit to the Com-
 30 mittee on Homeland Security and Governmental Affairs of the Senate
 31 and the Committee on Homeland Security and the Committee on En-
 32 ergy and Commerce of the House of Representatives a report that in-
 33 cludes, for the period covered by the report—

34 (A) the number of covered chemical facilities in the United
 35 States;

36 (B) information—

37 (i) describing—

38 (I) the number of instances in which the Secretary—

39 (aa) placed a covered chemical facility in a lower
 40 risk tier; or

1 (bb) determined that a facility that had pre-
 2 viously met the criteria for a covered chemical facil-
 3 ity under section 10651(3) of this title no longer
 4 met the criteria; and

5 (II) the basis, in summary form, for each action or de-
 6 termination under subclause (I); and

7 (ii) that is provided in a sufficiently anonymized form to
 8 ensure that the information does not identify any specific fa-
 9 cility or company as the source of the information when
 10 viewed alone or in combination with other public information;

11 (C) the average number of days spent reviewing site security or
 12 an alternative security program for a covered chemical facility
 13 prior to approval;

14 (D) the number of covered chemical facilities inspected;

15 (E) the average number of covered chemical facilities inspected
 16 per inspector; and

17 (F) any other information that the Secretary determines will be
 18 helpful to Congress in evaluating the performance of the Chemical
 19 Facility Anti-Terrorism Standards Program.

20 **§ 10653. Protection and sharing of information**

21 (a) IN GENERAL.—Information developed under this subchapter, includ-
 22 ing vulnerability assessments, site security plans, and other security related
 23 information, records, and documents shall be given protections from public
 24 disclosure consistent with the protection of similar information under sec-
 25 tion 70103(d) of title 46.

26 (b) SHARING OF INFORMATION WITH STATES AND LOCAL GOVERN-
 27 MENTS.—Nothing in this section shall be construed to prohibit the sharing
 28 of information developed under this subchapter, as the Secretary determines
 29 appropriate, with State and local government officials possessing a need to
 30 know and the necessary security clearances, including law enforcement offi-
 31 cials and first responders, for the purpose of carrying out this subchapter,
 32 provided that the information may not be disclosed pursuant to any State
 33 or local law.

34 (c) SHARING OF INFORMATION WITH FIRST RESPONDERS.—

35 (1) REQUIREMENT.—The Secretary shall provide to State, local, and
 36 regional fusion centers (as that term is defined in section 10512(a)(1)
 37 of this title) and State and local government officials, as the Secretary
 38 determines appropriate, such information as is necessary to help ensure
 39 that first responders are properly prepared and provided with the situa-
 40 tional awareness needed to respond to security incidents at covered
 41 chemical facilities.

1 (2) DISSEMINATION.—The Secretary shall disseminate information
2 under paragraph (1) through a medium or system determined by the
3 Secretary to be appropriate to ensure the secure and expeditious dis-
4 semination of the information to necessary selected individuals.

5 (d) ENFORCEMENT PROCEEDINGS.—In any proceeding to enforce this
6 section, vulnerability assessments, site security plans, and other information
7 submitted to or obtained by the Secretary under this subchapter, and re-
8 lated vulnerability or security information, shall be treated as if the infor-
9 mation were classified information.

10 (e) AVAILABILITY OF INFORMATION.—Notwithstanding any other provi-
11 sion of law (including section 552(b)(3) of title 5), section 552 of title 5
12 (known as the “Freedom of Information Act”) shall not apply to informa-
13 tion protected from public disclosure pursuant to subsection (a).

14 (f) SHARING OF INFORMATION WITH MEMBERS OF CONGRESS.—Nothing
15 in this section shall prohibit the Secretary from disclosing information devel-
16 oped under this subchapter to a Member of Congress in response to a re-
17 quest by a Member of Congress.

18 **§ 10654. Civil enforcement**

19 (a) NOTICE OF NONCOMPLIANCE.—

20 (1) IN GENERAL.—If the Secretary determines that a covered chem-
21 ical facility is not in compliance with this subchapter, the Secretary
22 shall—

23 (A) provide the owner or operator of the facility—

24 (i) not later than 14 days after the date on which the Sec-
25 retary makes the determination, a written notification of non-
26 compliance that includes a clear explanation of any deficiency
27 in the security vulnerability assessment or site security plan;
28 and

29 (ii) an opportunity for consultation with the Secretary or
30 the Secretary’s designee; and

31 (B) issue to the owner or operator of the facility an order to
32 comply with this subchapter by a date specified by the Secretary
33 in the order, which date shall be not later than 180 days after the
34 date on which the Secretary issues the order.

35 (2) CONTINUED NONCOMPLIANCE.—If an owner or operator remains
36 noncompliant after the procedures outlined in paragraph (1) have been
37 executed, or demonstrates repeated violations of this subchapter, the
38 Secretary may enter an order in accordance with this section assessing
39 a civil penalty, an order to cease operations, or both.

40 (b) CIVIL PENALTIES.—

1 (1) VIOLATIONS OF ORDERS.—Any person who violates an order
2 issued under this subchapter shall be liable for a civil penalty under
3 section 70119(a) of title 46.

4 (2) NON-REPORTING CHEMICAL FACILITIES OF INTEREST.—Any
5 owner of a chemical facility of interest who fails to comply with, or
6 knowingly submits false information under, this subchapter or the
7 CFATS regulations shall be liable for a civil penalty under section
8 70119(a) of title 46.

9 (c) EMERGENCY ORDERS.—

10 (1) IN GENERAL.—Notwithstanding subsection (a) or any site secu-
11 rity plan or alternative security program approved under this sub-
12 chapter, if the Secretary determines that there is an imminent threat
13 of death, serious illness, or severe personal injury, due to a violation
14 of this subchapter or the risk of a terrorist incident that may affect
15 a chemical facility of interest, the Secretary—

16 (A) shall consult with the facility, if practicable, on steps to
17 mitigate the risk; and

18 (B) may order the facility, without notice or opportunity for a
19 hearing, effective immediately or as soon as practicable, to—

20 (i) implement appropriate emergency security measures; or

21 (ii) cease or reduce some or all operations, in accordance
22 with safe shutdown procedures, if the Secretary determines
23 that such a cessation or reduction of operations is the most
24 appropriate means to address the risk.

25 (2) LIMITATION ON DELEGATION.—The Secretary may not delegate
26 the authority under paragraph (1) to any official other than the Under
27 Secretary responsible for overseeing critical infrastructure protection,
28 cybersecurity, and other related programs of the Department appointed
29 under section 10302(b)(1)(H) of this title.

30 (3) LIMITATION ON AUTHORITY.—The Secretary may exercise the
31 authority under this subsection only to the extent necessary to abate
32 the imminent threat determination under paragraph (1).

33 (4) DUE PROCESS FOR FACILITY OWNER OR OPERATOR.—

34 (A) WRITTEN ORDERS.—An order issued by the Secretary
35 under paragraph (1) shall be in the form of a written emergency
36 order that—

37 (i) describes the violation or risk that creates the imminent
38 threat;

39 (ii) states the security measures or order issued or im-
40 posed; and

1 (iii) describes the standards and procedures for obtaining
2 relief from the order.

3 (B) OPPORTUNITY FOR REVIEW.—After issuing an order under
4 paragraph (1) with respect to a chemical facility of interest, the
5 Secretary shall provide for review of the order under section 554
6 of title 5 if a petition for review is filed not later than 20 days
7 after the date on which the Secretary issues the order.

8 (C) EXPIRATION OF EFFECTIVENESS OF ORDER.—If a petition
9 for review of an order is filed under subparagraph (B) and the re-
10 view under that paragraph is not completed by the last day of the
11 30-day period beginning on the date on which the petition is filed,
12 the order shall vacate automatically at the end of that period un-
13 less the Secretary determines, in writing, that the imminent threat
14 providing a basis for the order continues to exist.

15 (d) RIGHT OF ACTION.—Nothing in this subchapter confers upon any in-
16 dividual except the Secretary or his or her designee a right of action against
17 an owner or operator of a covered chemical facility to enforce any provision
18 of this subchapter.

19 **§ 10655. Whistleblower protections**

20 (a) PROCEDURE FOR REPORTING PROBLEMS.—

21 (1) ESTABLISHMENT.—The Secretary shall establish, and provide in-
22 formation to the public regarding, a procedure under which any em-
23 ployee or contractor of a chemical facility of interest may submit a re-
24 port to the Secretary regarding a violation of a requirement under this
25 subchapter.

26 (2) CONFIDENTIALITY.—The Secretary shall keep confidential the
27 identity of an individual who submits a report under paragraph (1),
28 and the report shall be treated as a record containing protected infor-
29 mation to the extent that the report does not consist of publicly avail-
30 able information.

31 (3) ACKNOWLEDGMENT OF RECEIPT.—If a report submitted under
32 paragraph (1) identifies the individual making the report, the Secretary
33 shall promptly respond to the individual directly and shall promptly ac-
34 knowledge receipt of the report.

35 (4) STEPS TO ADDRESS PROBLEMS.—The Secretary—

36 (A) shall review and consider the information provided in any
37 report submitted under paragraph (1); and

38 (B) may take action under section 10654 of this title if nec-
39 essary to address any substantiated violation of a requirement
40 under this subchapter identified in the report.

41 (5) DUE PROCESS FOR FACILITY OWNER OR OPERATOR.—

1 (A) IN GENERAL.—If, on the review described in paragraph (4),
2 the Secretary determines that a violation of a provision of this
3 subchapter, or a regulation prescribed under this subchapter, has
4 occurred, the Secretary may—

5 (i) institute a civil enforcement under section 10654(a) of
6 this title; or

7 (ii) if the Secretary makes the determination under section
8 10654(e) of this title, issue an emergency order.

9 (B) WRITTEN ORDERS.—The action of the Secretary under
10 paragraph (4) shall be in a written form that—

11 (i) describes the violation;

12 (ii) states the authority under which the Secretary is pro-
13 ceeding; and

14 (iii) describes the standards and procedures for obtaining
15 relief from the order.

16 (C) OPPORTUNITY FOR REVIEW.—After taking action under
17 paragraph (4), the Secretary shall provide for review of the action
18 if a petition for review is filed within 20 calendar days of the date
19 of issuance of the order for the action.

20 (D) EXPIRATION OF EFFECTIVENESS OF ORDER.—If a petition
21 for review of an action is filed under subparagraph (C) and the
22 review under that subparagraph is not completed by the end of the
23 30-day period beginning on the date the petition is filed, the ac-
24 tion shall cease to be effective at the end of that period unless the
25 Secretary determines, in writing, that the violation providing a
26 basis for the action continues to exist.

27 (6) RETALIATION PROHIBITED.—

28 (A) IN GENERAL.—An owner or operator of a chemical facility
29 of interest or agent thereof may not discharge an employee or oth-
30 erwise discriminate against an employee with respect to the com-
31 pensation provided to, or terms, conditions, or privileges of the
32 employment of, the employee because the employee (or an indi-
33 vidual acting pursuant to a request of the employee) submitted a
34 report under paragraph (1).

35 (B) EXCEPTION.—An employee shall not be entitled to the pro-
36 tections under this section if the employee—

37 (i) knowingly and willfully makes any false, fictitious, or
38 fraudulent statement or representation; or

39 (ii) uses any false writing or document knowing the writing
40 or document contains any false, fictitious, or fraudulent state-
41 ment or entry.

1 (b) PROTECTED DISCLOSURES.—Nothing in this subchapter shall be con-
2 strued to limit the right of an individual to make any disclosure—

3 (1) protected or authorized under section 2302(b)(8) or 7211 of title
4 5;

5 (2) protected under any other Federal or State law that shields the
6 disclosing individual against retaliation or discrimination for having
7 made the disclosure in the public interest; or

8 (3) to the Special Counsel of an agency, the inspector general of an
9 agency, or any other employee designated by the head of an agency to
10 receive disclosures similar to the disclosures described in paragraphs
11 (1) and (2).

12 (c) PUBLICATION OF RIGHTS.—The Secretary, in partnership with indus-
13 try associations and labor organizations, shall make publicly available both
14 physically and online the rights that an individual who discloses information,
15 including security-sensitive information, regarding problems, deficiencies, or
16 vulnerabilities at a covered chemical facility would have under Federal whis-
17 tleblower protection laws or this subchapter.

18 (d) PROTECTED INFORMATION.—All information contained in a report
19 made under subsection (a) shall be protected in accordance with section
20 10653 of this title.

21 § 10656. Relationship to other laws

22 (a) OTHER FEDERAL LAWS.—Nothing in this subchapter shall be con-
23 strued to supersede, amend, alter, or affect any Federal law that—

24 (1) regulates (including by requiring information to be submitted or
25 made available) the manufacture, distribution in commerce, use, han-
26 dling, sale, other treatment, or disposal of chemical substances or mix-
27 tures; or

28 (2) authorizes or requires the disclosure of any record or information
29 obtained from a chemical facility under any law other than this sub-
30 chapter.

31 (b) STATES AND POLITICAL SUBDIVISIONS.—This subchapter shall not
32 preclude or deny any right of any State or political subdivision of a State
33 to adopt or enforce any regulation, requirement, or standard of performance
34 with respect to chemical facility security that is more stringent than a regu-
35 lation, requirement, or standard of performance issued under this sub-
36 chapter, or otherwise impair any right or jurisdiction of any State with re-
37 spect to chemical facilities within that State, unless there is an actual con-
38 flict between this section and the law of that State.

39 § 10657. CFATS regulations

40 (a) GENERAL AUTHORITY.—The Secretary may, in accordance with chap-
41 ter 5 of title 5, promulgate regulations or amend CFATS regulations that

1 existed 30 days after December 18, 2014, to implement the provisions under
2 this subchapter.

3 (b) EXISTING CFATS REGULATIONS.—

4 (1) IN GENERAL.—Notwithstanding section 4(b) of the Protecting
5 and Securing Chemical Facilities from Terrorist Attacks Act of 2014
6 (Public Law 113–254, 128 Stat. 2919), each CFATS regulation that
7 existed on December 18, 2014, remains in effect unless the Secretary
8 amends, consolidates, or repeals the regulation.

9 (2) REPEAL.—Not later than 30 days after December 18, 2014, the
10 Secretary shall repeal any CFATS regulation that existed on that date
11 that the Secretary determines is duplicative of, or conflicts with, this
12 subchapter.

13 (c) AUTHORITY.—The Secretary shall exclusively rely upon authority pro-
14 vided under this subchapter in—

- 15 (1) determining compliance with this subchapter;
- 16 (2) identifying chemicals of interest; and
- 17 (3) determining security risk associated with a chemical facility.

18 **§ 10658. Small covered chemical facilities**

19 (a) DEFINITION OF SMALL COVERED CHEMICAL FACILITY.—In this sec-
20 tion, the term “small covered chemical facility” means a covered chemical
21 facility that—

- 22 (1) has fewer than 100 employees employed at the covered chemical
23 facility; and
- 24 (2) is owned and operated by a small business concern (as defined
25 in section 3 of the Small Business Act (15 U.S.C. 632)).

26 (b) ASSISTANCE TO FACILITIES.—The Secretary may provide guidance
27 and, as appropriate, tools, methodologies, or computer software, to assist
28 small covered chemical facilities in developing the physical security, cyberse-
29 curity, recordkeeping, and reporting procedures required under this sub-
30 chapter.

31 (c) REPORT.—The Secretary shall submit to the Committee on Homeland
32 Security and Governmental Affairs of the Senate and the Committee on
33 Homeland Security and the Committee on Energy and Commerce of the
34 House of Representatives a report on best practices that may assist small
35 covered chemical facilities in the development of physical security best prac-
36 tices.

37 **§ 10659. Outreach to chemical facilities of interest**

38 The Secretary shall establish an outreach implementation plan, in coordi-
39 nation with the heads of other appropriate Federal and State agencies, rel-
40 evant business associations, and public and private labor organizations, to—

- 41 (1) identify chemical facilities of interest; and

- 1 (2) make available compliance assistance materials and information
2 on education and training.

3 **§ 10660. Termination**

4 The authority provided under this subchapter terminates on January 17,
5 2019.

6 **Chapter 107—Science and Technology in**
7 **Support of Homeland Security**

Sec.

10701. Responsibilities and authorities of the Under Secretary for Science and Technology.
10702. Functions transferred.
10703. Conduct of certain public health-related activities.
10704. Federally funded research and development centers.
10705. Miscellaneous provisions.
10706. Homeland Security Advanced Research Projects Agency.
10707. Conduct of research, development, demonstration, testing, and evaluation.
10708. Utilization of Department of Energy national laboratories and sites in support of
 homeland security activities.
10709. Transfer of Plum Island Animal Disease Center, Department of Agriculture.
10710. Homeland Security Science and Technology Advisory Committee.
10711. Technology clearinghouse to encourage and support innovative solutions to enhance
 homeland security.
10712. Enhancement of public safety communications interoperability.
10713. Office for Interoperability and Compatibility.
10714. Emergency communications interoperability research and development.
10715. National Biosurveillance Integration Center.
10716. Promoting antiterrorism through international cooperation program.
10717. National biodefense strategy and implementation plan.
10718. Transparency in research and development.
10719. EMP and GMD mitigation research and development.

8 **§ 10701. Responsibilities and authorities of the Under Sec-**
9 **retary for Science and Technology**

10 The Secretary, acting through the Under Secretary for Science and Tech-
11 nology, is responsible for—

- 12 (1) advising the Secretary regarding research and development ef-
13 forts and priorities in support of the Department’s missions;
14 (2) developing, in consultation with other appropriate executive agen-
15 cies, a national policy and strategic plan for, identifying priorities,
16 goals, objectives and policies for, and coordinating the Federal Govern-
17 ment’s civilian efforts to identify and develop, countermeasures to
18 chemical, biological, and other emerging terrorist threats, including the
19 development of—
20 (A) comprehensive, research-based definable goals for the ef-
21 forts; and
22 (B) annual measurable objectives and specific targets to accom-
23 plish and evaluate the goals for the efforts;
24 (3) supporting the Under Secretary for Intelligence and Analysis and
25 the Assistant Secretary for Infrastructure Protection, by assessing and
26 testing homeland security vulnerabilities and possible threats;

1 (4) conducting basic and applied research, development, demonstra-
2 tion, testing, and evaluation activities that are relevant to any or all
3 elements of the Department, through both intramural and extramural
4 programs, except that the responsibility does not extend to human
5 health-related research and development activities;

6 (5) establishing priorities for, directing, funding, and conducting na-
7 tional research, development, test and evaluation, and procurement of,
8 technology and systems for—

9 (A) preventing the importation of chemical, biological, and re-
10 lated weapons and material; and

11 (B) detecting, preventing, protecting against, and responding to,
12 terrorist attacks;

13 (6) establishing a system for transferring homeland security develop-
14 ments or technologies to Federal, State, local government, and private-
15 sector entities;

16 (7) entering into work agreements, joint sponsorships, contracts, or
17 other agreements with the Department of Energy regarding the use of
18 the national laboratories or sites, and the support of the science and
19 technology base at those facilities;

20 (8) collaborating with the Secretary of Agriculture and the Attorney
21 General as provided in section 212 of the Agricultural Bioterrorism
22 Protection Act of 2002 (7 U.S.C. 8401);

23 (9) collaborating with the Secretary of Health and Human Services
24 and the Attorney General in determining any new biological agents and
25 toxins that shall be listed as “select agents” in Appendix A of part 72
26 of title 42, Code of Federal Regulations, pursuant to section 351A of
27 the Public Health Service Act (42 U.S.C. 262a);

28 (10) supporting United States leadership in science and technology;

29 (11) establishing and administering the primary research and devel-
30 opment activities of the Department, including the long-term research
31 and development needs and capabilities for all elements of the Depart-
32 ment;

33 (12) coordinating and integrating all research, development, dem-
34 onstration, testing, and evaluation activities of the Department;

35 (13) coordinating with other appropriate executive agencies in devel-
36 oping and carrying out the science and technology agenda of the De-
37 partment to reduce duplication and identify unmet needs; and

38 (14) developing and overseeing the administration of guidelines for
39 merit review of research and development projects throughout the De-
40 partment, and for the dissemination of research conducted or sponsored
41 by the Department.

1 **§ 10702. Functions transferred**

2 The Secretary succeeds to the functions, personnel, assets, and liabilities
3 of the following entities:

4 (1) The following programs and activities of the Department of En-
5 ergy, including the functions of the Secretary of Energy relating there-
6 to (but not including programs and activities relating to the strategic
7 nuclear defense posture of the United States):

8 (A) The chemical and biological national security and sup-
9 porting programs and activities of the nonproliferation and
10 verification research and development program.

11 (B) The nuclear smuggling programs and activities within the
12 proliferation detection program of the nonproliferation and
13 verification research and development program. The programs and
14 activities described in this subparagraph may be designated by the
15 President either for transfer to the Department or for joint oper-
16 ation by the Secretary and the Secretary of Energy.

17 (C) The nuclear assessment program and activities of the as-
18 sessment, detection, and cooperation program of the international
19 materials protection and cooperation program.

20 (D) Life sciences activities of the biological and environmental
21 research program related to microbial pathogens designated by the
22 President for transfer to the Department.

23 (E) The Environmental Measurements Laboratory.

24 (F) The advanced scientific computing research program and
25 activities at Lawrence Livermore National Laboratory.

26 (2) The National Bio-Weapons Defense Analysis Center of the De-
27 partment of Defense, including the functions of the Secretary of De-
28 fense related thereto.

29 **§ 10703. Conduct of certain public health-related activities**

30 (a) IN GENERAL.—With respect to civilian human health-related research
31 and development activities relating to countermeasures for chemical, biologi-
32 cal, radiological, and nuclear and other emerging terrorist threats carried
33 out by the Department of Health and Human Services (including the Public
34 Health Service), the Secretary of Health and Human Services shall set pri-
35 orities, goals, objectives, and policies and develop a coordinated strategy for
36 the activities in collaboration with the Secretary of Homeland Security to
37 ensure consistency with the national policy and strategic plan developed
38 under section 10701 of this title.

39 (b) EVALUATION OF PROGRESS.—In carrying out subsection (a), the Sec-
40 retary of Health and Human Services shall collaborate with the Secretary
41 in developing specific benchmarks and outcome measurements for evaluating

1 progress toward achieving the priorities and goals described in the sub-
2 section.

3 **§ 10704. Federally funded research and development centers**

4 The Secretary, acting through the Under Secretary for Science and Tech-
5 nology, shall have the authority to establish or contract with one or more
6 federally funded research and development centers to provide independent
7 analysis of homeland security issues, or to carry out other responsibilities
8 under this subtitle, including coordinating and integrating both the extra-
9 mural and intramural programs described in section 10707 of this title.

10 **§ 10705. Miscellaneous provisions**

11 (a) CLASSIFICATION.—To the greatest extent practicable, research con-
12 ducted or supported by the Department shall be unclassified.

13 (b) CONSTRUCTION.—Nothing in this chapter shall be construed to pre-
14 clude any Under Secretary of the Department from carrying out research,
15 development, demonstration, or deployment activities, as long as the activi-
16 ties are coordinated through the Under Secretary for Science and Tech-
17 nology.

18 (c) REGULATIONS.—The Secretary, acting through the Under Secretary
19 for Science and Technology, may issue necessary regulations with respect
20 to research, development, demonstration, testing, and evaluation activities of
21 the Department, including the conducting, funding, and reviewing of the ac-
22 tivities.

23 **§ 10706. Homeland Security Advanced Research Projects**
24 **Agency**

25 (a) DEFINITIONS.—In this section:

26 (1) FUND.—The term “Fund” means the Acceleration Fund for Re-
27 search and Development of Homeland Security Technologies estab-
28 lished in subsection (c).

29 (2) HOMELAND SECURITY RESEARCH.—The term “homeland secu-
30 rity research” means research relevant to the detection of, prevention
31 of, protection against, response to, attribution of, and recovery from
32 homeland security threats, particularly acts of terrorism.

33 (3) HSARPA.—The term “HSARPA” means the Homeland Secu-
34 rity Advanced Research Projects Agency established in subsection (b).

35 (4) UNDER SECRETARY.—The term “Under Secretary” means the
36 Under Secretary for Science and Technology.

37 (b) HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY.—

38 (1) ESTABLISHMENT.—There is in the Department the Homeland
39 Security Advanced Research Projects Agency (HSARPA).

1 (2) DIRECTOR.—The Director is the head of HSARPA. The Director
2 is appointed by the Secretary. The Director reports to the Under Sec-
3 retary.

4 (3) RESPONSIBILITIES.—The Director shall administer the Fund to
5 award competitive, merit-reviewed grants, cooperative agreements, or
6 contracts to public or private entities, including businesses, federally
7 funded research and development centers, and universities. The Direc-
8 tor shall administer the Fund to—

9 (A) support basic and applied homeland security research to
10 promote revolutionary changes in technologies that would promote
11 homeland security;

12 (B) advance the development, testing and evaluation, and de-
13 ployment of critical homeland security technologies;

14 (C) accelerate the prototyping and deployment of technologies
15 that would address homeland security vulnerabilities; and

16 (D) conduct research and development for the purpose of ad-
17 vancing technology for the investigation of child exploitation
18 crimes, including child victim identification, trafficking in individ-
19 uals, and child pornography, and for advanced forensics.

20 (4) TARGETED COMPETITIONS.—The Director may solicit proposals
21 to address specific vulnerabilities identified by the Director.

22 (5) COORDINATION.—The Director shall ensure that the activities of
23 HSARPA are coordinated with those of other relevant research agen-
24 cies, and may run projects jointly with other agencies.

25 (6) PERSONNEL.—In hiring personnel for HSARPA, the Secretary
26 has the hiring and management authorities described in section 1101
27 of the Strom Thurmond National Defense Authorization Act for Fiscal
28 Year 1999 (Public Law 105–261, 5 U.S.C. 3104 note). The term of
29 appointments for employees under subsection (c)(1) of that section may
30 not exceed 5 years before the granting of an extension under subsection
31 (c)(2) of that section.

32 (7) DEMONSTRATIONS.—The Director, periodically, shall hold home-
33 land security technology demonstrations to improve contact among
34 technology developers, vendors and acquisition personnel.

35 (e) FUND.—

36 (1) ESTABLISHMENT.—There is in the Department the Acceleration
37 Fund for Research and Development of Homeland Security Tech-
38 nologies (in this subsection referred to as the “Acceleration Fund”).
39 The Director administers the Acceleration Fund.

1 (2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to
2 be appropriated to the Acceleration Fund such sums as may be nec-
3 essary.

4 **§ 10707. Conduct of research, development, demonstration,**
5 **testing, and evaluation**

6 (a) IN GENERAL.—The Secretary, acting through the Under Secretary
7 for Science and Technology, shall carry out the responsibilities under section
8 10701(4) of this title through both extramural and intramural programs.

9 (b) EXTRAMURAL PROGRAMS.—

10 (1) IN GENERAL.—The Secretary, acting through the Under Sec-
11 retary for Science and Technology, shall operate extramural research,
12 development, demonstration, testing, and evaluation programs so as
13 to—

14 (A) ensure that colleges, universities, private research institutes,
15 and companies (and consortia thereof) from as many areas of the
16 United States as practicable participate;

17 (B) ensure that the research funded is of high quality, as deter-
18 mined through merit review processes developed under section
19 10701(14) of this title; and

20 (C) distribute funds through grants, cooperative agreements,
21 and contracts.

22 (2) UNIVERSITY-BASED CENTERS FOR HOMELAND SECURITY.—

23 (A) DESIGNATION.—The Secretary, acting through the Under
24 Secretary for Science and Technology, shall designate a university-
25 based center or several university-based centers for homeland secu-
26 rity. The purpose of the center or these centers shall be to estab-
27 lish a coordinated, university-based system to enhance the Na-
28 tion's homeland security.

29 (B) CRITERIA FOR DESIGNATION.—Criteria for the designation
30 of colleges or universities as a center for homeland security, shall
31 include demonstrated expertise in—

32 (i) the training of first responders;

33 (ii) responding to incidents involving weapons of mass de-
34 struction and biological warfare;

35 (iii) emergency and diagnostic medical services;

36 (iv) chemical, biological, radiological, and nuclear counter-
37 measures or detection;

38 (v) animal and plant health and diagnostics;

39 (vi) food safety;

40 (vii) water and wastewater operations;

41 (viii) port and waterway security;

- 1 (ix) multi-modal transportation;
- 2 (x) information security and information engineering;
- 3 (xi) engineering;
- 4 (xii) educational outreach and technical assistance;
- 5 (xiii) border transportation and security; and
- 6 (xiv) the public policy implications and public dissemination
- 7 of homeland security related research and development;

8 (C) DISCRETION OF SECRETARY.—To the extent that exercising
9 discretion is in the interest of homeland security, and with respect
10 to the designation of any given university-based center for home-
11 land security, the Secretary may except certain criteria as speci-
12 fied in subparagraph (B) and consider additional criteria beyond
13 those specified in subparagraph (B). On designation of a univer-
14 sity-based center for homeland security, the Secretary shall that
15 day publish in the Federal Register the criteria that were excepted
16 or added in the selection process and the justification for the set
17 of criteria that were used for that designation.

18 (D) REPORT TO CONGRESS.—The Secretary shall report annu-
19 ally to Congress concerning the implementation of this section.
20 The report shall indicate which center or centers have been des-
21 ignated and how the designation or designations enhance home-
22 land security, as well as report any decisions to revoke or modify
23 the designations.

24 (E) AUTHORIZATION OF APPROPRIATIONS.—There are author-
25 ized to be appropriated such sums as may be necessary to carry
26 out this paragraph.

27 (c) INTRAMURAL PROGRAMS.—

28 (1) CONSULTATION.—In carrying out the duties under section 10701
29 of this title, the Secretary, acting through the Under Secretary for
30 Science and Technology, may draw upon the expertise of any labora-
31 tory of the Federal Government, whether operated by a contractor or
32 the Government.

33 (2) LABORATORIES.—The Secretary, acting through the Under Sec-
34 retary for Science and Technology, may establish a headquarters lab-
35 oratory for the Department at any laboratory or site and may establish
36 additional laboratory units at other laboratories or sites.

37 (3) CRITERIA FOR HEADQUARTERS LABORATORY.—If the Secretary
38 chooses to establish a headquarters laboratory under paragraph (2), the
39 Secretary shall do the following:

1 (A) Establish criteria for the selection of the headquarters lab-
 2 oratory in consultation with the National Academy of Sciences, ap-
 3 propriate Federal agencies, and other experts.

4 (B) Publish the criteria in the Federal Register.

5 (C) Evaluate all appropriate laboratories or sites against the
 6 criteria.

7 (D) Select a laboratory or site on the basis of the criteria.

8 (E) Report to the appropriate congressional committees on
 9 which laboratory was selected, how the selected laboratory meets
 10 the published criteria, and what duties the headquarters labora-
 11 tory shall perform.

12 (4) LIMITATION ON OPERATION OF LABORATORIES.—A laboratory
 13 may not begin operating as the headquarters laboratory of the Depart-
 14 ment until at least 30 days after the transmittal of the report required
 15 by paragraph (3)(E).

16 **§ 10708. Utilization of Department of Energy national lab-**
 17 **oratories and sites in support of homeland secu-**
 18 **urity activities**

19 (a) AUTHORITY TO UTILIZE NATIONAL LABORATORIES AND SITES.—

20 (1) IN GENERAL.—In carrying out the missions of the Department,
 21 the Secretary may utilize the Department of Energy national labora-
 22 tories and sites through one or more of the following methods, as the
 23 Secretary considers appropriate:

24 (A) A joint sponsorship arrangement referred to in subsection
 25 (b).

26 (B) A direct contract between the Department and the applica-
 27 ble Department of Energy laboratory or site, subject to subsection
 28 (c).

29 (C) A “work for others” basis made available by that laboratory
 30 or site.

31 (D) Any other method provided by law.

32 (2) ACCEPTANCE AND PERFORMANCE BY LABS AND SITES.—Not-
 33 withstanding any other law governing the administration, mission, use,
 34 or operations of Department of Energy national laboratories and sites,
 35 the laboratories and sites may accept and perform work for the Sec-
 36 retary, consistent with resources provided, and perform work on an
 37 equal basis to other missions at the laboratory and not on a noninter-
 38 ference basis with other missions of the laboratory or site.

39 (b) JOINT SPONSORSHIP ARRANGEMENTS.—

40 (1) LABORATORIES.—The Department may be a joint sponsor, under
 41 a multiple agency sponsorship arrangement with the Department of

1 Energy, of one or more Department of Energy national laboratories in
2 the performance of work.

3 (2) SITES.—The Department may be a joint sponsor of a Depart-
4 ment of Energy site in the performance of work as if the site were a
5 federally funded research and development center and the work were
6 performed under a multiple agency sponsorship arrangement with the
7 Department.

8 (3) PRIMARY SPONSOR.—The Department of Energy shall be the pri-
9 mary sponsor under a multiple agency sponsorship arrangement re-
10 ferred to in paragraph (1) or (2).

11 (4) LEAD AGENT.—The Secretary of Energy shall act as the lead
12 agent in coordinating the formation and performance of a joint spon-
13 sorship arrangement under this subsection between the Department
14 and a Department of Energy national laboratory or site.

15 (5) COMPLIANCE WITH FEDERAL ACQUISITION REGULATION.—Work
16 performed by a Department of Energy national laboratory or site under
17 a joint sponsorship arrangement under this subsection shall comply
18 with the policy on the use of federally funded research and development
19 centers under the Federal Acquisition Regulation.

20 (6) FUNDING.—The Department shall provide funds for work at the
21 Department of Energy national laboratories or sites, as the case may
22 be, under a joint sponsorship arrangement under this subsection under
23 the same terms and conditions as apply to the primary sponsor of a
24 national laboratory under section 3303(a)(1)(C) of title 41 or of a site
25 to the extent the section applies to the site as a federally funded re-
26 search and development center by reason of this subsection.

27 (c) SEPARATE CONTRACTING.—To the extent that programs or activities
28 transferred by the Homeland Security Act of 2002 (Public Law 107-296,
29 116 Stat. 2135) from the Department of Energy to the Department are
30 being carried out through direct contracts with the operator of a national
31 laboratory or site of the Department of Energy, the Secretary and the Sec-
32 retary of Energy shall ensure that direct contracts for the programs and
33 activities between the Department and the operator are separate from the
34 direct contracts of the Department of Energy with the operator.

35 (d) AUTHORITY WITH RESPECT TO COOPERATIVE RESEARCH AND DE-
36 VELOPMENT AGREEMENTS AND LICENSING AGREEMENTS.—In connection
37 with utilization of Department of Energy national laboratories and sites
38 under this section, the Secretary may permit the director of a national lab-
39 oratory or site to enter into cooperative research and development agree-
40 ments or to negotiate licensing agreements with any person, any agency or
41 instrumentality, of the United States, any unit of State or local government,

1 and any other entity under the authority granted by section 12 of the Ste-
2 venson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3710a).
3 Technology may be transferred to a non-Federal party to an agreement con-
4 sistent with the provisions of sections 11 and 12 of that Act (15 U.S.C.
5 3710, 3710a).

6 (e) REIMBURSEMENT OF COSTS.—In the case of an activity carried out
7 by the operator of a Department of Energy national laboratory or site in
8 connection with the utilization of the laboratory or site under this section,
9 the Department shall reimburse the Department of Energy for costs of the
10 activity through a method under which the Secretary of Energy waives any
11 requirement for the Department to pay administrative charges or personnel
12 costs of the Department of Energy or its contractors in excess of the
13 amount that the Secretary of Energy pays for an activity carried out by the
14 contractor and paid for by the Department of Energy.

15 (f) LABORATORY-DIRECTED RESEARCH AND DEVELOPMENT BY THE DE-
16 PARTMENT OF ENERGY.—No funds authorized to be appropriated or other-
17 wise made available to the Department in a fiscal year may be obligated
18 or expended for laboratory directed research and development activities car-
19 ried out by the Department of Energy unless the activities support the mis-
20 sions of the Department.

21 (g) OFFICE FOR NATIONAL LABORATORIES.—There is in the Directorate
22 of Science and Technology the Office for National Laboratories. The Office
23 is responsible for the coordination and utilization of the Department of En-
24 ergy national laboratories and sites under this section in a manner to create
25 a networked laboratory system for the purpose of supporting the missions
26 of the Department.

27 (h) DEPARTMENT OF ENERGY COORDINATION ON HOMELAND SECURITY-
28 RELATED RESEARCH.—The Secretary of Energy shall ensure that research,
29 development, test, and evaluation activities conducted in the Department of
30 Energy that are directly or indirectly related to homeland security are fully
31 coordinated with the Secretary to minimize duplication of effort and maxi-
32 mize the effective application of Federal budget resources.

33 **§ 10709. Transfer of Plum Island Animal Disease Center, De-**
34 **partment of Agriculture**

35 (a) IN GENERAL.— The Secretary succeeds the Secretary of Agriculture
36 as head of the Plum Island Animal Disease Center of the Department of
37 Agriculture (in this section referred to as the “Center”), including the as-
38 sets and liabilities of the Center.

39 (b) CONTINUED DEPARTMENT OF AGRICULTURE ACCESS.—On comple-
40 tion of the transfer of the Center under subsection (a), the Secretary and
41 the Secretary of Agriculture shall enter into an agreement to ensure that

1 the Department of Agriculture is able to carry out research, diagnostic, and
2 other activities of the Department of Agriculture at the Center.

3 (c) DIRECTION OF ACTIVITIES.—The Secretary of Agriculture shall con-
4 tinue to direct the research, diagnostic, and other activities of the Depart-
5 ment of Agriculture at the Center.

6 (d) NOTIFICATION.—At least 180 days before a change in the biosafety
7 level at the Center, the President shall notify Congress of the change and
8 describe the reasons for the change.

9 (e) RELOCATION OF NATIONAL BIO- AND AGRO-DEFENSE FACILITY.—

10 (1) IN GENERAL.—Notwithstanding any other provision of law, if the
11 Secretary determines that the National Bio- and Agro-defense Facility
12 should be located at a site other than Plum Island, New York, the Sec-
13 retary shall ensure that the Administrator of General Services sells
14 through public sale all real and related personal property and transpor-
15 tation assets that support Plum Island operations, subject to terms and
16 conditions necessary to protect Government interests and meet program
17 requirements.

18 (2) PROCEEDS OF SALE.—The proceeds of the sale described in sub-
19 section (a) shall be deposited as offsetting collections into the Depart-
20 ment of Homeland Security Science and Technology “Research, Devel-
21 opment, Acquisition, and Operations” account and, subject to appro-
22 priation, shall be available until expended, for site acquisition, construc-
23 tion, and costs related to the construction of the National Bio- and
24 Agro-defense Facility, including the costs associated with the sale, in-
25 cluding due diligence requirements, necessary environmental remedi-
26 ation at Plum Island, and reimbursement of expenses incurred by the
27 General Services Administration.

28 **§ 10710. Homeland Security Science and Technology Advi-**
29 **sory Committee**

30 (a) ESTABLISHMENT.—There is in the Department a Homeland Security
31 Science and Technology Advisory Committee (in this section referred to as
32 the “Advisory Committee”). The Advisory Committee shall make rec-
33 ommendations with respect to the activities of the Under Secretary for
34 Science and Technology, including identifying research areas of potential
35 importance to the security of the Nation.

36 (b) MEMBERSHIP.—

37 (1) APPOINTMENT.—The Advisory Committee consists of 20 mem-
38 bers appointed by the Under Secretary for Science and Technology, in-
39 cluding emergency first-responders or representatives of organizations
40 or associations of emergency first-responders. The Advisory Committee
41 also shall include representatives of citizen groups, including economi-

1 cally disadvantaged communities. The individuals appointed as mem-
2 bers of the Advisory Committee—

3 (A) shall be eminent in fields such as emergency response, re-
4 search, engineering, new product development, business, and man-
5 agement consulting;

6 (B) shall be selected solely on the basis of established records
7 of distinguished service;

8 (C) shall not be employees of the Federal Government; and

9 (D) shall be selected to provide representation of a cross-section
10 of the research, development, demonstration, and deployment ac-
11 tivities supported by the Under Secretary for Science and Tech-
12 nology.

13 (2) NATIONAL RESEARCH COUNCIL.—The Under Secretary for
14 Science and Technology may enter into an arrangement for the Na-
15 tional Research Council to select members of the Advisory Committee,
16 but only if the panel used by the National Research Council reflects
17 the representation described in paragraph (1).

18 (c) TERMS OF OFFICE.—

19 (1) IN GENERAL.—Except as otherwise provided in this subsection,
20 the term of office of each member of the Advisory Committee shall be
21 3 years.

22 (2) VACANCIES.—A member appointed to fill a vacancy occurring be-
23 fore the expiration of the term for which the member's predecessor was
24 appointed shall be appointed for the remainder of the term.

25 (d) ELIGIBILITY.—A person who has completed 2 consecutive full terms
26 of service on the Advisory Committee is ineligible for appointment during
27 the 1-year period following the expiration of the 2d term.

28 (e) MEETINGS.—The Advisory Committee shall meet at least quarterly at
29 the call of the Chair or whenever one-third of the members request a meet-
30 ing in writing. Each member shall be given appropriate notice of the call
31 of each meeting, whenever possible not less than 15 days before the meet-
32 ing.

33 (f) QUORUM.—A majority of the members of the Advisory Committee not
34 having a conflict of interest in the matter being considered by the Advisory
35 Committee constitutes a quorum.

36 (g) CONFLICT OF INTEREST RULES.—The Advisory Committee shall es-
37 tablish rules for determining when 1 of its members has a conflict of inter-
38 est in a matter being considered by the Advisory Committee.

39 (h) REPORTS.—

40 (1) ANNUAL REPORT.—The Advisory Committee shall submit an an-
41 nual report to the Under Secretary for Science and Technology for

1 transmittal to Congress on or before January 31 each year. The report
2 shall describe the activities and recommendations of the Advisory Com-
3 mittee during the previous year.

4 (2) ADDITIONAL REPORTS.—The Advisory Committee may submit to
5 the Under Secretary for transmittal to Congress additional reports on
6 specific policy matters it considers appropriate.

7 (i) FEDERAL ADVISORY COMMITTEE ACT EXEMPTION.—Section 14 of
8 the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the
9 Advisory Committee.

10 **§ 10711. Technology clearinghouse to encourage and sup-**
11 **port innovative solutions to enhance homeland se-**
12 **curity**

13 (a) ESTABLISHMENT OF PROGRAM.—The Secretary, acting through the
14 Under Secretary for Science and Technology, shall establish and promote
15 a program to encourage technological innovation in facilitating the mission
16 of the Department (as described in section 10301 of this title).

17 (b) ELEMENTS OF PROGRAM.—The program described in subsection (a)
18 shall include the following components:

19 (1) The establishment of a centralized Federal clearinghouse for in-
20 formation relating to technologies that would further the mission of the
21 Department for dissemination, as appropriate, to Federal, State, and
22 local government and private-sector entities for additional review, pur-
23 chase, or use.

24 (2) The issuance of announcements seeking unique and innovative
25 technologies to advance the mission of the Department.

26 (3) The establishment of a technical assistance team to assist in
27 screening, as appropriate, proposals submitted to the Secretary (except
28 as provided in subsection (c)(2)) to assess the feasibility, scientific and
29 technical merits, and estimated cost of the proposals, as appropriate.

30 (4) The provision of guidance, recommendations, and technical as-
31 sistance, as appropriate, to assist Federal, State, and local government
32 and private-sector efforts to evaluate and implement the use of tech-
33 nologies described in paragraph (1) or (2).

34 (5) The provision of information for persons seeking guidance on
35 how to pursue proposals to develop or deploy technologies that would
36 enhance homeland security, including information relating to Federal
37 funding, regulation, or acquisition.

38 (c) MISCELLANEOUS PROVISIONS.—

39 (1) IN GENERAL.—Nothing in this section shall be construed as au-
40 thorizing the Secretary or the technical assistance team established
41 under subsection (b)(3) to set standards for technology to be used by

1 the Department, another executive agency, a State or local government
2 entity, or a private-sector entity.

3 (2) CERTAIN PROPOSALS.—The technical assistance team established
4 under subsection (b)(3) shall not consider or evaluate proposals sub-
5 mitted in response to a solicitation for offers for a pending procure-
6 ment or for a specific agency requirement.

7 (3) COORDINATION.—In carrying out this section, the Secretary shall
8 coordinate with the Technical Support Working Group (organized
9 under the April 1982 National Security Decision Directive Numbered
10 30).

11 **§ 10712. Enhancement of public safety communications**
12 **interoperability**

13 (a) DEFINITION OF INTEROPERABLE COMMUNICATIONS.—In this section,
14 the term “interoperable communications” means the ability of emergency
15 response providers and relevant Federal, State, and local government agen-
16 cies to communicate with each other as necessary, through a dedicated pub-
17 lic safety network utilizing information technology systems and radio com-
18 munications systems, and to exchange voice, data, and video with one an-
19 other on demand, in real time, as necessary.

20 (b) COORDINATION OF PUBLIC SAFETY INTEROPERABLE COMMUNICA-
21 TIONS PROGRAMS.—

22 (1) PROGRAM.—The Secretary, in consultation with the Secretary of
23 Commerce and the Chairman of the Federal Communications Commis-
24 sion, shall establish a program to enhance public safety interoperable
25 communications at all levels of government. The program shall—

26 (A) establish a comprehensive national approach to achieving
27 public safety interoperable communications;

28 (B) coordinate with other Federal agencies in carrying out sub-
29 paragraph (A);

30 (C) develop, in consultation with other appropriate Federal
31 agencies and State and local authorities, appropriate minimum ca-
32 pabilities for communications interoperability for Federal, State,
33 and local public safety agencies;

34 (D) accelerate, in consultation with other Federal agencies, in-
35 cluding the National Institute of Standards and Technology, the
36 private sector, and nationally recognized standards organizations
37 as appropriate, the development of national voluntary consensus
38 standards for public safety interoperable communications, recog-
39 nizing—

40 (i) the value, life cycle, and technical capabilities of existing
41 communications infrastructure;

1 (ii) the need for cross-border interoperability between
2 States and nations;

3 (iii) the unique needs of small, rural communities; and

4 (iv) the interoperability needs for daily operations and cata-
5 strophic events;

6 (E) encourage the development and implementation of flexible
7 and open architectures incorporating, where possible, technologies
8 that currently are commercially available, with appropriate levels
9 of security, for short-term and long-term solutions to public safety
10 communications interoperability;

11 (F) assist other Federal agencies in identifying priorities for re-
12 search, development, testing, and evaluation with regard to public
13 safety interoperable communications;

14 (G) identify priorities in the Department for research, develop-
15 ment, and testing and evaluation with regard to public safety
16 interoperable communications;

17 (H) establish coordinated guidance for Federal grant programs
18 for public safety interoperable communications;

19 (I) provide technical assistance to State and local public safety
20 agencies regarding planning, acquisition strategies, interoperability
21 architectures, training, and other functions necessary to achieve
22 public safety communications interoperability;

23 (J) develop and disseminate best practices to improve public
24 safety communications interoperability; and

25 (K) develop appropriate performance measures and milestones
26 to systematically measure the Nation's progress toward achieving
27 public safety communications interoperability, including the devel-
28 opment of national voluntary consensus standards.

29 (2) OFFICE FOR INTEROPERABILITY AND COMPATIBILITY.—

30 (A) ESTABLISHMENT.—The Secretary may establish an Office
31 for Interoperability and Compatibility in the Directorate of Science
32 and Technology to carry out this subsection.

33 (B) FUNCTIONS.—If the Secretary establishes an office, the
34 Secretary shall, through the office, carry out Department respon-
35 sibilities and authorities relating to the SAFECOM Program.

36 (c) INTERNATIONAL INTEROPERABILITY.—The President shall establish a
37 mechanism for coordinating cross-border interoperability issues between—

38 (1) the United States and Canada; and

39 (2) the United States and Mexico.

40 (d) MULTIYEAR INTEROPERABILITY GRANTS.—

1 (1) MULTIYEAR COMMITMENTS.—In awarding grants to a State, re-
2 gion, local government, or Indian tribe for the purposes of enhancing
3 interoperable communications capabilities for emergency response pro-
4 viders, the Secretary may commit to obligate Federal assistance beyond
5 the current fiscal year, subject to the limitations and restrictions in this
6 subsection.

7 (2) RESTRICTIONS.—

8 (A) TIME LIMIT.—No multiyear interoperability commitment
9 may exceed 3 years in duration.

10 (B) AMOUNT OF COMMITTED FUNDS.—The total amount of as-
11 sistance the Secretary has committed to obligate for a future fiscal
12 year under paragraph (1) may not exceed \$150,000,000.

13 (3) LETTERS OF INTENT.—

14 (A) ISSUANCE.—Under paragraph (1), the Secretary may issue
15 a letter of intent to an applicant committing to obligate from fu-
16 ture budget authority an amount, not more than the Federal Gov-
17 ernment’s share of the project’s cost, for an interoperability com-
18 munications project (including interest costs and costs of formu-
19 lating the project).

20 (B) SCHEDULE.—A letter of intent under this paragraph shall
21 establish a schedule under which the Secretary will reimburse the
22 applicant for the Federal Government’s share of the project’s
23 costs, as amounts become available, if the applicant, after the Sec-
24 retary issues the letter, carries out the project before receiving
25 amounts under a grant issued by the Secretary.

26 (C) NOTICE TO SECRETARY.—An applicant that is issued a let-
27 ter of intent under this subsection shall notify the Secretary of the
28 applicant’s intent to carry out a project pursuant to the letter be-
29 fore the project begins.

30 (D) NOTICE TO CONGRESS.—The Secretary shall transmit a
31 written notification to Congress no later than 3 days before the
32 issuance of a letter of intent under this section.

33 (E) LIMITATIONS.—A letter of intent issued under this section
34 is not an obligation of the Government under section 1501 of title
35 31, and is not deemed to be an administrative commitment for fi-
36 nancing. An obligation or administrative commitment may be
37 made only as amounts are provided in authorization and appro-
38 priations laws.

39 (F) STATUTORY CONSTRUCTION.—Nothing in this subsection
40 shall be construed—

1 (i) to prohibit the obligation of amounts pursuant to a let-
2 ter of intent under this subsection in the same fiscal year as
3 the letter of intent is issued; or

4 (ii) to apply to, or replace, Federal assistance intended for
5 interoperable communications that is not provided pursuant
6 to a commitment under this subsection.

7 (e) INTEROPERABLE COMMUNICATIONS PLANS.—An applicant requesting
8 funding assistance from the Secretary for interoperable communications for
9 emergency response providers shall submit an Interoperable Communica-
10 tions Plan to the Secretary for approval. A plan shall—

11 (1) describe the current state of communications interoperability in
12 the applicable jurisdictions among Federal, State, and local emergency
13 response providers and other relevant private resources;

14 (2) describe the available and planned use of public safety frequency
15 spectrum and resources for interoperable communications within the
16 jurisdictions;

17 (3) describe how the planned use of spectrum and resources for
18 interoperable communications is compatible with surrounding capabili-
19 ties and interoperable communications plans of Federal, State, and
20 local governmental entities, military installations, foreign governments,
21 critical infrastructure, and other relevant entities;

22 (4) include a 5-year plan for the dedication of Federal, State, and
23 local government and private resources to achieve a consistent, secure,
24 and effective interoperable communications system, including planning,
25 system design and engineering, testing and technology development,
26 procurement and installation, training, and operations and mainte-
27 nance;

28 (5) describe how the 5-year plan meets or exceeds applicable stand-
29 ards and grant requirements established by the Secretary;

30 (6) include information on the governance structure used to develop
31 the plan, including this information about all agencies and organiza-
32 tions that participated in developing the plan and the scope and time-
33 frame of the plan; and

34 (7) describe the method by which multijurisdictional, multidisci-
35 plinary input is provided from all regions of the jurisdiction, including
36 high-threat urban areas located in the jurisdiction, and the process for
37 continuing to incorporate input.

38 (f) EXPANDED REPORTING REQUIREMENT.—In addition to the commit-
39 tees specifically enumerated to receive reports under title XII of the Imple-
40 menting Recommendations Of The 9/11 Commission Act Of 2007 (Public
41 Law 110–53, 121 Stat. 381), any report transmitted under the provisions

1 of title XII shall be transmitted to the appropriate congressional commit-
2 tees.

3 **§ 10713. Office for Interoperability and Compatibility**

4 (a) CLARIFICATION OF RESPONSIBILITIES.—The Director of the Office
5 for Interoperability and Compatibility shall—

6 (1) assist the Secretary in developing and implementing the science
7 and technology aspects of the program described in subparagraphs (D),
8 (E), (F), and (G) of section 10712(b)(1) of this title;

9 (2) in coordination with the Federal Communications Commission,
10 the National Institute of Standards and Technology, and other Federal
11 departments and agencies with responsibility for standards, support the
12 creation of national voluntary consensus standards for interoperable
13 emergency communications;

14 (3) establish a comprehensive research, development, testing, and
15 evaluation program for improving interoperable emergency communica-
16 tions;

17 (4) establish, in coordination with the Director for Emergency Com-
18 munications, requirements for interoperable emergency communications
19 capabilities, which shall be nonproprietary where standards for the ca-
20 pabilities exist, for all public safety radio and data communications sys-
21 tems and equipment purchased using homeland security assistance ad-
22 ministered by the Department, excluding an alert and warning device,
23 technology, or system;

24 (5) carry out the Department's responsibilities and authorities relat-
25 ing to research, development, testing, evaluation, or standards-related
26 elements of the SAFECOM Program;

27 (6) evaluate and assess new technology in real-world environments
28 to achieve interoperable emergency communications capabilities;

29 (7) encourage more efficient use of existing resources, including
30 equipment, to achieve interoperable emergency communications capa-
31 bilities;

32 (8) test public safety communications systems that are less prone to
33 failure, support new nonvoice services, use spectrum more efficiently,
34 and cost less than existing systems;

35 (9) coordinate with the private sector to develop solutions to improve
36 emergency communications capabilities and achieve interoperable emer-
37 gency communications capabilities; and

38 (10) conduct pilot projects, in coordination with the Director for
39 Emergency Communications, to test and demonstrate technologies, in-
40 cluding data and video, that enhance—

1 (A) the ability of emergency response providers and relevant
2 government officials to continue to communicate in the event of
3 natural disasters, acts of terrorism, and other man-made disasters;
4 and

5 (B) interoperable emergency communications capabilities.

6 (b) COORDINATION.—The Director of the Office for Interoperability and
7 Compatibility shall coordinate with the Director for Emergency Communica-
8 tions with respect to the SAFECOM program.

9 (c) SUFFICIENCY OF RESOURCES.—The Secretary shall provide the Office
10 for Interoperability and Compatibility the resources and staff necessary to
11 carry out the responsibilities under this section.

12 **§ 10714. Emergency communications interoperability re-**
13 **search and development**

14 (a) DEFINITION OF INTEROPERABLE EMERGENCY COMMUNICATIONS.—
15 In this section, the term “interoperable emergency communications” has the
16 meaning given the term “interoperable communications” under section
17 10712(a) of this title.

18 (b) IN GENERAL.—The Secretary, acting through the Under Secretary for
19 Science and Technology and the Director of the Office for Interoperability
20 and Compatibility, shall establish a comprehensive research and development
21 program to support and promote—

22 (1) the ability of emergency response providers and relevant govern-
23 ment officials to continue to communicate in the event of natural disas-
24 ters, acts of terrorism, and other man-made disasters; and

25 (2) interoperable emergency communications capabilities among
26 emergency response providers and relevant government officials, includ-
27 ing by—

28 (A) supporting research on a competitive basis, including
29 through the Directorate of Science and Technology and Homeland
30 Security Advanced Research Projects Agency; and

31 (B) considering the establishment of a Center of Excellence
32 under the Department of Homeland Security Centers of Excel-
33 lence Program focused on improving emergency response pro-
34 viders’ communication capabilities.

35 (c) PURPOSES.—The purposes of the program established under sub-
36 section (b) include—

37 (1) supporting research, development, testing, and evaluation on
38 emergency communication capabilities;

39 (2) understanding the strengths and weaknesses of the public safety
40 communications systems in use;

1 (3) examining how current and emerging technology can make emer-
 2 gency response providers more effective, and how Federal, State, local,
 3 and tribal government agencies can use this technology in a coherent
 4 and cost-effective manner;

5 (4) investigating technologies that could lead to long-term advance-
 6 ments in emergency communications capabilities and supporting re-
 7 search on advanced technologies and potential systemic changes to dra-
 8 matically improve emergency communications; and

9 (5) evaluating and validating advanced technology concepts, and fa-
 10 cilitating the development and deployment of interoperable emergency
 11 communication capabilities.

12 § 10715. National Biosurveillance Integration Center

13 (a) DEFINITIONS.—In this section:

14 (1) BIOLOGICAL AGENT.—The term “biological agent” has the mean-
 15 ing given the term in section 178 of title 18.

16 (2) BIOLOGICAL EVENT OF NATIONAL CONCERN.—The term “bio-
 17 logical event of national concern” means—

18 (A) an act of terrorism involving a biological agent or toxin; or

19 (B) a naturally occurring outbreak of an infectious disease that
 20 may result in a national epidemic.

21 (3) HOMELAND SECURITY INFORMATION.—The term “homeland se-
 22 curity information” has the meaning given the term in section 11707
 23 of this title.

24 (4) MEMBER AGENCY.—The term “Member Agency” means any
 25 Federal department or agency that, at the discretion of the head of
 26 that department or agency, has entered into a memorandum of under-
 27 standing regarding participation in the National Biosurveillance Inte-
 28 gration Center.

29 (5) PRIVACY OFFICER.—The term “Privacy Officer” means the Pri-
 30 vacy Officer appointed under section 10543 of this title.

31 (6) TOXIN.—The term “toxin” has the meaning given the term in
 32 section 178 of title 18.

33 (b) ESTABLISHMENT.—The Secretary shall establish, operate, and main-
 34 tain a National Biosurveillance Integration Center (in this section referred
 35 to as the “NBIC”) under an office or directorate of the Department that
 36 was in existence as of August 3, 2007. The Directing Officer is the head
 37 of the NBIC.

38 (c) PRIMARY MISSION.—The primary mission of the NBIC is to—

39 (1) enhance the capability of the Federal Government to—

40 (A) rapidly identify, characterize, localize, and track a biological
 41 event of national concern by integrating and analyzing data relat-

1 ing to human health, animal, plant, food, and environmental moni-
2 toring systems (both national and international); and

3 (B) disseminate alerts and other information to Member Agen-
4 cies and, in coordination with (and where possible through) Mem-
5 ber Agencies, to agencies of State, local, and tribal governments,
6 as appropriate, to enhance the ability of the agencies to respond
7 to a biological event of national concern; and

8 (2) oversee development and operation of the National Biosurveil-
9 lance Integration System.

10 (d) REQUIREMENTS.—The NBIC shall detect, as early as possible, a bio-
11 logical event of national concern that presents a risk to the United States
12 or the infrastructure or key assets of the United States, including by—

13 (1) consolidating data from all relevant surveillance systems main-
14 tained by Member Agencies to detect biological events of national con-
15 cern across human, animal, and plant species;

16 (2) seeking private sources of surveillance, both foreign and domes-
17 tic, when the sources would enhance coverage of critical surveillance
18 gaps;

19 (3) using an information technology system that uses the best avail-
20 able statistical and other analytical tools to identify and characterize
21 biological events of national concern in as close to real-time as is prac-
22 ticable;

23 (4) providing the infrastructure for integration, including informa-
24 tion technology systems and space, and support for personnel from
25 Member Agencies with sufficient expertise to enable analysis and inter-
26 pretation of data;

27 (5) working with Member Agencies to create information technology
28 systems that use the minimum amount of patient data necessary and
29 consider patient confidentiality and privacy issues at all stages of devel-
30 opment and apprise the Privacy Officer of these efforts; and

31 (6) alerting Member Agencies and, in coordination with (and where
32 possible through) Member Agencies, public health agencies of State,
33 local, and tribal governments regarding an incident that could develop
34 into a biological event of national concern.

35 (e) RESPONSIBILITIES OF DIRECTING OFFICER.—

36 (1) IN GENERAL.—The Directing Officer of the NBIC shall—

37 (A) on an ongoing basis, monitor the availability and appro-
38 priateness of surveillance systems used by the NBIC and those
39 systems that could enhance biological situational awareness or the
40 overall performance of the NBIC;

1 (B) on an ongoing basis, review and seek to improve the statis-
2 tical and other analytical methods used by the NBIC;

3 (C) receive and consider other relevant homeland security infor-
4 mation, as appropriate; and

5 (D) provide technical assistance, as appropriate, to all Federal,
6 regional, State, local, and tribal government entities and private-
7 sector entities that contribute data relevant to the operation of the
8 NBIC.

9 (2) ASSESSMENTS.—The Directing Officer of the NBIC shall—

10 (A) on an ongoing basis, evaluate available data for evidence of
11 a biological event of national concern; and

12 (B) integrate homeland security information with NBIC data to
13 provide overall situational awareness and determine whether a bio-
14 logical event of national concern has occurred.

15 (3) INFORMATION SHARING.—

16 (A) IN GENERAL.—The Directing Officer of the NBIC shall—

17 (i) establish a method of real-time communication with the
18 National Operations Center;

19 (ii) in the event that a biological event of national concern
20 is detected, notify the Secretary and disseminate results of
21 NBIC assessments relating to that biological event of national
22 concern to appropriate Federal response entities and, in co-
23 ordination with relevant Member Agencies, regional, State,
24 local, and tribal governmental response entities in a timely
25 manner;

26 (iii) provide any report on NBIC assessments to Member
27 Agencies and, in coordination with relevant Member Agencies,
28 an affected regional, State, local, or tribal government, and
29 any private-sector entity considered appropriate that may en-
30 hance the mission of the Member Agencies, governments, or
31 entities or the ability of the Nation to respond to biological
32 events of national concern; and

33 (iv) share NBIC incident or situational awareness reports,
34 and other relevant information, consistent with the informa-
35 tion sharing environment established under section 11708 of
36 this title and policies, guidelines, procedures, instructions, or
37 standards established under that section.

38 (B) CONSULTATION.—The Directing Officer of the NBIC shall
39 implement the activities described in subparagraph (A) consistent
40 with the policies, guidelines, procedures, instructions, or standards
41 established under section 11708 of this title and in consultation

1 with the Director of National Intelligence, the Under Secretary for
2 Intelligence and Analysis, and other offices or agencies of the Fed-
3 eral Government, as appropriate.

4 (f) RESPONSIBILITIES OF MEMBER AGENCIES.—Each Member Agency
5 shall—

6 (1) use its best efforts to integrate biosurveillance information into
7 the NBIC, with the goal of promoting information sharing between
8 Federal, State, local, and tribal governments to detect biological events
9 of national concern;

10 (2) provide timely information to assist the NBIC in maintaining bi-
11 ological situational awareness for accurate detection and response pur-
12 poses;

13 (3) enable the NBIC to receive and use biosurveillance information
14 from Member Agencies to carry out its requirements under subsection
15 (e);

16 (4) connect the biosurveillance data systems of that Member Agency
17 to the NBIC data system under mutually agreed protocols that are
18 consistent with subsection (d)(5);

19 (5) participate in the formation of strategy and policy for the oper-
20 ation of the NBIC and its information sharing;

21 (6) provide personnel to the NBIC under an interagency personnel
22 agreement and consider the qualifications of the personnel necessary to
23 provide human, animal, and environmental data analysis and interpre-
24 tation support to the NBIC; and

25 (7) retain responsibility for the surveillance and intelligence systems
26 of that department or agency, if applicable.

27 (g) ADMINISTRATIVE AUTHORITIES.—

28 (1) HIRING OF EXPERTS.—The Directing Officer of the NBIC shall
29 hire individuals with the necessary expertise to develop and operate the
30 NBIC.

31 (2) DETAIL OF PERSONNEL.—On request of the Directing Officer of
32 the NBIC, the head of a Federal department or agency may detail, on
33 a reimbursable basis, personnel of the department or agency to the De-
34 partment to assist the NBIC in carrying out this section.

35 (h) NBIC INTERAGENCY WORKING GROUP.—The Directing Officer of the
36 NBIC shall—

37 (1) establish an interagency working group to facilitate interagency
38 cooperation and to advise the Directing Officer of the NBIC regarding
39 recommendations to enhance the biosurveillance capabilities of the De-
40 partment; and

41 (2) invite Member Agencies to serve on that working group.

1 (i) RELATIONSHIP TO OTHER DEPARTMENTS AND AGENCIES.—The au-
 2 thority of the Directing Officer of the NBIC under this section shall not
 3 affect the authority or responsibility of another department or agency of the
 4 Federal Government with respect to biosurveillance activities under a pro-
 5 gram administered by that department or agency.

6 (j) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be
 7 appropriated such sums as are necessary to carry out this section.

8 **§ 10716. Promoting antiterrorism through international co-**
 9 **operation program**

10 (a) DEFINITIONS.—In this section:

11 (1) DIRECTOR.—The term “Director” means the Director selected
 12 under subsection (b)(2).

13 (2) INTERNATIONAL COOPERATIVE ACTIVITY.—The term “inter-
 14 national cooperative activity” includes—

15 (A) coordinated research projects, joint research projects, or
 16 joint ventures;

17 (B) joint studies or technical demonstrations;

18 (C) coordinated field exercises, scientific seminars, conferences,
 19 symposia, and workshops;

20 (D) training of scientists and engineers;

21 (E) visits and exchanges of scientists, engineers, or other appro-
 22 priate personnel;

23 (F) exchanges or sharing of scientific and technological informa-
 24 tion; and

25 (G) joint use of laboratory facilities and equipment.

26 (b) SCIENCE AND TECHNOLOGY HOMELAND SECURITY INTERNATIONAL
 27 COOPERATIVE PROGRAMS OFFICE.—

28 (1) ESTABLISHMENT.—There is in the Department the Science and
 29 Technology Homeland Security International Cooperative Programs Of-
 30 fice.

31 (2) DIRECTOR.—A Director is the head of the Office. The Direc-
 32 tor—

33 (A) shall be selected, in consultation with the Assistant Sec-
 34 retary for International Affairs, by and shall report to the Under
 35 Secretary for Science and Technology; and

36 (B) may be an officer of the Department serving in another po-
 37 sition.

38 (3) RESPONSIBILITIES.—

39 (A) DEVELOPMENT OF MECHANISMS.—The Director is respon-
 40 sible for developing, in coordination with the Department of State
 41 and, as appropriate, the Department of Defense, the Department

1 of Energy, and other Federal agencies, understandings and agree-
2 ments to allow and to support international cooperative activity in
3 support of homeland security.

4 (B) PRIORITIES.—The Director is responsible for developing, in
5 coordination with the Office of International Affairs and other
6 Federal agencies, strategic priorities for international cooperative
7 activity for the Department in support of homeland security.

8 (C) ACTIVITIES.—The Director shall facilitate the planning, de-
9 velopment, and implementation of international cooperative activ-
10 ity to address the strategic priorities developed under subpara-
11 graph (B) through mechanisms the Under Secretary for Science
12 and Technology considers appropriate, including grants, coopera-
13 tive agreements, or contracts to or with foreign public or private
14 entities, governmental organizations, businesses (including small
15 businesses and socially and economically disadvantaged small busi-
16 nesses (as the terms are defined in sections 3 and 8 of the Small
17 Business Act (15 U.S.C. 632 and 637), respectively)), federally
18 funded research and development centers, and universities.

19 (D) IDENTIFICATION OF PARTNERS.—The Director shall facili-
20 tate the matching of United States entities engaged in homeland
21 security research with non-United States entities engaged in home-
22 land security research so that they may partner in homeland secu-
23 rity research activities.

24 (4) COORDINATION.—The Director shall ensure that the activities
25 under this subsection are coordinated with the Office of International
26 Affairs and the Department of State and, as appropriate, the Depart-
27 ment of Defense, the Department of Energy, and other relevant Fed-
28 eral agencies or interagency bodies. The Director may enter into joint
29 activities with other Federal agencies.

30 (c) MATCHING FUNDING.—

31 (1) IN GENERAL.—

32 (A) EQUITABILITY.—The Director shall ensure that funding
33 and resources expended in international cooperative activity will be
34 equitably matched by the foreign partner government or other en-
35 tity through direct funding, funding of complementary activities,
36 or the provision of staff, facilities, material, or equipment.

37 (B) GRANT MATCHING AND REPAYMENT.—

38 (i) IN GENERAL.—The Secretary may require a recipient of
39 a grant under this section—

1 (I) to make a matching contribution of not more than
2 50 percent of the total cost of the proposed project for
3 which the grant is awarded; and

4 (II) to repay to the Secretary the amount of the grant
5 (or a portion thereof), interest on the amount at an ap-
6 propriate rate, and charges for administration of the
7 grant the Secretary determines appropriate.

8 (ii) LIMIT ON REPAYMENT.—The Secretary may not re-
9 quire that repayment under clause (i)(II) be more than 150
10 percent of the amount of the grant, adjusted for inflation on
11 the basis of the Consumer Price Index.

12 (2) FOREIGN PARTNERS.—Partners may include Israel, the United
13 Kingdom, Canada, Australia, Singapore, and other allies in the global
14 war on terrorism as determined to be appropriate by the Secretary and
15 the Secretary of State.

16 (3) LOANS OF EQUIPMENT.—The Director may make or accept loans
17 of equipment for research and development and comparative testing
18 purposes.

19 (d) FOREIGN REIMBURSEMENTS.—If the Science and Technology Home-
20 land Security International Cooperative Programs Office participates in an
21 international cooperative activity with a foreign partner on a cost-sharing
22 basis, reimbursements or contributions received from that foreign partner
23 to meet its share of the project may be credited to appropriate current ap-
24 propriations accounts of the Directorate of Science and Technology.

25 (e) REPORT TO CONGRESS ON INTERNATIONAL COOPERATIVE ACTIVI-
26 TIES.—The Secretary, acting through the Under Secretary for Science and
27 Technology and the Director, shall submit to Congress every five years a
28 report containing—

29 (1) a brief description of each grant, cooperative agreement, or con-
30 tract made or entered into under subsection (b)(3)(C), including the
31 participants, goals, and amount and sources of funding;

32 (2) a list of international cooperative activities underway, including
33 the participants, goals, expected duration, and amount and sources of
34 funding, including resources provided to support the activities in lieu
35 of direct funding;

36 (3) for international cooperative activities identified in the previous
37 reporting period, a status update on the progress of such activities, in-
38 cluding whether goals were realized, explaining any lessons learned, and
39 evaluating overall success; and

40 (4) a discussion of obstacles encountered in the course of forming,
41 executing, or implementing agreements for international cooperative ac-

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, the Secre-
8 taries of Defense, Health and Human Services, and Agriculture jointly shall
9 develop a national biodefense strategy and associated implementation plan,
10 which shall include a review and assessment of biodefense policies, practices,
11 programs, and initiatives. The Secretaries shall review and, as appropriate,
12 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.—Not later than 275 days after December
4 23, 2016, the Secretary and the Secretaries of Defense, Health and Human
5 Services, and Agriculture shall submit to the appropriate congressional com-
6 mittees the strategy and associated implementation plan required by sub-
7 section (b). The strategy and implementation plan shall be submitted in un-
8 classified form but may include a classified index.

9 (e) BRIEFINGS.—Not later than March 1, 2018, and 2019, the Secretary
10 and the Secretaries of Defense, Health and Human Services, and Agri-
11 culture shall provide to the Committees on Armed Services, Energy and
12 Commerce, Homeland Security, and Agriculture of the House of Represent-
13 atives a joint briefing on the strategy developed under subsection (b) and
14 the status of the implementation of the strategy.

15 (f) COMPTROLLER GENERAL REVIEW.—Not later than 180 days after the
16 date of the submittal of the strategy and implementation plan under sub-
17 section (d), the Comptroller General shall conduct a review of the strategy
18 and implementation plan to analyze gaps and resources mapped against the
19 requirements of the national biodefense strategy and existing United States
20 biodefense policy documents.

21 **§ 10718. Transparency in research and development**

22 (a) DEFINITIONS.—In this section:

23 (1) ALL APPROPRIATE DETAILS.—The term “all appropriate details”
24 means, with respect to a research and development project—

25 (A) the name of the project, including classified and unclassified
26 names if applicable;

27 (B) the name of the component of the Department carrying out
28 the project;

29 (C) an abstract or summary of the project;

30 (D) funding levels for the project;

31 (E) project duration or timeline;

32 (F) the name of each contractor, grantee, or cooperative agree-
33 ment partner involved in the project;

34 (G) expected objectives and milestones for the project; and

35 (H) to the maximum extent practicable, relevant literature and
36 patents that are associated with the project.

37 (2) CLASSIFIED.—The term “classified” means anything con-
38 taining—

39 (A) classified national security information as defined in section
40 6.1 of Executive Order 13526 (50 U.S.C. 3161 note) or any suc-
41 cessor order;

1 (B) Restricted Data or data that was formerly Restricted Data,
2 as defined in section 11(y) of the Atomic Energy Act of 1954 (42
3 U.S.C. 2014(y));

4 (C) material classified at the Sensitive Compartmented Informa-
5 tion (SCI) level, as defined in section 309 of the Intelligence Au-
6 thorization Act for Fiscal Year 2001 (50 U.S.C. 3345); or

7 (D) information relating to a special access program, as defined
8 in section 6.1 of Executive Order 13526 (50 U.S.C. 3161 note)
9 or any successor order.

10 (3) CONTROLLED UNCLASSIFIED INFORMATION.—The term “con-
11 trolled unclassified information” means information described as “Con-
12 trolled Unclassified Information” under Executive Order 13556 (44
13 U.S.C. 3501 note) or any successor order.

14 (4) PROJECT.—The term “project” means a research or development
15 project, program, or activity administered by the Department, whether
16 ongoing, completed, or otherwise terminated.

17 (b) REQUIREMENT TO LIST RESEARCH AND DEVELOPMENT
18 PROJECTS.—

19 (1) IN GENERAL.—The Secretary shall maintain a detailed list of the
20 following:

21 (A) Each classified and unclassified research and development
22 project, and all appropriate details for each project, including the
23 component of the Department responsible for each project.

24 (B) Each task order for a federally funded research and devel-
25 opment center not associated with a research and development
26 project.

27 (C) Each task order for a university-based center of excellence
28 not associated with a research and development project.

29 (D) The indicators developed and tracked by the Under Sec-
30 retary for Science and Technology with respect to transitioned
31 projects pursuant to subsection (d).

32 (2) EXCEPTION.—Paragraph (1) shall not apply to a project com-
33 pleted or otherwise terminated before December 23, 2016.

34 (3) UPDATES.—The list required under paragraph (1) shall be up-
35 dated as frequently as possible, but not less frequently than once per
36 quarter.

37 (4) PROVIDE DEFINITION OF RESEARCH AND DEVELOPMENT.—For
38 purposes of the list required under paragraph (1), the Secretary shall
39 provide a definition for the term “research and development”.

40 (c) REPORT.—The Secretary each year shall submit to the Committee on
41 Homeland Security of the House of Representatives and the Committee on

1 Homeland Security and Governmental Affairs of the Senate a classified and
2 unclassified report, as applicable, that lists each ongoing classified and un-
3 classified project at the Department, including all appropriate details of
4 each project.

5 (d) INDICATORS OF SUCCESS FOR TRANSITIONED PROJECTS.—

6 (1) IN GENERAL.—For each project that has been transitioned to
7 practice from research and development, the Under Secretary for
8 Science and Technology shall develop and track indicators to dem-
9 onstrate the uptake of the technology or project among customers or
10 end-users.

11 (2) PERIOD OF TRACKING.—To the fullest extent possible, the track-
12 ing of a project required under paragraph (1) shall continue for the
13 3-year period beginning on the date the project was transitioned to
14 practice from research and development.

15 (e) LIMITATION.—Nothing in this section overrides or otherwise affects
16 the requirements specified in section 10312 of this title.

17 **§ 10719. EMP and GMD mitigation research and develop-**
18 **ment**

19 (a) IN GENERAL.—In furtherance of domestic preparedness and response,
20 the Secretary, acting through the Under Secretary for Science and Tech-
21 nology, and in consultation with other relevant executive agencies, relevant
22 State, local, and tribal governments, and relevant owners and operators of
23 critical infrastructure, shall, to the extent practicable, conduct research and
24 development to mitigate the consequences of threats of EMP and GMD.

25 (b) SCOPE.—The scope of the research and development under subsection
26 (a) shall include the following:

27 (1) An objective scientific analysis evaluating the risks to critical in-
28 frastructure from a range of threats of EMP and GMD that shall—

29 (A) be conducted in conjunction with the Office of Intelligence
30 and Analysis; and

31 (B) include a review and comparison of the range of threats and
32 hazards facing critical infrastructure of the electrical grid.

33 (2) Determination of the critical utilities and national security assets
34 and infrastructure that are at risk from EMP and GMD.

35 (3) An evaluation of emergency planning and response technologies
36 that would address the findings and recommendations of experts, in-
37 cluding those of the Commission to Assess the Threat to the United
38 States from Electromagnetic Pulse Attack, which shall include a review
39 of the feasibility of rapidly isolating 1 or more portions of the electrical
40 grid from the main electrical grid.

1 (4) An analysis of technology options that are available to improve
 2 the resiliency of critical infrastructure to threats of EMP and GMD,
 3 including an analysis of neutral current blocking devices that may pro-
 4 tect high-voltage transmission lines.

5 (5) The restoration and recovery capabilities of critical infrastructure
 6 under different levels of damage and disruption from various threats
 7 of EMP and GMD, as informed by the scientific analysis conducted
 8 under paragraph (1).

9 (6) An analysis of the feasibility of a real-time alert system to inform
 10 electoral grid operators and other stakeholders within milliseconds of
 11 a high-altitude nuclear explosion.

12 (c) EXEMPTION FROM DISCLOSURE.—

13 (1) INFORMATION SHARED WITH FEDERAL GOVERNMENT.—Section
 14 10533 of this title, and any regulations issued pursuant to section
 15 10533 of this title, apply to any information shared with the Federal
 16 Government under this section.

17 (2) INFORMATION SHARED BY FEDERAL GOVERNMENT.—Informa-
 18 tion shared by the Federal Government with a State, local, or tribal
 19 government under this section is exempt from disclosure under any
 20 provision of State, local, or tribal freedom of information law, open gov-
 21 ernment law, open meetings law, open records law, sunshine law, or
 22 similar law requiring the disclosure of information or records.

23 **Chapter 109—Border, Maritime, and**
 24 **Transportation Security**

**Subchapter I—Border, Maritime, and Transportation Security Responsibil-
 ities and Functions**

Sec.

- 10901. Secretary.
- 10902. Commissioner of U.S. Customs and Border Protection.
- 10903. Limitation on reorganization of functions and units.
- 10904. Employee discipline.

Subchapter II—Customs and Border Protection

- 10911. Definition of customs revenue function.
- 10912. Retention of customs revenue functions by Secretary of the Treasury.
- 10913. Preservation of customs funds.
- 10914. Separate budget request for U.S. Customs and Border Protection.
- 10915. Allocation of resources by the Secretary.
- 10916. Methamphetamine and methamphetamine precursor chemicals.
- 10917. Polygraph and background examinations for law enforcement personnel of U.S. Customs and Border Protection
- 10918. Fees authorized for Advanced Training Center.
- 10919. Border security metrics.
- 10920. Trusted traveler program.
- 10921. Hiring members of the armed forces separating from military service.

Subchapter III—Immigration Enforcement Functions

- 10931. Transfer of functions.
- 10932. Responsibilities of U.S. Immigration and Customs Enforcement officials.
- 10933. Professional responsibility and quality review.
- 10934. Annual report on cross-border tunnels.

Subchapter IV—Citizenship and Immigration Services

- 10941. Transfer of functions to Director of U.S. Citizenship and Immigration Services.

- 10942. Responsibilities of U.S. Citizenship and Immigration Services officials.
- 10943. Citizenship and Immigration Services Ombudsman.
- 10944. Professional responsibility and quality review.
- 10945. Employee discipline.
- 10946. Transition.
- 10947. Application of Internet-based technologies.

Subchapter V—General Immigration Provisions

- 10961. Director of Shared Services.
- 10962. Separation of funding.
- 10963. Annual immigration functions report.

Subchapter VI—U.S. Customs and Border Protection Public-Private Partnerships

- 10971. Definitions.
- 10972. Fee agreements for certain services at ports of entry.
- 10973. Ports of entry donation authority.
- 10974. Current and proposed agreements.

Subchapter VII—Miscellaneous Provisions

- 10981. Coordination of information and information technology.
- 10982. Visa issuance.
- 10983. Information on visa denials required to be entered into electronic data system.
- 10984. Purpose and responsibilities of Office of Cargo Security Policy.
- 10985. Purpose, composition, and operation of Border Enforcement Security Task Force.
- 10986. Cyber Crimes Center.

1 **Subchapter I—Border, Maritime, and**
 2 **Transportation Security Responsibilities**
 3 **and Functions**

4 **§ 10901. Secretary**

5 (a) IN GENERAL.—The Secretary is responsible for the following:

6 (1) Preventing the entry of terrorists and the instruments of ter-
 7 rorism into the United States.

8 (2) Securing the borders, territorial waters, ports, terminals, water-
 9 ways, and air, land, and sea transportation systems of the United
 10 States, including managing and coordinating those functions trans-
 11 ferred to the Department at ports of entry.

12 (3) Carrying out the immigration enforcement functions vested by
 13 statute in, or performed by, the Commissioner of Immigration and Nat-
 14 uralization (or an officer, employee, or component of the Immigration
 15 and Naturalization Service) immediately before the date on which the
 16 transfer of functions specified under section 10931 of this title takes
 17 effect.

18 (4) Establishing and administering rules, under section 10982 of this
 19 title, governing the granting of visas or other forms of permission, in-
 20 cluding parole, to enter the United States to individuals who are not
 21 citizens or aliens lawfully admitted for permanent residence in the
 22 United States.

23 (5) Establishing national immigration enforcement policies and prior-
 24 ities.

25 (6) Except as provided in sections 10981 through 10985 of this title,
 26 administering the customs laws of the United States.

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 to the Federal Protective Service.

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 subsection (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 **§ 10902. 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 10901(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 10917(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); and

16 (18) carry out other duties and powers prescribed by law or dele-
17 gated by the Secretary.

18 (c) STANDARD OPERATING PROCEDURES.—

19 (1) IN GENERAL.—The Commissioner shall establish—

20 (A) standard operating procedures for searching, reviewing, re-
21 taining, and sharing information contained in communication,
22 electronic, or digital devices encountered by U.S. Customs and
23 Border Protection personnel at United States ports of entry;

24 (B) standard use of force procedures that officers and agents
25 of U.S. Customs and Border Protection may employ in the execu-
26 tion of their duties, including the use of deadly force;

27 (C) a uniform, standardized, and publicly available procedure
28 for processing and investigating complaints against officers,
29 agents, and employees of U.S. Customs and Border Protection for
30 violations of professional conduct, including the timely disposition
31 of complaints and a written notification to the complainant of the
32 status or outcome, as appropriate, of the related investigation, in
33 accordance with section 552a of title 5 (known as the “Privacy
34 Act” or the “Privacy Act of 1974”);

35 (D) an internal, uniform reporting mechanism regarding inci-
36 dents involving the use of deadly force by an officer or agent of
37 U.S. Customs and Border Protection, including an evaluation of
38 the degree to which the procedures required under subparagraph
39 (B) were followed; and

40 (E) standard operating procedures, acting through the Assistant
41 Commissioner for Air and Marine Operations and in coordination

1 with the Office for Civil Rights and Civil Liberties and the Office
2 of Privacy of the Department, to provide command, control, com-
3 munication, surveillance, and reconnaissance assistance through
4 the use of unmanned aerial systems, including the establishment
5 of—

6 (i) a process for other Federal, State, and local law en-
7 forcement agencies to submit mission requests;

8 (ii) a formal procedure to determine whether to approve or
9 deny a mission request;

10 (iii) a formal procedure to determine how mission requests
11 are prioritized and coordinated; and

12 (iv) a process regarding the protection and privacy of data
13 and images collected by U.S. Customs and Border Protection
14 through the use of unmanned aerial systems.

15 (2) REQUIREMENTS REGARDING CERTAIN NOTIFICATIONS.—The
16 standard operating procedures established pursuant to paragraph
17 (1)(A) shall require—

18 (A) in the case of a search of information conducted on an elec-
19 tronic device by U.S. Customs and Border Protection personnel,
20 the Commissioner to notify the individual subject to the search of
21 the purpose and authority for the search and how the individual
22 may obtain information on reporting concerns about the search;
23 and

24 (B) in the case of information collected by U.S. Customs and
25 Border Protection through a search of an electronic device, if the
26 information is transmitted to another Federal agency for subject
27 matter assistance, translation, or decryption, the Commissioner to
28 notify the individual subject to the search of the transmission.

29 (3) EXCEPTIONS.—The Commissioner may withhold the notifications
30 required under paragraphs (1)(C) and (2) if the Commissioner deter-
31 mines, in the sole and unreviewable discretion of the Commissioner,
32 that the notifications would impair national security, law enforcement,
33 or other operational interests.

34 (4) UPDATE AND REVIEW.—The Commissioner shall review and up-
35 date every 3 years the standard operating procedures required under
36 this subsection.

37 (5) AUDITS.—The Inspector General of the Department shall de-
38 velop and annually administer, during 2017, 2018, and 2019, an audit-
39 ing mechanism to review whether searches of electronic devices at or
40 between United States ports of entry are being conducted in conformity
41 with the standard operating procedures required under paragraph

1 (1)(A). Audits shall be submitted to the Committee on Homeland Secu-
2 rity of the House of Representatives and the Committee on Homeland
3 Security and Governmental Affairs of the Senate and shall include the
4 following:

5 (A) A description of the activities of officers and agents of U.S.
6 Customs and Border Protection with respect to the searches.

7 (B) The number of searches.

8 (C) The number of instances in which information contained in
9 devices that were subjected to searches was retained, copied,
10 shared, or entered in an electronic database.

11 (D) The number of devices detained as the result of searches.

12 (E) The number of instances in which information collected
13 from a device that was subjected to searches was transmitted to
14 another Federal agency, including whether the transmission re-
15 sulted in a prosecution or conviction.

16 (6) REQUIREMENTS REGARDING OTHER NOTIFICATIONS.—The
17 standard operating procedures established pursuant to paragraph
18 (1)(B) shall require—

19 (A) in the case of an incident of the use of deadly force by U.S.
20 Customs and Border Protection personnel, the Commissioner to
21 notify the Committee on Homeland Security of the House of Rep-
22 resentatives and the Committee on Homeland Security and Gov-
23 ernmental Affairs of the Senate; and

24 (B) the Commissioner to provide to those committees a copy of
25 the evaluation pursuant to paragraph (1)(D) not later than 30
26 days after completion of the evaluation.

27 (7) REPORT ON UNMANNED AERIAL SYSTEMS.—The Commissioner
28 shall submit to the Committee on Homeland Security of the House of
29 Representatives and the Committee on Homeland Security and Govern-
30 mental Affairs of the Senate, during 2017, 2018, and 2019, an annual
31 report that reviews whether the use of unmanned aerial systems is
32 being conducted in conformity with the standard operating procedures
33 required under paragraph (1)(E). The report—

34 (A) shall be submitted with the President's annual budget;

35 (B) may be submitted in classified form if the Commissioner de-
36 termines that it is appropriate; and

37 (C) shall include—

38 (i) a detailed description of how, where, and for how long
39 data and images collected through the use of unmanned aerial
40 systems by U.S. Customs and Border Protection are collected
41 and stored; and

1 (ii) a list of Federal, State, and local law enforcement
2 agencies that submitted mission requests in the previous year
3 and the disposition of the requests.

4 (d) TRAINING.—The Commissioner shall require all officers and agents
5 of U.S. Customs and Border Protection to participate in a specified amount
6 of continuing education (to be determined by the Commissioner) to maintain
7 an understanding of Federal legal rulings, court decisions, and departmental
8 policies, procedures, and guidelines.

9 (e) SHORT TERM DETENTION STANDARDS.—

10 (1) DEFINITION OF SHORT TERM DETENTION.—In this subsection,
11 the term “short term detention” means detention in a U.S. Customs
12 and Border Protection processing center for 72 hours or less, before
13 repatriation to a country of nationality or last habitual residence.

14 (2) ACCESS TO FOOD AND WATER.—The Commissioner shall make
15 every effort to ensure that adequate access to food and water is pro-
16 vided to an individual apprehended and detained at or between a
17 United States port of entry as soon as practicable following the time
18 of the apprehension or during subsequent short term detention.

19 (3) ACCESS TO INFORMATION ON DETAINEE RIGHTS AT BORDER PA-
20 TROL PROCESSING CENTERS.—

21 (A) IN GENERAL.—The Commissioner shall ensure that an indi-
22 vidual apprehended by a U.S. Border Patrol agent or an Office
23 of Field Operations officer is provided with information concerning
24 the individual’s rights, including the right to contact a representa-
25 tive of the individual’s government for purposes of United States
26 treaty obligations.

27 (B) HOW INFORMATION IS TO BE PROVIDED.—The information
28 referred to in subparagraph (A) may be provided either orally or
29 in writing, and shall be posted in the detention holding cell in
30 which the individual is being held. The information shall be pro-
31 vided in a language understandable to the individual.

32 (4) DAYTIME REPATRIATION.—When practicable, repatriations shall
33 be limited to daylight hours and avoid locations that are determined
34 to have high indices of crime and violence.

35 (5) REPORT ON PROCUREMENT PROCESS AND STANDARDS.—Not
36 later than 180 days after February 24, 2016, the Comptroller General
37 shall submit to the Committee on Homeland Security of the House of
38 Representatives and the Committee on Homeland Security and Govern-
39 mental Affairs of the Senate a report on the procurement process and
40 standards of entities with which U.S. Customs and Border Protection
41 has contracts for the transportation and detention of individuals appre-

1 hended by agents or officers of U.S. Customs and Border Protection.
2 The report should also consider the operational efficiency of contracting
3 the transportation and detention of those individuals.

4 (6) REPORT ON INSPECTIONS OF SHORT TERM CUSTODY FACILI-
5 TIES.—The Commissioner shall—

6 (A) annually inspect all facilities utilized for short term deten-
7 tion; and

8 (B) make publicly available information collected pursuant to
9 the inspections, including information regarding the requirements
10 under paragraphs (2) and (3), and, where appropriate, issue rec-
11 ommendations to improve the conditions of the facilities.

12 (f) WAIT TIMES TRANSPARENCY.—

13 (1) IN GENERAL.—The Commissioner shall—

14 (A) publish live wait times at the 20 United States airports that
15 support the highest volume of international travel (as determined
16 by available Federal flight data);

17 (B) make information about the wait times available to the pub-
18 lic in real time through the U.S. Customs and Border Protection
19 website;

20 (C) submit to the Committee on Homeland Security of the
21 House of Representatives and the Committee on Homeland Secu-
22 rity and Governmental Affairs of the Senate, during 2017, 2018,
23 2019, 2020, and 2021, a report that includes compilations of all
24 those wait times and a ranking of those United States airports by
25 wait times; and

26 (D) provide adequate staffing at the U.S. Customs and Border
27 Protection information center to ensure timely access for travelers
28 attempting to submit comments or speak with a representative
29 about their entry experiences.

30 (2) CALCULATION.—The wait times referred to in paragraph (1)(A)
31 shall be determined by calculating the time elapsed between an individ-
32 ual's entry into the U.S. Customs and Border Protection inspection
33 area and the individual's clearance by a U.S. Customs and Border Pro-
34 tection officer.

35 (g) CONTINUED SUBMISSION OF REPORTS TO COMMITTEES.—The Com-
36 mission shall continue to submit to the Committee on Homeland Security
37 and the Committee on Ways and Means of the House of Representatives
38 and the Committee on Homeland Security and Governmental Affairs and
39 the Committee on Finance of the Senate any report required to be sub-
40 mitted on February 23, 2016, under any provision of law.

1 (h) AUTHORITY OF OTHER FEDERAL AGENCIES NOT AFFECTED.—Noth-
2 ing in this section may be construed as affecting in any manner the author-
3 ity, which existed on February 23, 2016, of any other Federal agency or
4 component of the Department.

5 **§ 10903. Limitation on reorganization of functions and units**

6 The authority provided by section 1502 of the Homeland Security Act of
7 2002 (Public Law 107–296, 116 Stat. 2308) may be used to reorganize
8 functions or organizational units in U.S. Immigration and Customs Enforce-
9 ment or U. S. Citizenship and Immigration Services, but may not be used
10 to recombine U.S. Immigration and Customs Enforcement and U.S. Citizen-
11 ship and Immigration Services into a single agency or otherwise to combine,
12 join, or consolidate functions or organizational units of U.S. Immigration
13 and Customs Enforcement and U.S. Citizenship and Immigration Services
14 with each other.

15 **§ 10904. Employee discipline**

16 The Secretary may impose disciplinary action on an employee of U.S. Im-
17 migration and Customs Enforcement and U.S. Customs and Border Protec-
18 tion who willfully deceives Congress or agency leadership on any matter.

19 **Subchapter II—Customs and Border**
20 **Protection**

21 **§ 10911. Definition of customs revenue function**

22 In this subchapter, the term “customs revenue function” means the fol-
23 lowing:

24 (1) Assessing and collecting customs duties (including antidumping
25 and countervailing duties and duties imposed under safeguard provi-
26 sions), excise taxes, fees, and penalties due on imported merchandise,
27 including classifying and valuing merchandise for purposes of assess-
28 ment.

29 (2) Processing and denial of entry of persons, baggage, cargo, and
30 mail, with respect to the assessment and collection of import duties.

31 (3) Detecting and apprehending persons engaged in fraudulent prac-
32 tices designed to circumvent the customs laws of the United States.

33 (4) Enforcing section 337 of the Tariff Act of 1930 (19 U.S.C.
34 1337) and provisions relating to import quotas and the marking of im-
35 ported merchandise, and providing Customs Recordations for copy-
36 rights, patents, and trademarks.

37 (5) Collecting accurate import data for compilation of international
38 trade statistics.

39 (6) Enforcing reciprocal trade agreements.

1 (7) Functions performed by the following personnel, and associated
 2 support staff, of U. S. Customs and Border Protection on January 23,
 3 2003:

4 (A) Import Specialists.

5 (B) Entry Specialists.

6 (C) Drawback Specialists.

7 (D) National Import Specialists.

8 (E) Fines and Penalties Specialists.

9 (F) Attorneys of the Office of Regulations and Rulings.

10 (G) Customs Auditors.

11 (H) International Trade Specialists.

12 (I) Financial Systems Specialists.

13 (8) Functions performed by the following offices, with respect to any
 14 function described in any of paragraphs (1) through (7), and associated
 15 support staff, of the United States Customs Service on January 23,
 16 2003, and of U.S. Customs and Border Protection on February 23,
 17 2016:

18 (A) Office of Information and Technology.

19 (B) Office of Laboratory Services.

20 (C) Office of the Chief Counsel.

21 (D) Office of Congressional Affairs.

22 (E) Office of International Affairs.

23 (F) Office of Training and Development.

24 **§ 10912. Retention of customs revenue functions by Sec-**
 25 **retary of the Treasury**

26 (a) RETENTION OF CUSTOMS REVENUE FUNCTIONS BY SECRETARY OF
 27 THE TREASURY.—

28 (1) RETENTION OF AUTHORITY.—Notwithstanding section
 29 10901(b)(1) of this title, authority relating to customs revenue func-
 30 tions that was vested in the Secretary of the Treasury by law before
 31 January 24, 2003, under those provisions of law set forth in paragraph
 32 (2) shall not be transferred to the Secretary by reason of the Homeland
 33 Security Act of 2002 (Public Law 107–296, 116 Stat. 2135) and, on
 34 and after January 24, 2004, the Secretary of the Treasury may dele-
 35 gate that authority to the Secretary at the discretion of the Secretary
 36 of the Treasury. The Secretary of the Treasury shall consult with the
 37 Secretary regarding the exercise of authority not delegated to the Sec-
 38 retary.

39 (2) STATUTES.—The provisions of law referred to in paragraph (1)
 40 are the following:

1 (A) Section 249 of the Revised Statutes of the United States
2 (19 U.S.C. 3).

3 (B) Section 2 of the Act of March 4, 1923 (19 U.S.C. 6).

4 (C) Section 13031 of the Consolidated Omnibus Budget Rec-
5 onciliation Act of 1985 (19 U.S.C. 58e).

6 (D) Section 251 of the Revised Statutes of the United States
7 (19 U.S.C. 66).

8 (E) Section 1 of the Act of June 26, 1930 (19 U.S.C. 68).

9 (F) The Act of June 18, 1934 (known as the “Foreign Trade
10 Zones Act”) (19 U.S.C. 81a et seq.).

11 (G) Section 1 of the Act of March 2, 1911 (19 U.S.C. 198).

12 (H) The Tariff Act of 1930 (19 U.S.C. 1202 et seq.).

13 (I) The Trade Act of 1974 (19 U.S.C. 2101 et seq.).

14 (J) The Trade Agreements Act of 1979 (19 U.S.C. 2501 et
15 seq.).

16 (K) The Caribbean Basin Economic Recovery Act (19 U.S.C.
17 2701 et seq.).

18 (L) The Andean Trade Preference Act (19 U.S.C. 3201 et seq.).

19 (M) The North American Free Trade Agreement Implementa-
20 tion Act (19 U.S.C. 3311 et seq.).

21 (N) The Uruguay Round Agreements Act (19 U.S.C. 3501 et
22 seq.).

23 (O) The African Growth and Opportunity Act (19 U.S.C. 3701
24 et seq.).

25 (P) Any other provision of law vesting customs revenue func-
26 tions in the Secretary of the Treasury.

27 (b) MAINTENANCE OF CUSTOMS REVENUE FUNCTIONS.—

28 (1) MAINTENANCE OF FUNCTIONS.—Notwithstanding any other pro-
29 vision of this subtitle, the Secretary may not consolidate, discontinue,
30 or diminish those functions described in paragraph (2) performed by
31 U.S. Customs and Border Protection on or after January 24, 2003, re-
32 duce the staffing level, or reduce the resources attributable to the func-
33 tions, and the Secretary shall ensure that an appropriate management
34 structure is implemented to carry out the functions.

35 (2) FUNCTIONS.—The functions referred to in paragraph (1) are
36 those functions performed by the following personnel, and associated
37 support staff, of U. S. Customs and Border Protection on January 23,
38 2003:

39 (A) Import Specialists.

40 (B) Entry Specialists.

41 (C) Drawback Specialists.

- 1 (D) National Import Specialists.
- 2 (E) Fines and Penalties Specialists.
- 3 (F) Attorneys of the Office of Regulations and Rulings.
- 4 (G) Customs Auditors.
- 5 (H) International Trade Specialists.
- 6 (I) Financial Systems Specialists.

7 (e) NEW PERSONNEL.—The Secretary of the Treasury may appoint up
8 to 20 new personnel to work with personnel of the Department in per-
9 forming customs revenue functions.

10 **§ 10913. Preservation of customs funds**

11 Notwithstanding any other provision of this subtitle, no funds collected
12 under section 13031(a) (1) through (8) of the Consolidated Omnibus Budg-
13 et Reconciliation Act of 1985 (19 U.S.C. 58c(a)(1) through (8)) may be
14 transferred for use by another agency or office in the Department.

15 **§ 10914. Separate budget request for U.S. Customs and Bor-**
16 **der Protection**

17 (a) IN GENERAL.—The President shall include in each budget trans-
18 mitted to Congress under section 1105 of title 31 a separate budget request
19 for U.S. Customs and Border Protection.

20 (b) FIVE-YEAR PLAN FOR LAND BORDER PORT OF ENTRY PROJECTS.—
21 The annual budget submission of U. S. Customs and Border Protection for
22 “Construction and Facilities Management” shall, in consultation with the
23 General Services Administration, include a detailed 5-year plan for all Fed-
24 eral land border port-of-entry projects, with a yearly update of total pro-
25 jected future funding needs delineated by Federal land border port of entry.

26 **§ 10915. Allocation of resources by the Secretary**

27 (a) DEFINITION OF CUSTOMS REVENUE SERVICES.—In this section, the
28 term “customs revenue services” means those customs revenue functions de-
29 scribed in section 10911(1) through (6) and (8) of this title.

30 (b) IN GENERAL.—The Secretary shall ensure that adequate staffing is
31 provided to ensure that levels of customs revenue services provided on Janu-
32 ary 23, 2003, shall continue to be provided.

33 (c) NOTIFICATION OF CONGRESS.—The Secretary shall notify the Com-
34 mittee on Ways and Means of the House of Representatives and the Com-
35 mittee on Finance of the Senate at least 90 days prior to taking an action
36 that would—

37 (1) result in a significant reduction in customs revenue services, in-
38 cluding hours of operation, provided at an office within the Department
39 or a port of entry;

40 (2) eliminate or relocate an office of the Department that provides
41 customs revenue services; or

1 (3) eliminate a port of entry.

2 **§ 10916. Methamphetamine and methamphetamine pre-**
3 **cursor chemicals**

4 (a) DEFINITION OF METHAMPHETAMINE PRECURSOR CHEMICALS.—In
5 this section, the term “methamphetamine precursor chemicals” means the
6 chemicals ephedrine, pseudoephedrine, or phenylpropanolamine, including
7 each of the salts, optical isomers, and salts of optical isomers of the chemi-
8 cals.

9 (b) COMPLIANCE WITH PERFORMANCE PLAN REQUIREMENTS.—As part
10 of the annual performance plan required in the budget submission of U.S.
11 Customs and Border Protection under section 1115 of title 31, the Commis-
12 sioner shall establish performance indicators relating to the seizure of meth-
13 amphetamine and methamphetamine precursor chemicals in order to evalu-
14 ate the performance goals of U.S. Customs and Border Protection with re-
15 spect to the interdiction of illegal drugs entering the United States.

16 (c) STUDY AND REPORT RELATING TO METHAMPHETAMINE AND METH-
17 AMPHETAMINE PRECURSOR CHEMICALS.—

18 (1) ANALYSIS.—The Commissioner shall, on an ongoing basis, ana-
19 lyze the movement of methamphetamine and methamphetamine pre-
20 cursor chemicals into the United States. In conducting the analysis, the
21 Commissioner shall—

22 (A) consider the entry of methamphetamine and methamphet-
23 amine precursor chemicals through ports of entry, between ports
24 of entry, through international mails, and through international
25 courier services;

26 (B) examine the export procedures of each foreign country
27 where the shipments of methamphetamine and methamphetamine
28 precursor chemicals originate and determine if changes in the
29 country’s customs overtime provisions would alleviate the export of
30 methamphetamine and methamphetamine precursor chemicals;
31 and

32 (C) identify emerging trends in smuggling techniques and strat-
33 egies.

34 (2) REPORT.—Not later than September 30 of each odd-numbered
35 year, the Commissioner, in consultation with the Attorney General,
36 United States Immigration and Customs Enforcement, the United
37 States Drug Enforcement Administration, and the United States De-
38 partment of State, shall submit a report to the Committee on Finance
39 of the Senate, the Committee on Foreign Relations of the Senate, the
40 Committee on the Judiciary of the Senate, the Committee on Ways and
41 Means of the House of Representatives, the Committee on Foreign Af-

1 fairs of the House of Representatives, and the Committee on the Judi-
2 ciary of the House of Representatives, that includes—

3 (A) a comprehensive summary of the analysis described in para-
4 graph (1); and

5 (B) a description of how U.S. Customs and Border Protection
6 utilized the analysis described in paragraph (1) to target ship-
7 ments presenting a high risk for smuggling or circumvention of
8 the Combat Methamphetamine Epidemic Act of 2005 (Public Law
9 109–177, title VII, 120 Stat. 256).

10 (3) AVAILABILITY OF ANALYSIS.—The Commissioner shall ensure
11 that the analysis described in paragraph (1) is made available in a
12 timely manner to the Secretary of State to facilitate the Secretary in
13 fulfilling the Secretary’s reporting requirements in section 722 of the
14 Combat Methamphetamine Epidemic Act of 2005 (Public Law 109–
15 177, title VII, 120 Stat. 268).

16 **§ 10917. Polygraph and background examinations for law**
17 **enforcement personnel of U.S. Customs and Bor-**
18 **der Protection**

19 (a) IN GENERAL.—The Secretary shall ensure that—

20 (1) all applicants for law enforcement positions with U.S. Customs
21 and Border Protection (except as provided in subsection (b)) receive
22 polygraph examinations before being hired for a position; and

23 (2) U.S. Customs and Border Protection initiates all periodic back-
24 ground reinvestigations for all law enforcement personnel of U.S. Cus-
25 toms and Border Protection who should receive periodic background re-
26 investigations pursuant to relevant policies of U.S. Customs and Bor-
27 der Protection in effect on January 3, 2011.

28 (b) WAIVER.—The Commissioner of U.S. Customs and Border Protection
29 may waive the polygraph examination requirement under subsection (a)(1)
30 for any applicant who—

31 (1) is considered suitable for employment;

32 (2) holds a current, active Top Secret/Sensitive Compartmented In-
33 formation Clearance;

34 (3) has a current Single Scope Background Investigation;

35 (4) was not granted any waivers to obtain his or her clearance; and

36 (5) is a veteran (as defined in section 2108 of title 5).

37 **§ 10918. Fees authorized for Advanced Training Center**

38 U.S. Customs and Border Protection’s Advanced Training Center may
39 charge fees for a service and/or thing of value it provides to Federal Govern-
40 ment or non-government entities or individuals, so long as the fees charged
41 do not exceed the full costs associated with the service or thing of value pro-

1 vided. Notwithstanding 31 U.S.C. 3302(b), fees collected by the Advanced
2 Training Center—

3 (1) shall be deposited in a separate account entitled “Advanced
4 Training Center Revolving Fund;

5 (2) are available, without further appropriations, for necessary ex-
6 penses of the Advanced Training Center program; and

7 (3) remain available until expended.

8 **§ 10919. Border security metrics**

9 (a) DEFINITIONS.—In this section:

10 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appro-
11 priate congressional committees” means—

12 (A) the Committee on Homeland Security and Governmental
13 Affairs of the Senate; and

14 (B) the Committee on Homeland Security of the House of Rep-
15 resentatives.

16 (2) CONSEQUENCE DELIVERY SYSTEM.—The term “Consequence De-
17 livery System” means the series of consequences applied by the U.S.
18 Border Patrol in collaboration with other Federal agencies to individ-
19 uals unlawfully entering the United States, to prevent unlawful border
20 crossing recidivism.

21 (3) GOT AWAY.—The term “got away” means an unlawful border
22 crosser who—

23 (A) is directly or indirectly observed making an unlawful entry
24 into the United States;

25 (B) is not apprehended; and

26 (C) is not a turn back.

27 (4) KNOWN MARITIME MIGRANT FLOW.—The term “known maritime
28 migrant flow” means the sum of the number of undocumented mi-
29 grants—

30 (A) interdicted in the waters over which the United States has
31 jurisdiction;

32 (B) identified at sea either directly or indirectly, but not inter-
33 dicted; or

34 (C) if not described in subparagraph (A) or (B), who were oth-
35 erwise reported, with a significant degree of certainty, as having
36 entered, or attempted to enter, the United States through the
37 maritime border.

38 (5) MAJOR VIOLATOR.—The term “major violator” means a person
39 or entity that has engaged in serious criminal activities at any land,
40 air, or sea port of entry, including the following:

41 (A) Possession of illicit drugs.

- 1 (B) Smuggling of prohibited products.
- 2 (C) Human smuggling.
- 3 (D) Possession of illegal weapons.
- 4 (E) Use of fraudulent documents.
- 5 (F) Any other offense that is serious enough to result in an ar-
- 6 rest.

7 (6) SITUATIONAL AWARENESS.—The term “situational awareness”
8 means knowledge and understanding of current unlawful cross-border
9 activity, including the following:

- 10 (A) Threats and trends concerning illicit trafficking and unlaw-
11 ful crossings.
- 12 (B) The ability to forecast future shifts in those threats and
13 trends.
- 14 (C) The ability to evaluate those threats and trends at a level
15 sufficient to create actionable plans.
- 16 (D) The operational capability to conduct persistent and inte-
17 grated surveillance of the international borders of the United
18 States.

19 (7) TRANSIT ZONE.—The term “transit zone” means the sea cor-
20 ridors of the western Atlantic Ocean, the Gulf of Mexico, the Caribbean
21 Sea, and the eastern Pacific Ocean through which undocumented mi-
22 grants and illicit drugs transit, either directly or indirectly, to the
23 United States.

24 (8) TURN BACK.—The term “turn back” means an unlawful border
25 crosser who, after making an unlawful entry into the United States,
26 responds to United States enforcement efforts by returning promptly
27 to the country from which the crosser entered.

28 (9) UNLAWFUL BORDER CROSSING EFFECTIVENESS RATE.—The
29 term “unlawful border crossing effectiveness rate” means the percent-
30 age that results from dividing the number of apprehensions and turn
31 backs by the sum of the number of apprehensions, estimated unde-
32 tected unlawful entries, turn backs, and got aways.

33 (10) UNLAWFUL ENTRY.—The term “unlawful entry” means an un-
34 lawful border crosser who enters the United States and is not appre-
35 hended by a border security component of the Department.

36 (b) METRICS FOR SECURING THE BORDER BETWEEN PORTS OF
37 ENTRY.—

38 (1) IN GENERAL.—Not later than 180 days after December 23,
39 2016, the Secretary shall develop metrics, informed by situational
40 awareness, to measure the effectiveness of security between ports of

1 entry. The Secretary shall annually implement the metrics developed
2 under this subsection, which shall include the following:

3 (A) Estimates, using alternative methodologies where appro-
4 priate, including recidivism data, survey data, known-flow data,
5 and technologically measured data, of the following:

6 (i) The rate of apprehension of attempted unlawful border
7 crossers.

8 (ii) The number of detected unlawful entries.

9 (iii) The number of estimated undetected unlawful entries.

10 (iv) Turn backs.

11 (v) Got aways.

12 (B) A measurement of situational awareness achieved in each
13 U.S. Border Patrol sector.

14 (C) An unlawful border crossing effectiveness rate in each U.S.
15 Border Patrol sector.

16 (D) A probability of detection rate, which compares the esti-
17 mated total unlawful border crossing attempts not detected by
18 U.S. Border Patrol to the unlawful border crossing effectiveness
19 rate under subparagraph (C), as informed by subparagraph (A).

20 (E) The number of apprehensions in each U.S. Border Patrol
21 sector.

22 (F) The number of apprehensions of unaccompanied alien chil-
23 dren, and the nationality of the children, in each U.S. Border Pa-
24 trol sector.

25 (G) The number of apprehensions of family units, and the na-
26 tionality of the family units, in each U.S. Border Patrol sector.

27 (H) An illicit drugs seizure rate for drugs seized by the U.S.
28 Border Patrol between ports of entry, which compares the ratio
29 of the amount and type of illicit drugs seized between ports of
30 entry in any fiscal year to the average of the amount and type of
31 illicit drugs seized between ports of entry in the immediately pre-
32 ceding 5 fiscal years.

33 (I) Estimates of the impact of the Consequence Delivery System
34 on the rate of recidivism of unlawful border crossers over multiple
35 fiscal years.

36 (J) An examination of each consequence under the Consequence
37 Delivery System referred to in subparagraph (I), including the fol-
38 lowing:

39 (i) Voluntary return.

40 (ii) Warrant of arrest or notice to appear.

41 (iii) Expedited removal.

- 1 (iv) Reinstatement of removal.
- 2 (v) Alien transfer exit program.
- 3 (vi) Criminal consequence program.
- 4 (vii) Standard prosecution.
- 5 (viii) Operation Against Smugglers Initiative on Safety and
- 6 Security.

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) where appropriate, consult with the heads of other agencies,
13 including the Office of Refugee Resettlement of the Department
14 of Health and Human Services and the Executive Office for Immi-
15 gration Review of the Department of Justice.

16 (3) MANNER OF COLLECTION.—The data collected to inform the
17 metrics developed in accordance with paragraph (1) shall be collected
18 and reported in a consistent and standardized manner across all U.S.
19 Border Patrol sectors, informed by situational awareness.

20 (e) METRICS FOR SECURING THE BORDER AT PORTS OF ENTRY.—

21 (1) IN GENERAL.— Not later than 180 days after December 23,
22 2016, the Secretary shall develop metrics, informed by situational
23 awareness, to measure the effectiveness of security at ports of entry.
24 The Secretary shall annually implement the metrics developed under
25 this subsection, which shall include the following:

26 (A) Estimates, using alternative methodologies where appro-
27 priate, including recidivism data, survey data, and randomized sec-
28 ondary screening data, of the following:

29 (i) Total inadmissible travelers who attempt to, or success-
30 fully, enter the United States at a port of entry.

31 (ii) The rate of refusals and interdictions for travelers who
32 attempt to, or successfully, enter the United States at a port
33 of entry.

34 (iii) The number of unlawful entries at a port of entry.

35 (B) The amount and type of illicit drugs seized by the Office
36 of Field Operations of U.S. Customs and Border Protection at
37 ports of entry during the previous fiscal year.

38 (C) An illicit drugs seizure rate for drugs seized by the Office
39 of Field Operations, which compares the ratio of the amount and
40 type of illicit drugs seized by the Office of Field Operations in any
41 fiscal year to the average of the amount and type of illicit drugs

1 seized by the Office of Field Operations in the immediately pre-
2 ceding 5 fiscal years.

3 (D) The number of infractions related to travelers and cargo
4 committed by major violators who are interdicted by the Office of
5 Field Operations at ports of entry, and the estimated number of
6 those infractions committed by major violators who are not so
7 interdicted.

8 (E) In consultation with the heads of the Office of National
9 Drug Control Policy and the United States Southern Command,
10 a cocaine seizure effectiveness rate, which is the percentage result-
11 ing from dividing the amount of cocaine seized by the Office of
12 Field Operations by the total estimated cocaine flow rate at ports
13 of entry along the United States land border with Mexico and
14 Canada.

15 (F) A measurement of how border security operations affect
16 crossing times, including the following:

17 (i) A wait time ratio that compares the average wait times
18 to total commercial and private vehicular traffic volumes at
19 each land port of entry.

20 (ii) An infrastructure capacity utilization rate that meas-
21 ures traffic volume against the physical and staffing capacity
22 at each land port of entry.

23 (iii) A secondary examination rate that measures the fre-
24 quency of secondary examinations at each land port of entry.

25 (iv) An enforcement rate that measures the effectiveness of
26 the secondary examinations at detecting major violators.

27 (G) A seaport scanning rate that includes the following:

28 (i) The number of all cargo containers that are considered
29 potentially high-risk, as determined by the Executive Assist-
30 ant Commissioner of the Office of Field Operations.

31 (ii) A comparison of the number of potentially high-risk
32 cargo containers scanned by the Office of Field Operations at
33 each sea port of entry during a fiscal year to the total num-
34 ber of high-risk cargo containers entering the United States
35 at each such sea port of entry during the previous fiscal year.

36 (iii) The number of potentially high-risk cargo containers
37 scanned on arrival at a United States sea port of entry.

38 (iv) The number of potentially high-risk cargo containers
39 scanned before arrival at a United States sea port of entry.

1 (2) METRICS CONSULTATION.—To ensure that authoritative data
2 sources are utilized in the development of the metrics described in
3 paragraph (1), the Secretary shall—

4 (A) consult with the heads of the appropriate components of the
5 Department; and

6 (B) where appropriate, work with heads of other appropriate
7 agencies, including the Office of Refugee Resettlement of the De-
8 partment of Health and Human Services and the Executive Office
9 for Immigration Review of the Department of Justice.

10 (3) MANNER OF COLLECTION.—The data collected to inform the
11 metrics developed in accordance with paragraph (1) shall be collected
12 and reported in a consistent and standardized manner across all United
13 States ports of entry, informed by situational awareness.

14 (d) METRICS FOR SECURING THE MARITIME BORDER.—

15 (1) IN GENERAL.— Not later than 180 days after December 23,
16 2016, the Secretary shall develop metrics, informed by situational
17 awareness, to measure the effectiveness of security in the maritime en-
18 vironment. The Secretary shall annually implement the metrics devel-
19 oped under this subsection, which shall include the following:

20 (A) Situational awareness achieved in the maritime environ-
21 ment.

22 (B) A known maritime migrant flow rate.

23 (C) An illicit drugs removal rate for drugs removed inside and
24 outside of a transit zone, which compares the amount and type of
25 illicit drugs removed, including drugs abandoned at sea, by the
26 maritime security components of the Department of Homeland Se-
27 curity in any fiscal year to the average of the amount and type
28 of illicit drugs removed by the maritime components for the imme-
29 diately preceding 5 fiscal years.

30 (D) In consultation with the heads of the Office of National
31 Drug Control Policy and the United States Southern Command,
32 a cocaine removal effectiveness rate for cocaine removed inside a
33 transit zone and outside a transit zone, which compares the
34 amount of cocaine removed by the maritime security components
35 of the Department of Homeland Security to the total documented
36 cocaine flow rate, as contained in Federal drug databases.

37 (E) A response rate, which compares the ability of the maritime
38 security components of the Department of Homeland Security to
39 respond to and resolve known maritime threats, whether inside or
40 outside a transit zone, by placing assets on-scene, to the total

1 number of events with respect to which the Department has
2 known threat information.

3 (F) An intergovernmental response rate, which compares the
4 ability of the maritime security components of the Department or
5 other United States Government entities to respond to and resolve
6 actionable maritime threats, whether inside or outside a transit
7 zone, with the number of those threats detected.

8 (2) METRICS CONSULTATION.—To ensure that authoritative data
9 sources are utilized in the development of the metrics described in
10 paragraph (1), the Secretary shall—

11 (A) consult with the heads of the appropriate components of the
12 Department; and

13 (B) where appropriate, work with the heads of other agencies,
14 including the Drug Enforcement Agency, the Department of De-
15 fense, and the Department of Justice.

16 (3) METHODS OF COLLECTION.—The data used by the Secretary
17 shall be collected and reported in a consistent and standardized manner
18 by the maritime security components of the Department, informed by
19 situational awareness.

20 (e) AIR AND MARINE SECURITY METRICS IN THE LAND DOMAIN.—

21 (1) IN GENERAL.—Not later than 180 days after December 23,
22 2016, the Secretary shall develop metrics, informed by situational
23 awareness, to measure the effectiveness of the aviation assets and oper-
24 ations of Air and Marine Operations of U.S. Customs and Border Pro-
25 tection. The Secretary shall annually implement the metrics developed
26 under this subsection, which shall include the following:

27 (A) A flight hour effectiveness rate, which compares Air and
28 Marine Operations flight hours requirements to the number of
29 flight hours flown by Air and Marine Operations.

30 (B) A funded flight hour effectiveness rate, which compares the
31 number of funded flight hours appropriated to Air and Marine Op-
32 erations to the number of actual flight hours flown by Air and Ma-
33 rine Operations.

34 (C) A readiness rate, which compares the number of aviation
35 missions flown by Air and Marine Operations to the number of
36 aviation missions cancelled by Air and Marine Operations due to
37 maintenance, operations, or other causes.

38 (D) The number of missions cancelled by Air and Marine Oper-
39 ations due to weather compared to the total planned missions.

1 (E) The number of individuals detected by Air and Marine Op-
2 erations through the use of unmanned aerial systems and manned
3 aircraft.

4 (F) The number of apprehensions assisted by Air and Marine
5 Operations through the use of unmanned aerial systems and
6 manned aircraft.

7 (G) The number and quantity of illicit drug seizures assisted by
8 Air and Marine Operations through the use of unmanned aerial
9 systems and manned aircraft.

10 (H) The number of times that actionable intelligence related to
11 border security was obtained through the use of unmanned aerial
12 systems and manned aircraft.

13 (2) METRICS CONSULTATION.—To ensure that authoritative data
14 sources are utilized in the development of the metrics described in
15 paragraph (1), the Secretary shall—

16 (A) consult with the heads of the appropriate components of the
17 Department; and

18 (B) as appropriate, work with the heads of other departments
19 and agencies, including the Department of Justice.

20 (3) MANNER OF COLLECTION.—The data collected to inform the
21 metrics developed in accordance with paragraph (1) shall be collected
22 and reported in a consistent and standardized manner by Air and Ma-
23 rine Operations, informed by situational awareness.

24 (f) DATA TRANSPARENCY.—The Secretary shall—

25 (1) in accordance with applicable privacy laws, make data relating
26 to apprehensions, inadmissible aliens, drug seizures, and other enforce-
27 ment actions available to the public, law enforcement communities, and
28 academic research communities; and

29 (2) provide the Office of Immigration Statistics of the Department
30 with unfettered access to the data referred to in paragraph (1).

31 (g) EVALUATIONS BY GOVERNMENT ACCOUNTABILITY OFFICE AND SEC-
32 RETARY.—

33 (1) METRIC REPORT.—

34 (A) MANDATORY DISCLOSURES.—The Secretary shall submit to
35 the appropriate congressional committees and the Comptroller
36 General an annual report containing the metrics required under
37 this section and the data and methodology used to develop the
38 metrics.

39 (B) PERMISSIBLE DISCLOSURES.—The Secretary, for the pur-
40 pose of validation and verification, may submit the annual report
41 described in subparagraph (A) to—

1 (i) the Center for Borders, Trade, and Immigration Re-
2 search of the Centers of Excellence network of the Depart-
3 ment;

4 (ii) the head of a national laboratory in the Department
5 laboratory network with prior expertise in border security;
6 and

7 (iii) a federally funded research and development center.

8 (2) GOVERNMENT ACCOUNTABILITY OFFICE REPORT.—Not later
9 than 270 days after receiving the first report under paragraph (1)(A)
10 and biennially thereafter for the following 10 years with respect to
11 every other report, the Comptroller General shall submit to the appro-
12 priate congressional committees a report that—

13 (A) analyzes the suitability and statistical validity of the data
14 and methodology contained in each report; and

15 (B) includes recommendations on—

16 (i) the feasibility of other suitable metrics that may be used
17 to measure the effectiveness of border security; and

18 (ii) improvements that need to be made to the metrics
19 being used to measure the effectiveness of border security.

20 (3) STATE OF THE BORDER REPORT.—Not later than 60 days after
21 the end of each fiscal year through fiscal year 2026, the Secretary shall
22 submit to the appropriate congressional committees a State of the Bor-
23 der report that—

24 (A) provides trends for each metric under this section for the
25 last 10 fiscal years, to the greatest extent possible;

26 (B) provides selected analysis into related aspects of illegal flow
27 rates, including undocumented migrant flows and stock estimation
28 techniques;

29 (C) provides selected analysis into related aspects of legal flow
30 rates; and

31 (D) includes any other information that the Secretary deter-
32 mines appropriate.

33 (4) METRICS UPDATE.—

34 (A) IN GENERAL.—After submitting the 10th report to the
35 Comptroller General under paragraph (1), the Secretary may re-
36 evaluate and update any of the metrics developed in accordance
37 with this section to ensure that the metrics are suitable to meas-
38 ure the effectiveness of border security.

39 (B) CONGRESSIONAL NOTIFICATION.—Not later than 30 days
40 before updating the metrics pursuant to subparagraph (A), the

1 Secretary shall notify the appropriate congressional committees of
2 the updates.

3 **§ 10920. Trusted traveler program**

4 The Secretary may not enter into or renew an agreement with the govern-
5 ment of a foreign country for a trusted traveler program administered by
6 U.S. Customs and Border Protection unless the Secretary certifies in writ-
7 ing that the government—

8 (1) routinely submits to INTERPOL for inclusion in INTERPOL's
9 Stolen and Lost Travel Documents database information about lost and
10 stolen passports and travel documents of the citizens and nationals of
11 the country; or

12 (2) makes available to the United States Government the informa-
13 tion described in paragraph (1) through another means of reporting.

14 **§ 10921. Hiring members of the armed forces separating**
15 **from military service**

16 (a) EXPEDITED HIRING.—The Secretary shall consider the expedited hir-
17 ing of qualified candidates who have the ability to perform the essential
18 functions of the position of a U.S. Customs and Border Protection officer
19 and who are eligible for a veterans recruitment appointment authorized
20 under section 4214 of title 38.

21 (b) ENHANCED RECRUITING EFFORTS.—The Secretary, in consultation
22 with the Secretary of Defense, and acting through existing programs, au-
23 thorities, and agreements, where applicable, shall enhance the efforts of the
24 Department to recruit members of the armed forces who are separating
25 from military service to serve as U.S. Customs and Border Protection offi-
26 cers. The enhanced recruiting efforts shall—

27 (1) include U.S. Customs and Border Protection officer opportunities
28 in relevant job assistance efforts under the Transition Assistance Pro-
29 gram;

30 (2) place U.S. Customs and Border Protection officials or other rel-
31 evant Department officials at recruiting events and jobs fairs involving
32 members of the armed forces who are separating from military service;

33 (3) provide opportunities for local U.S. Customs and Border Protec-
34 tion field offices to partner with military bases in the region;

35 (4) include outreach efforts to educate members of the armed forces
36 with Military Occupational Specialty Codes and Officer Branches, Air
37 Force Specialty Codes, Naval Enlisted Classifications and Officer Des-
38 ignators, and Coast Guard competencies that are transferable to the re-
39 quirements, qualifications, and duties assigned to U.S. Customs and
40 Border Protection officers of available hiring opportunities to become
41 U.S. Customs and Border Protection officers;

1 (5) identify shared activities and opportunities for reciprocity related
2 to steps in hiring U.S. Customs and Border Protection officers with the
3 goal of minimizing the time required to hire qualified applicants;

4 (6) ensure the streamlined interagency transfer of relevant back-
5 ground investigations and security clearances; and

6 (7) include such other elements as may be necessary to ensure that
7 members of the armed forces who are separating from military service
8 are aware of opportunities to fill vacant U.S. Customs and Border Pro-
9 tection officer positions.

10 (c) REPORTS.—Not later than 180 days after October 16, 2015, and by
11 December 31 of each of the next 3 years, the Secretary, in consultation with
12 the Secretary of Defense, shall submit a report to the Committee on Home-
13 land Security and the Committee on Armed Services of the House of Rep-
14 resentatives and the Committee on Homeland Security and Governmental
15 Affairs and the Committee on Armed Services of the Senate that includes
16 a description and assessment of the efforts of the Department under this
17 section to hire members of the armed forces who are separating from mili-
18 tary service as U.S. Customs and Border Protection officers. The report
19 shall include—

20 (1) a detailed description of the efforts to implement subsection (b),
21 including—

22 (A) elements of the enhanced recruiting efforts and the goals
23 associated with those elements; and

24 (B) a description of how the elements and goals referred to in
25 subparagraph (A) will assist in meeting statutorily mandated
26 staffing levels and agency hiring benchmarks;

27 (2) a detailed description of the efforts that have been undertaken
28 under subsection (b);

29 (3) the estimated number of separating service members made aware
30 of U.S. Customs and Border Protection officer vacancies;

31 (4) the number of U.S. Customs and Border Protection officer va-
32 cancies filled with separating service members; and

33 (5) the number of U.S. Customs and Border Protection officer va-
34 cancies filled with separating service members under veterans recruit-
35 ment appointments authorized under section 4214 of title 38.

36 (d) RULES OF CONSTRUCTION.—Nothing in this section may be con-
37 strued—

38 (1) as superseding, altering, or amending existing Federal veterans'
39 hiring preferences or Federal hiring authorities; or

40 (2) to authorize the appropriation of additional amounts to carry out
41 this section.

tion and Customs Enforcement holding positions involving supervisory or managerial responsibility and classified, in accordance with chapter 51 of title 5, as a GS-14 or above, shall—

(A) gain some experience in all the major functions performed by U.S. Immigration and Customs Enforcement; and

(B) work in at least one local office of U.S. Immigration and Customs Enforcement.

(b) CHIEF OF POLICY AND STRATEGY.—

(1) IN GENERAL.—There is a Chief of Policy and Strategy for U.S. Immigration and Customs Enforcement.

(2) FUNCTIONS.—In consultation with U.S. Immigration and Customs Enforcement personnel in local offices, the Chief of Policy and Strategy is responsible for—

(A) making policy recommendations and performing policy research and analysis on immigration enforcement issues; and

(B) coordinating immigration policy issues with the Chief of Policy and Strategy for U.S. Citizenship and Immigration Services, as appropriate.

(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.

§ 10933. Professional responsibility and quality review

The Secretary is responsible for—

(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;

(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

(3) providing an analysis of the management of U.S. Immigration and Customs Enforcement.

§ 10934. Annual report on cross-border tunnels

(a) DEFINITION OF CONGRESSIONAL COMMITTEES.—In this section, the term “congressional committees” means—

(1) the Committee on Homeland Security and Governmental Affairs of the Senate;

- 1 (2) the Committee on the Judiciary of the Senate;
 2 (3) the Committee on Appropriations of the Senate;
 3 (4) the Committee on Homeland Security of the House of Represent-
 4 atives;
 5 (5) the Committee on the Judiciary of the House of Representatives;
 6 and
 7 (6) the Committee on Appropriations of the House of Representa-
 8 tives.

9 (b) CONTENT.—The Secretary shall submit an annual report to the con-
 10 gressional committees that includes a description of—

- 11 (1) the cross-border tunnels along the border between Mexico and
 12 the United States discovered during the preceding fiscal year; and
 13 (2) the needs of the Department to effectively prevent, investigate,
 14 and prosecute border tunnel construction along the border between
 15 Mexico and the United States.

16 **Subchapter IV—Citizenship and** 17 **Immigration Services**

18 **§ 10941. Transfer of functions to Director of U.S. Citizenship** 19 **and Immigration Services**

20 The Director of U.S. Citizenship and Immigration Services succeeds to
 21 the following functions of the Commissioner of Immigration and Naturaliza-
 22 tion, and all personnel, infrastructure, and funding provided to the Commis-
 23 sioner in support of the functions immediately before March 1, 2003:

- 24 (1) Adjudications of immigrant visa petitions.
 25 (2) Adjudications of naturalization petitions.
 26 (3) Adjudications of asylum and refugee applications.
 27 (4) Adjudications performed at service centers.
 28 (5) All other adjudications performed by the Immigration and Natu-
 29 ralization Service immediately before March 1, 2003.

30 **§ 10942. Responsibilities of U.S. Citizenship and Immigra-** 31 **tion Services officials**

- 32 (a) DIRECTOR.—
 33 (1) FUNCTIONS.—The Director of U.S. Citizenship and Immigration
 34 Services—
 35 (A) shall establish the policies for performing the functions
 36 transferred to the Director by section 10941 of this title or the
 37 Homeland Security Act of 2002 (Public Law 107–296, 116 Stat.
 38 2135) or otherwise vested in the Director by law;
 39 (B) shall oversee the administration of the policies;
 40 (C) shall advise the Deputy Secretary of Homeland Security
 41 with respect to a policy or operation of U.S. Citizenship and Immi-

1 gration Services that may affect U.S. Immigration and Customs
2 Enforcement, including potentially conflicting policies or oper-
3 ations;

4 (D) shall establish national immigration services policies and
5 priorities;

6 (E) shall meet regularly with the Ombudsman described in sec-
7 tion 10943 of this title to correct serious service problems identi-
8 fied by the Ombudsman; and

9 (F) shall establish procedures requiring a formal response to
10 recommendations submitted in the Ombudsman's annual report to
11 Congress within 3 months after its submission to Congress.

12 (2) MANAGERIAL ROTATION PROGRAM.—The Director of U.S. Citi-
13 zenship and Immigration Services shall design and implement a mana-
14 gerial rotation program under which employees of U.S. Citizenship and
15 Immigration Services holding positions involving supervisory or mana-
16 gerial responsibility and classified, in accordance with chapter 51 of
17 title 5, as a GS-14 or above, shall—

18 (A) gain some experience in all the major functions performed
19 by U.S. Citizenship and Immigration Services; and

20 (B) work in at least one field office and one service center of
21 U.S. Citizenship and Immigration Services.

22 (3) PILOT INITIATIVES FOR BACKLOG ELIMINATION.—The Director
23 of U.S. Citizenship and Immigration Services may implement innova-
24 tive pilot initiatives to eliminate a remaining backlog in the processing
25 of immigration benefit applications, and to prevent a backlog in the
26 processing of applications from recurring, under section 204(a) of the
27 Immigration Services and Infrastructure Improvements Act of 2000 (8
28 U.S.C. 1573(a)). Initiatives may include measures such as increasing
29 personnel, transferring personnel to focus on areas with the largest po-
30 tential for backlog, and streamlining paperwork.

31 (b) CHIEF OF POLICY AND STRATEGY.—

32 (1) IN GENERAL.—There is a Chief of Policy and Strategy for U.S.
33 Citizenship and Immigration Services.

34 (2) FUNCTIONS.—In consultation with U.S. Citizenship and Immi-
35 gration Services personnel in field offices, the Chief of Policy and
36 Strategy is responsible for—

37 (A) making policy recommendations and performing policy re-
38 search and analysis on immigration services issues; and

39 (B) coordinating immigration policy issues with the Chief of
40 Policy and Strategy for U.S. Immigration and Customs Enforce-
41 ment.

1 (c) LEGAL ADVISOR.—

2 (1) IN GENERAL.—There is a principal legal advisor to the Director
3 of U.S. Citizenship and Immigration Services.

4 (2) FUNCTIONS.—The legal advisor is responsible for—

5 (A) providing specialized legal advice, opinions, determinations,
6 regulations, and other assistance to the Director of U.S. Citizen-
7 ship and Immigration Services with respect to legal matters affect-
8 ing U.S. Citizenship and Immigration Services; and

9 (B) representing U.S. Citizenship and Immigration Services in
10 visa petition appeal proceedings before the Executive Office for
11 Immigration Review.

12 (d) BUDGET OFFICER.—

13 (1) IN GENERAL.—There is a Budget Officer for U.S. Citizenship
14 and Immigration Services.

15 (2) FUNCTIONS.—The Budget Officer is responsible for—

16 (A) formulating and executing the budget of U.S. Citizenship
17 and Immigration Services;

18 (B) financial management of U.S. Citizenship and Immigration
19 Services; and

20 (C) collecting all payments, fines, and other debts for U.S. Citi-
21 zenship and Immigration Services.

22 (e) CHIEF OF OFFICE OF CITIZENSHIP.—

23 (1) IN GENERAL.—There is a Chief of the Office of Citizenship for
24 U.S. Citizenship and Immigration Services.

25 (2) FUNCTIONS.—The Chief of the Office of Citizenship for U.S.
26 Citizenship and Immigration Services is responsible for promoting in-
27 struction and training on citizenship responsibilities for aliens inter-
28 ested in becoming naturalized citizens of the United States, including
29 the development of educational materials.

30 **§ 10943. Citizenship and Immigration Services Ombudsman**

31 (a) IN GENERAL.—There is in the Department a Citizenship and Immi-
32 gration Services Ombudsman (in this section referred to as the “Ombuds-
33 man”). The Ombudsman shall report directly to the Deputy Secretary of
34 Homeland Security. The Ombudsman shall have a background in customer
35 service as well as immigration law.

36 (b) FUNCTIONS.—The Ombudsman—

37 (1) shall assist individuals and employers in resolving problems with
38 U.S. Citizenship and Immigration Services;

39 (2) shall identify areas in which individuals and employers have
40 problems in dealing with U.S. Citizenship and Immigration Services;
41 and

1 (3) to the extent possible, shall propose changes in the administrative
2 practices of U.S. Citizenship and Immigration Services to mitigate
3 problems identified under paragraph (2).

4 (e) ANNUAL REPORT.—

5 (1) OBJECTIVES.—Not later than June 30 each year, the Ombuds-
6 man shall report to the Committees on the Judiciary of the House of
7 Representatives and the Senate on the objectives of the Office of the
8 Ombudsman for the fiscal year beginning in that year. The report shall
9 contain full and substantive analysis, in addition to statistical informa-
10 tion, and—

11 (A) shall identify the recommendations the Office of the Om-
12 budsman has made on improving services and responsiveness of
13 U.S. Citizenship and Immigration Services;

14 (B) shall contain a summary of the most pervasive and serious
15 problems encountered by individuals and employers, including a
16 description of the nature of the problems;

17 (C) shall contain an inventory of the items described in sub-
18 paragraphs (A) and (B) for which action has been taken and the
19 result of the action;

20 (D) shall contain an inventory of the items described in sub-
21 paragraphs (A) and (B) for which action remains to be completed
22 and the period during which each item has remained on the inven-
23 tory;

24 (E) shall contain an inventory of the items described in sub-
25 paragraphs (A) and (B) for which no action has been taken, the
26 period during which each item has remained on the inventory, the
27 reasons for the inaction, and shall identify any official of U.S.
28 Citizenship and Immigration Services who is responsible for inac-
29 tion;

30 (F) shall contain recommendations for administrative action ap-
31 propriate to resolve problems encountered by individuals and em-
32 ployers, including problems created by excessive backlogs in the
33 adjudication and processing of immigration benefit petitions and
34 applications; and

35 (G) shall include other information the Ombudsman may deem
36 advisable.

37 (2) REPORT TO BE SUBMITTED DIRECTLY TO COMMITTEES.—Each
38 report required under this subsection shall be provided directly to the
39 committees described in paragraph (1) without prior comment or
40 amendment from the Secretary, the Deputy Secretary of Homeland Se-
41 curity, the Director of U.S. Citizenship and Immigration Services, or

1 another officer or employee of the Department or the Office of Manage-
2 ment and Budget.

3 (d) OTHER RESPONSIBILITIES.—The Ombudsman—

4 (1) shall monitor the coverage and geographic allocation of local of-
5 fices of the Ombudsman;

6 (2) shall develop guidance to be distributed to all officers and em-
7 ployees of U.S. Citizenship and Immigration Services outlining the cri-
8 teria for referral of inquiries to local offices of the Ombudsman;

9 (3) shall ensure that the local telephone number for each local office
10 of the Ombudsman is published and available to individuals and em-
11 ployers served by the office; and

12 (4) shall meet regularly with the Director of U.S. Citizenship and
13 Immigration Services to identify serious service problems and to
14 present recommendations for administrative action appropriate to re-
15 solve problems encountered by individuals and employers.

16 (e) PERSONNEL ACTIONS.—

17 (1) IN GENERAL.—The Ombudsman has the responsibility and au-
18 thority—

19 (A) to appoint local ombudsmen and make available at least one
20 ombudsman for each State; and

21 (B) to evaluate and take personnel actions (including dismissal)
22 with respect to an employee of a local office of the Ombudsman.

23 (2) CONSULTATION.—The Ombudsman may consult with the appro-
24 priate supervisory personnel of U.S. Citizenship and Immigration Serv-
25 ices in carrying out the Ombudsman’s responsibilities under this sub-
26 section.

27 (f) RESPONSIBILITIES OF DIRECTOR OF U.S. CITIZENSHIP AND IMMIGRA-
28 TION SERVICES.—The Director of U.S. Citizenship and Immigration Serv-
29 ices shall establish procedures requiring a formal response to all rec-
30 ommendations submitted to the Director by the Ombudsman within 3
31 months after submission.

32 (g) OPERATION OF LOCAL OFFICES.—

33 (1) IN GENERAL.—Each local ombudsman—

34 (A) shall report to the Ombudsman or the delegate of the Om-
35 budsman;

36 (B) may consult with the appropriate supervisory personnel of
37 U.S. Citizenship and Immigration Services regarding the daily op-
38 eration of the local office of the Ombudsman;

39 (C) shall, at the initial meeting with an individual or employer
40 seeking the assistance of the local office, notify the individual or
41 employer that the local offices of the Ombudsman operate inde-

pendently of any other component of the Department and report directly to Congress through the Ombudsman; and

(D) at the local ombudsman's discretion, may determine not to disclose to U.S. Citizenship and Immigration Services contact with, or information provided by, the individual or employer.

(2) MAINTENANCE OF INDEPENDENT COMMUNICATIONS.—Each local office of the Ombudsman shall maintain a phone, facsimile, and other means of electronic communication access, and a post office address, that is separate from those maintained by U.S. Citizenship and Immigration Services, or any component of U.S. Citizenship and Immigration Services.

§ 10944. Professional responsibility and quality review

(a) IN GENERAL.—The Director of U.S. Citizenship and Immigration Services is responsible for—

(1) conducting investigations of noncriminal allegations of misconduct, corruption, and fraud involving an employee of U.S. Citizenship and Immigration Services that are not subject to investigation by the Inspector General for the Department;

(2) inspecting the operations of U.S. Citizenship and Immigration Services and providing assessments of the quality of the operations of U.S. Citizenship and Immigration Services as a whole and each of its components; and

(3) providing an analysis of the management of U.S. Citizenship and Immigration Services.

(b) SPECIAL CONSIDERATIONS.—In providing assessments under subsection (a)(2) with respect to a decision of U.S. Citizenship and Immigration Services, or of its components, consideration shall be given to—

(1) the accuracy of the findings of fact and conclusions of law used in rendering the decision;

(2) fraud or misrepresentation associated with the decision; and

(3) the efficiency with which the decision was rendered.

§ 10945. Employee discipline

The Director of U.S. Citizenship and Immigration Services may impose disciplinary action, including termination of employment, pursuant to policies and procedures applicable to employees of the Federal Bureau of Investigation, on an employee of U.S. Citizenship and Immigration Services who willfully deceives Congress or agency leadership on any matter.

§ 10946. Transition

(a) REFERENCES.—With respect to a function transferred by this subchapter to, and exercised on or after March 1, 2003, by, the Director of U.S. Citizenship and Immigration Services, a reference in any other Federal

1 law, Executive order, rule, regulation, delegation of authority, or document
2 of or pertaining to a component of government from which the function is
3 transferred—

4 (1) to the head of the component is deemed to refer to the Director
5 of U.S. Citizenship and Immigration Services; or

6 (2) to the component is deemed to refer to U.S. Citizenship and Im-
7 migration Services.

8 (b) EXERCISE OF AUTHORITIES.—Except as otherwise provided by law,
9 a Federal official to whom a function is transferred by this subchapter may,
10 for purposes of performing the function, exercise all authorities under any
11 other provision of law that were available with respect to the performance
12 of that function to the official responsible for the performance of the func-
13 tion immediately before March 1, 2003.

14 **§ 10947. Application of Internet-based technologies**

15 (a) ESTABLISHMENT OF TRACKING SYSTEM.—The Secretary, in consulta-
16 tion with the Technology Advisory Committee established under subsection
17 (c), shall establish an Internet-based system, that will permit a person, em-
18 ployer, immigrant, or nonimmigrant who has filings with the Secretary for
19 a benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et
20 seq.), access to online information about the processing status of the filing
21 involved.

22 (b) FEASIBILITY STUDY FOR ONLINE FILING AND IMPROVED PROC-
23 ESSING.—

24 (1) ONLINE FILING.—The Secretary, in consultation with the Tech-
25 nology Advisory Committee established under subsection (c), shall con-
26 duct a feasibility study on the online filing of the filings described in
27 subsection (a). The study shall include a review of computerization and
28 technology of U.S. Immigration and Customs Enforcement relating to
29 the immigration services and processing of filings relating to immigrant
30 services. The study shall also include an estimate of the timeframe and
31 cost and shall consider other factors in implementing such a filing sys-
32 tem, including the feasibility of fee payment online.

33 (2) REPORT.—A report on the study under this subsection shall be
34 submitted to the Committees on the Judiciary of the House of Rep-
35 resentatives and the Senate not later than January 24, 2004.

36 (c) TECHNOLOGY ADVISORY COMMITTEE.—

37 (1) ESTABLISHMENT.—The Secretary shall establish the Technology
38 Advisory Committee to assist the Secretary in—

39 (A) establishing the tracking system under subsection (a); and

40 (B) conducting the study under subsection (b).

1 (2) CONSULTATION.—The Technology Advisory Committee shall be
2 established after consultation with the Committees on the Judiciary of
3 the House of Representatives and the Senate.

4 (3) COMPOSITION.—The Technology Advisory Committee shall be
5 composed of representatives from high technology companies capable of
6 establishing and implementing the system in an expeditious manner,
7 and representatives of persons who may use the tracking system de-
8 scribed in subsection (a) and the online filing system described in sub-
9 section (b)(1).

10 **Subchapter V—General Immigration** 11 **Provisions**

12 **§ 10961. Director of Shared Services**

13 (a) IN GENERAL.—There is in the Office of the Deputy Secretary of
14 Homeland Security a Director of Shared Services.

15 (b) FUNCTIONS.—The Director of Shared Services is responsible for the
16 coordination of resources for U.S. Immigration and Customs Enforcement
17 and U.S. Citizenship and Immigration Services, including—

- 18 (1) information resources management, including computer data-
19 bases and information technology;
- 20 (2) records and file management; and
- 21 (3) forms management.

22 **§ 10962. Separation of funding**

23 (a) IN GENERAL.—There are in the Treasury separate accounts for ap-
24 propriated funds and other deposits available for U.S. Citizenship and Im-
25 migration Services and U.S. Immigration and Customs Enforcement.

26 (b) SEPARATE BUDGETS.—To ensure that U.S. Citizenship and Immigra-
27 tion Services and U.S. Immigration and Customs Enforcement are funded
28 to the extent necessary to fully carry out their respective functions, the Di-
29 rector of the Office of Management and Budget shall separate the budget
30 requests for each entity.

31 (c) FEES.—Fees imposed for a particular service, application, or benefit
32 shall be deposited in the account established under subsection (a) that is
33 for whichever of U.S. Immigration and Customs Enforcement or U.S. Citi-
34 zenship and Immigration Services has jurisdiction over the function to
35 which the fee relates.

36 (d) FEES NOT TRANSFERABLE.—A fee may not be transferred between
37 U.S. Citizenship and Immigration Services and U.S. Immigration and Cus-
38 toms Enforcement for purposes not authorized by section 286 of the Immi-
39 gration and Nationality Act (8 U.S.C. 1356).

1 **§ 10963. Annual immigration functions report**

2 (a) ANNUAL REPORT.—The Secretary shall submit a report annually to
3 the President, to the Committees on the Judiciary and Oversight and Gov-
4 ernment Reform of the House of Representatives, and to the Committees
5 on the Judiciary and Homeland Security and Governmental Affairs of the
6 Senate, on the impact the transfers made by Subtitle F of Title IV of the
7 Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2205) has
8 had on immigration functions.

9 (b) CONTENT.—The report shall address the following with respect to the
10 period covered by the report:

11 (1) The aggregate number of all immigration applications and peti-
12 tions received, and processed, by the Department.

13 (2) Region-by-region statistics on the aggregate number of immigra-
14 tion applications and petitions filed by an alien (or filed on behalf of
15 an alien) and denied, disaggregated by category of denial and applica-
16 tion or petition type.

17 (3) The quantity of backlogged immigration applications and peti-
18 tions that have been processed, the aggregate number awaiting process-
19 ing, and a detailed plan for eliminating the backlog.

20 (4) The average processing period for immigration applications and
21 petitions, disaggregated by application or petition type.

22 (5) The number and types of immigration-related grievances filed
23 with an official of the Department of Justice, and if those grievances
24 were resolved.

25 (6) Plans to address grievances and improve immigration services.

26 (7) Whether immigration-related fees were used consistent with legal
27 requirements regarding their use.

28 (8) Whether immigration-related questions conveyed by customers to
29 the Department (whether conveyed in person, by telephone, or by
30 means of the Internet) were answered effectively and efficiently.

31 **Subchapter VI—U.S. Customs and Border**
32 **Protection Public-Private Partnerships**

33 **§ 10971. Definitions**

34 In this subchapter:

35 (1) DONOR.—The term “donor” means an entity that is proposing
36 to make a donation under this title (except chapters 113 and 409).

37 (2) ENTITY.—The term “entity” means—

38 (A) a person;

39 (B) a partnership, corporation, trust, estate, cooperative, asso-
40 ciation, or other organized group of persons;

1 (C) the Federal Government or a State or local government (in-
 2 cluding a subdivision, agency, or instrumentality of the Federal
 3 Government or a State or local government); or

4 (D) another private person or governmental entity.

5 **§ 10972. Fee agreements for certain services at ports of**
 6 **entry**

7 (a) IN GENERAL.—Notwithstanding section 10301(e) of the Consolidated
 8 Omnibus Budget Reconciliation Act of 1985 (19 U.S.C. 58c(e)) and section
 9 451 of the Tariff Act of 1930 (19 U.S.C. 1451), the Commissioner of U.S.
 10 Customs and Border Protection, on the request of any entity, may enter
 11 into a fee agreement with the entity under which—

12 (1) U. S. Customs and Border Protection shall provide services de-
 13 scribed in subsection (b) at a United States port of entry or any other
 14 facility at which U.S. Customs and Border Protection provides the
 15 services;

16 (2) the entity shall remit to U.S. Customs and Border Protection a
 17 fee imposed under subsection (h) in an amount equal to the full costs
 18 that are incurred or will be incurred in providing the services; and

19 (3) if space is provided by the entity, each facility at which U.S.
 20 Customs and Border Protection services are performed shall be main-
 21 tained and equipped by the entity, without cost to the Federal Govern-
 22 ment, in accordance with U.S. Customs and Border Protection speci-
 23 fications.

24 (b) SERVICES DESCRIBED.—The services referred to in subsection (a) are
 25 activities of an employee or Office of Field Operations contractor of U.S.
 26 Customs and Border Protection (except employees of U.S. Border Patrol,
 27 as established under section 10306(e) of this title) pertaining to, or in sup-
 28 port of, customs, agricultural processing, border security, or immigration in-
 29 spection-related matters at a port of entry or other facility at which U.S.
 30 Customs and Border Protection provides or will provide the services.

31 (c) MODIFICATION OF PRIOR AGREEMENTS.—The Commissioner of U.S.
 32 Customs and Border Protection, at the request of an entity that has pre-
 33 viously entered into an agreement with U.S. Customs and Border Protection
 34 for the reimbursement of fees in effect on December 16, 2016, may modify
 35 the agreement to implement provisions of this section.

36 (d) LIMITATIONS.—

37 (1) IMPACTS OF SERVICES.—The Commissioner of U.S. Customs and
 38 Border Protection—

39 (A) may enter into fee agreements under this section only for
 40 services that—

1 (i) will increase or enhance the operational capacity of U.S.
2 Customs and Border Protection based on available staffing
3 and workload; and

4 (ii) will not shift the cost of services funded in an appro-
5 priations Act, or provided from an account in the Treasury
6 derived by the collection of fees, to entities under this title
7 (except chapters 113 and 409); and

8 (B) may not enter into a fee agreement under this section if the
9 agreement would unduly and permanently impact services funded
10 in an appropriations Act, or provided from an account in the
11 Treasury, derived by the collection of fees.

12 (2) NO LIMIT.—There shall be no limit to the number of fee agree-
13 ments that the Commissioner of U.S. Customs and Border Protection
14 may enter into under this section.

15 (e) AIR PORTS OF ENTRY.—

16 (1) IN GENERAL.—Except as otherwise provided in this subsection,
17 a fee agreement for U.S. Customs and Border Protection services at
18 an air port of entry may only provide for the payment of overtime costs
19 of U.S. Customs and Border Protection officers and salaries and ex-
20 penses of U.S. Customs and Border Protection employees to support
21 U.S. Customs and Border Protection officers in performing services de-
22 scribed in subsection (b).

23 (2) SMALL AIRPORTS.—Notwithstanding paragraph (1), U.S. Cus-
24 toms and Border Protection may receive reimbursement in addition to
25 overtime costs if the fee agreement is for services at an air port of
26 entry that has fewer than 100,000 arriving international passengers
27 annually.

28 (3) COVERED SERVICES.—In addition to costs described in para-
29 graph (1), a fee agreement for U.S. Customs and Border Protection
30 services at an air port of entry referred to in paragraph (2) may pro-
31 vide for the reimbursement of—

32 (A) salaries and expenses of not more than 5 fulltime equivalent
33 U.S. Customs and Border Protection officers beyond the number
34 of officers assigned to the port of entry on the date on which the
35 fee agreement was signed;

36 (B) salaries and expenses of employees of U.S. Customs and
37 Border Protection, other than the officers referred to in subpara-
38 graph (A), to support U.S. Customs and Border Protection offi-
39 cers in performing law enforcement functions; and

40 (C) other costs incurred by U.S. Customs and Border Protec-
41 tion relating to services described in subparagraph (B), such as

1 temporary placement or permanent relocation of employees, in-
2 cluding incentive pay for relocation, as appropriate.

3 (f) PORT OF ENTRY SIZE NOT A FACTOR.—The Commissioner of U.S.
4 Customs and Border Protection shall ensure that each fee agreement pro-
5 posal is given equal consideration regardless of the size of the port of entry.

6 (g) DENIED APPLICATION.—

7 (1) IN GENERAL.—If the Commissioner of U.S. Customs and Border
8 Protection denies a proposal for a fee agreement under this section, the
9 Commissioner shall provide the entity submitting the proposal with the
10 reason for the denial unless—

11 (A) the reason for the denial is law enforcement sensitive; or

12 (B) withholding the reason for the denial is in the national secu-
13 rity interests of the United States.

14 (2) JUDICIAL REVIEW.—Decisions of the Commissioner of U.S. Cus-
15 toms and Border Protection under paragraph (1) are in the discretion
16 of the Commissioner of U.S. Customs and Border Protection and are
17 not subject to judicial review.

18 (h) FEE.—

19 (1) IN GENERAL.—The amount of the fee to be charged under an
20 agreement authorized under subsection (a) shall be paid by each entity
21 requesting U.S. Customs and Border Protection services, and shall be
22 for the full cost of providing the services, including the salaries and ex-
23 penses of employees and contractors of U.S. Customs and Border Pro-
24 tection, to provide the services and other costs incurred by U.S. Cus-
25 toms and Border Protection relating to the services, such as temporary
26 or permanent relocation of the employees and contractors.

27 (2) TIMING.—The Commissioner of U.S. Customs and Border Pro-
28 tection may require that the fee referred to in paragraph (1) be paid
29 by each entity that has entered into a fee agreement under subsection
30 (a) with U.S. Customs and Border Protection in advance of the per-
31 formance of U.S. Customs and Border Protection services.

32 (3) OVERSIGHT.—The Commissioner of U.S. Customs and Border
33 Protection shall develop a process to oversee the services for which fees
34 are charged pursuant to an agreement under subsection (a), includ-
35 ing—

36 (A) a determination and report on the full costs of providing the
37 services, and a process for increasing the fees, as necessary;

38 (B) the establishment of a periodic remittance schedule to re-
39 plenish appropriations, accounts, or funds, as necessary; and

40 (C) the identification of costs paid by the fees.

41 (i) DEPOSIT OF FUNDS.—

1 (1) ACCOUNT.—Funds collected pursuant to an agreement entered
2 into pursuant to subsection (a)—

3 (A) shall be deposited as offsetting collections;

4 (B) shall remain available until expended without fiscal year
5 limitation; and

6 (C) shall be credited to the applicable appropriation, account, or
7 fund for the amount paid out of the appropriation, account, or
8 fund for any expenses incurred or to be incurred by U.S. Customs
9 and Border Protection in providing U.S. Customs and Border Pro-
10 tection services under the agreement and for any other costs in-
11 curred or to be incurred by U.S. Customs and Border Protection
12 relating to the services.

13 (2) RETURN OF UNUSED FUNDS.—The Commissioner of U.S. Cus-
14 toms and Border Protection shall return any unused funds collected
15 and deposited in the account described in paragraph (1) if a fee agree-
16 ment entered into pursuant to subsection (a) is terminated for any rea-
17 son or the terms of the fee agreement change by mutual agreement to
18 cause a reduction of U.S. Customs and Border Protection services. No
19 interest shall be owed on the return of the unused funds.

20 (j) TERMINATION.—

21 (1) IN GENERAL.—The Commissioner of U.S. Customs and Border
22 Protection shall terminate the services provided pursuant to a fee
23 agreement entered into under subsection (a) with an entity that, after
24 receiving notice from the Commissioner of U.S. Customs and Border
25 Protection that a fee under subsection (h) is due, fails to pay the fee
26 in a timely manner. If the services are terminated, all costs incurred
27 by U.S. Customs and Border Protection that have not been paid shall
28 become immediately due and payable. Interest on unpaid fees shall ac-
29 crue based on the rate and amount established under sections 6221
30 and 6222 of the Internal Revenue Code of 1986 (26 U.S.C. 6221,
31 6222).

32 (2) PENALTY.—An entity that, after notice and demand for payment
33 of a fee under subsection (h), fails to pay the fee in a timely manner
34 shall be liable for a penalty or liquidated damage equal to 2 times the
35 amount of the fee. The amount collected under this paragraph shall be
36 deposited into the appropriate account specified under subsection (i)
37 and shall be available as described in subsection (i).

38 (3) TERMINATION BY THE ENTITY.—An entity that has previously
39 entered into an agreement with U.S. Customs and Border Protection
40 for the reimbursement of fees in effect on December 16, 2016, or
41 under the provisions of this section, may request that the agreement

1 be amended to provide for termination on advance notice, length, and
 2 terms that are negotiated between the entity and U.S. Customs and
 3 Border Protection.

4 (k) ANNUAL REPORT.—The Commissioner of U.S. Customs and Border
 5 Protection shall—

6 (1) submit an annual report identifying the activities undertaken and
 7 the agreements entered into pursuant to this section to—

8 (A) the Committee on Appropriations of the Senate;

9 (B) the Committee on Finance of the Senate;

10 (C) the Committee on Homeland Security and Governmental Af-
 11 fairs of the Senate;

12 (D) the Committee on the Judiciary of the Senate;

13 (E) the Committee on Appropriations of the House of Rep-
 14 resentatives;

15 (F) the Committee on Homeland Security of the House of Rep-
 16 resentatives;

17 (G) the Committee on the Judiciary of the House of Represent-
 18 atives; and

19 (H) the Committee on Ways and Means of the House of Rep-
 20 resentatives; and

21 (2) not later than 15 days before entering into a fee agreement, no-
 22 tify the members of Congress who represent the State or congressional
 23 district in which the affected port of entry or facility is located of the
 24 agreement.

25 (l) RULE OF CONSTRUCTION.—Nothing in this section may be construed
 26 as imposing on U.S. Customs and Border Protection any responsibilities,
 27 duties, or authorities relating to real property.

28 **§ 10973. Port of entry donation authority**

29 (a) PERSONAL PROPERTY, MONEY, OR NONPERSONAL SERVICES.—

30 (1) IN GENERAL.—The Commissioner of U.S. Customs and Border
 31 Protection, in consultation with the Administrator of General Services,
 32 may enter into an agreement with an entity to accept a donation of
 33 personal property, money, or nonpersonal services for the uses de-
 34 scribed in paragraph (3) only with respect to the following locations at
 35 which U.S. Customs and Border Protection performs or will be per-
 36 forming inspection services:

37 (A) A new or existing sea or air port of entry.

38 (B) An existing Federal Government-owned land port of entry.

39 (C) A new Federal Government-owned land port of entry if—

40 (i) the fair market value of the donation is \$50,000,000 or
 41 less; and

1 (ii) the fair market value, including any personal and real
 2 property donations in total, of the port of entry when com-
 3 plete, is \$50,000,000 or less.

4 (2) LIMITATION ON MONETARY DONATIONS.—A monetary donation
 5 accepted pursuant to this subsection may not be used to pay the sala-
 6 ries of U.S. Customs and Border Protection employees performing in-
 7 spection services.

8 (3) USES.—Donations accepted pursuant to this subsection may be
 9 used for activities of the Office of Field Operations, set forth in sub-
 10 paragraphs (A) through (F) of section 10306(g)(3) of this title, that
 11 are related to a new or existing sea or air port of entry or a new or
 12 existing Federal Government-owned land port of entry described in
 13 paragraph (1), including expenses relating to—

14 (A) furniture, fixtures, equipment, or technology, including the
 15 installation or deployment of those items; and

16 (B) the operation and maintenance of the furniture, fixtures,
 17 equipment, or technology.

18 (b) REAL PROPERTY OR MONEY.—

19 (1) IN GENERAL.—Subject to paragraph (3), the Commissioner of
 20 U.S. Customs and Border Protection, and the Administrator of General
 21 Services, as applicable, may enter into an agreement with an entity to
 22 accept a donation of real property or money for uses described in para-
 23 graph (2) only with respect to the following locations at which U.S.
 24 Customs and Border Protection performs or will be performing inspec-
 25 tion services:

26 (A) A new or existing sea or air port of entry.

27 (B) An existing Federal Government-owned land port of entry.

28 (C) A new Federal Government-owned land port of entry if—

29 (i) the fair market value of the donation is \$50,000,000 or
 30 less; and

31 (ii) the fair market value, including any personal and real
 32 property donations in total, of the port of entry when com-
 33 plete, is \$50,000,000 or less.

34 (2) USES.—Donations accepted pursuant to this subsection may be
 35 used for activities of the Office of Field Operations set forth in section
 36 10306(g) of this title that are related to the construction, alteration,
 37 operation, or maintenance of a new or existing sea or air port of entry
 38 or a new or existing Federal Government-owned land port of entry de-
 39 scribed in paragraph (1), including expenses related to—

40 (A) land acquisition, design, construction, repair, or alteration;
 41 and

1 (B) operation and maintenance of the port of entry facility.

2 (3) LIMITATION ON REAL PROPERTY DONATIONS.—A donation of
3 real property under this subsection at an existing land port of entry
4 owned by the General Services Administration may only be accepted by
5 the Administrator of General Services.

6 (4) SUNSET.—

7 (A) IN GENERAL.—The authority to enter into an agreement
8 under this subsection shall terminate on December 16, 2020.

9 (B) RULE OF CONSTRUCTION.—The termination date referred
10 to in subparagraph (A) shall not apply to carrying out the terms
11 of an agreement under this subsection if the agreement is entered
12 into before December 16, 2020.

13 (c) GENERAL PROVISIONS.—

14 (1) DURATION.—An agreement entered into under subsection (a) or
15 (b) (and in the case of subsection (b), in accordance with paragraph
16 (4) of subsection (b)) may last as long as required to meet the terms
17 of the agreement.

18 (2) CRITERIA.—In carrying out an agreement entered into under
19 subsection (a) or (b), the Commissioner of U.S. Customs and Border
20 Protection, in consultation with the Administrator of General Services,
21 shall establish criteria regarding—

22 (A) the selection and evaluation of donors;

23 (B) the identification of roles and responsibilities between U.S.
24 Customs and Border Protection, the General Services Administra-
25 tion, and donors;

26 (C) the identification, allocation, and management of explicit
27 and implicit risks of partnering between the Federal Government
28 and donors;

29 (D) decision-making and dispute resolution processes; and

30 (E) processes for U.S. Customs and Border Protection, and the
31 General Services Administration, as applicable, to terminate agree-
32 ments if selected donors are not meeting the terms of the agree-
33 ment, including the security standards established by U.S. Cus-
34 toms and Border Protection.

35 (3) EVALUATION PROCEDURES.—

36 (A) IN GENERAL.—The Commissioner of U.S. Customs and
37 Border Protection, in consultation with the Administrator of Gen-
38 eral Services, as applicable, shall—

39 (i) establish criteria for evaluating a proposal to enter into
40 an agreement under subsection (a) or (b); and

41 (ii) make the criteria publicly available.

1 (B) CONSIDERATIONS.—Criteria established pursuant to sub-
2 paragraph (A) shall consider—

3 (i) the impact of a proposal referred to in subparagraph
4 (A) on the land, sea, or air port of entry at issue and other
5 ports of entry or similar facilities or other infrastructure near
6 the location of the proposed donation;

7 (ii) the proposal's potential to increase trade and travel ef-
8 ficiency through added capacity;

9 (iii) the proposal's potential to enhance the security of the
10 port of entry at issue;

11 (iv) the impact of the proposal on reducing wait times at
12 the port of entry or facility and other ports of entry on the
13 same border;

14 (v) for a donation under subsection (b)—

15 (I) whether the donation satisfies the requirements of
16 the proposal or whether additional real property would
17 be required; and

18 (II) how the donation was acquired, including if emi-
19 nent domain was used;

20 (vi) the funding available to complete the intended use of
21 the donation;

22 (vii) the costs of maintaining and operating the donation;

23 (viii) the impact of the proposal on U.S. Customs and Bor-
24 der Protection staffing requirements; and

25 (ix) other factors that the Commissioner of U.S. Customs
26 and Border Protection or the Administrator of General Serv-
27 ices determines to be relevant.

28 (C) DETERMINATION AND NOTIFICATION.—

29 (i) INCOMPLETE PROPOSALS.—

30 (I) IN GENERAL.—Not later than 60 days after receiv-
31 ing the proposals for a donation agreement from an enti-
32 ty, the Commissioner of U.S. Customs and Border Pro-
33 tection shall notify the entity as to whether the proposal
34 is complete or incomplete.

35 (II) RESUBMISSION.—If the Commissioner of U.S.
36 Customs and Border Protection determines that a pro-
37 posal is incomplete, the Commissioner shall—

38 (aa) notify the appropriate entity and provide the
39 entity with a description of all information or mate-
40 rial that is needed to complete review of the pro-
41 posal; and

1 (bb) allow the entity to resubmit the proposal
2 with additional information and material described
3 in item (aa) to complete the proposal.

4 (ii) COMPLETE PROPOSAL.—Not later than 180 days after
5 receiving a completed proposal to enter into an agreement
6 under subsection (a) or (b), the Commissioner of U.S. Cus-
7 toms and Border Protection, with the concurrence of the Ad-
8 ministrator of General Services, as applicable, shall—

9 (I) determine whether to approve or deny the proposal;
10 and

11 (II) notify the entity that submitted the proposal of
12 the determination.

13 (4) SUPPLEMENTAL FUNDING.—Except as required under section
14 3307 of title 40, real property donations to the Administrator of Gen-
15 eral Services made pursuant to subsection (b) at a GSA-owned land
16 port of entry may be used in addition to any other funding for the port
17 of entry, including appropriated funds, property, or services.

18 (5) RETURN OF DONATIONS.—The Commissioner of U.S. Customs
19 and Border Protection, or the Administrator of General Services, as
20 applicable, may return a donation made pursuant to subsection (a) or
21 (b). No interest shall be owed to the donor with respect to any donation
22 provided under subsection (a) or (b) that is returned pursuant to this
23 subsection.

24 (6) PROHIBITION ON CERTAIN FUNDING.—

25 (A) IN GENERAL.—Except as provided in subsections (a) and
26 (b) regarding the acceptance of donations, the Commissioner of
27 U.S. Customs and Border Protection and the Administrator of
28 General Services, as applicable, may not, with respect to an agree-
29 ment entered into under subsection (a) or (b), obligate or expend
30 amounts in excess of amounts that have been appropriated pursu-
31 ant to any appropriations Act for purposes specified in subsection
32 (a) or (b) or otherwise made available for those purposes.

33 (B) CERTIFICATION REQUIREMENT.—Before accepting any do-
34 nations pursuant to an agreement under subsection (a) or (b), the
35 Commissioner of U.S. Customs and Border Protection shall certify
36 to the congressional committees set forth in paragraph (7) that
37 the donation will not be used for the construction of a detention
38 facility or a border fence or wall.

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 an annual report to the congressional committees referred to
23 in subsection (c)(7) that evaluates—

24 (1) fee agreements entered into pursuant to section 10972 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 **§ 10974. 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 title V
6 of division D of the Consolidated and Further Continuing Appropria-
7 tions Act, 2013 (Public Law 113–6, 127 Stat. 378) or section 559 of
8 title V of division F of the Consolidated Appropriations Act, 2014
9 (Public Law 113–76, 128 Stat. 279) as in existence on December 15,
10 2016, and the agreement shall continue to have full force and effect
11 on and after December 15, 2016; or

12 (2) a proposal accepted for consideration by U.S. Customs and Bor-
13 der Protection pursuant to section 559 of title V of division F of the
14 Consolidated Appropriations Act, 2014 (Public Law 113–76, 128 Stat.
15 279) as in existence on December 15, 2016.

16 **Subchapter VII—Miscellaneous Provisions**

17 **§ 10981. 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 **§ 10982. 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 provision of law, and
39 except as provided in subsection (c) of this section, the Secretary—

40 (1) shall be vested exclusively with all authorities to issue regulations
41 with respect to, administer, and enforce the provisions of the Act, and

1 of all other immigration and nationality laws, relating to the functions
2 of consular officers of the United States in connection with the grant-
3 ing or refusal of visas, and shall have the authority to refuse visas in
4 accordance with law and to develop programs of homeland security
5 training for consular officers (in addition to consular training provided
6 by the Secretary of State), which authorities shall be exercised through
7 the Secretary of State, except that the Secretary shall not have author-
8 ity to alter or reverse the decision of a consular officer to refuse a visa
9 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.

1 (2) FUNCTIONS.—Employees assigned under paragraph (1) shall
2 perform the following functions:

3 (A) Provide expert advice and training to consular officers re-
4 garding specific security threats relating to the adjudication of in-
5 dividual visa applications or classes of applications.

6 (B) Review applications, either on the initiative of the employee
7 of the Department or upon request by a consular officer or other
8 person charged with adjudicating applications.

9 (C) Conduct investigations with respect to consular matters
10 under the jurisdiction of the Secretary

11 (3) EVALUATION OF CONSULAR OFFICERS.—The Secretary of State
12 shall evaluate, in consultation with the Secretary, as considered appro-
13 priate by the Secretary, the performance of consular officers with re-
14 spect to the processing and adjudication of applications for visas in ac-
15 cordance with performance standards developed by the Secretary for
16 these procedures.

17 (4) REPORT.—The Secretary shall, on an annual basis, submit a re-
18 port to Congress that describes the basis for each determination under
19 paragraph (1) that the assignment of an employee of the Department
20 at a particular diplomatic post would not promote homeland security.

21 (5) PERMANENT ASSIGNMENT; PARTICIPATION IN TERRORIST LOOK-
22 OUT COMMITTEE.—When appropriate, employees of the Department as-
23 signed to perform functions described in paragraph (2) may be as-
24 signed permanently to overseas diplomatic or consular posts with coun-
25 try-specific or regional responsibility. If the Secretary so directs, an
26 employee, when present at an overseas post, shall participate in the ter-
27 rorist lookout committee established under section 304 of the Enhanced
28 Border Security and Visa Entry Reform Act of 2002 (8 U.S.C. 1733).

29 (6) TRAINING AND HIRING.—

30 (A) IN GENERAL.—The Secretary shall ensure, to the extent
31 possible, that employees of the Department assigned to perform
32 functions under paragraph (2) and, as appropriate, consular offi-
33 cers, shall be provided the necessary training to enable them to
34 carry out the functions, including training in foreign languages,
35 interview techniques, and fraud detection techniques, in conditions
36 in the particular country where each employee is assigned, and in
37 other appropriate areas of study.

38 (B) USE OF CENTER.—The Secretary may use the George P.
39 Shultz National Foreign Affairs Training Center, on a reimburs-
40 able basis, to obtain the training described in subparagraph (A).

1 (f) NO CREATION OF PRIVATE RIGHT OF ACTION.—Nothing in this sec-
2 tion shall be construed to create or authorize a private right of action to
3 challenge a decision of a consular officer or other United States official or
4 employee to grant or deny a visa.

5 (g) VISA ISSUANCE PROGRAM FOR SAUDI ARABIA.—On-site personnel of
6 the Department shall review all visa applications for Saudi Arabia prior to
7 adjudication.

8 **§ 10983. Information on visa denials required to be entered**
9 **into electronic data system**

10 (a) IN GENERAL.—Whenever a consular officer of the United States de-
11 nies a visa to an applicant, the consular officer shall enter the fact and the
12 basis of the denial and the name of the applicant into the interoperable elec-
13 tronic data system implemented under section 202(a) of the Enhanced Bor-
14 der Security and Visa Entry Reform Act of 2002 (8 U.S.C. 1722(a)).

15 (b) PROHIBITION.—In the case of an alien with respect to whom a visa
16 has been denied under subsection (a)—

17 (1) no subsequent visa may be issued to the alien unless the consular
18 officer considering the alien’s visa application has reviewed the infor-
19 mation concerning the alien placed in the interoperable electronic data
20 system, has indicated on the alien’s application that the information
21 has been reviewed, and has stated for the record why the visa is being
22 issued or a waiver of visa ineligibility recommended in spite of that in-
23 formation; and

24 (2) the alien may not be admitted to the United States without a
25 visa issued in accordance with the procedures described in paragraph
26 (1).

27 **§ 10984. Purpose and responsibilities of Office of Cargo Se-**
28 **curity Policy**

29 (a) PURPOSES.—The Office of Cargo Security Policy—

30 (1) coordinates all Department policies relating to cargo security;
31 and

32 (2) consults with stakeholders and coordinates with other Federal
33 agencies in the establishment of standards and regulations and the pro-
34 motion of best practices.

35 (b) RESPONSIBILITIES OF DIRECTOR.—The Director of the Office of
36 Cargo Security Policy—

37 (1) advises the Assistant Secretary for Policy in the development of
38 Department-wide policies regarding cargo security;

39 (2) coordinates all policies relating to cargo security among the agen-
40 cies and offices within the Department relating to cargo security; and

1 (3) coordinates the cargo security policies of the Department with
2 the policies of other executive agencies.

3 (c) RELATIONSHIP WITH COAST GUARD.—Nothing in this section shall be
4 construed to affect—

5 (1) the authorities, functions, or capabilities of the Coast Guard to
6 perform its missions; or

7 (2) the requirement under section 10312 of this title that those au-
8 thorities, functions, and capabilities be maintained intact.

9 **§ 10985. Purpose, composition, and operation of Border En-**
10 **forcement Security Task Force**

11 (a) PURPOSE.—The purpose of the Border Enforcement Security Task
12 Force (in this section referred to as “BEST”) is to establish units to en-
13 hance border security by addressing and reducing border security threats
14 and violence by—

15 (1) facilitating collaboration among Federal, State, local, tribal, and
16 foreign law enforcement agencies to execute coordinated activities in
17 furtherance of border security, and homeland security; and

18 (2) enhancing information sharing, including the dissemination of
19 homeland security information among these agencies.

20 (b) COMPOSITION AND ESTABLISHMENT OF UNITS.—

21 (1) COMPOSITION.—BEST units may be comprised of personnel
22 from—

23 (A) U.S. Immigration and Customs Enforcement;

24 (B) U.S. Customs and Border Protection;

25 (C) the Coast Guard;

26 (D) other Department personnel, as appropriate;

27 (E) other Federal agencies, as appropriate;

28 (F) appropriate State law enforcement agencies;

29 (G) foreign law enforcement agencies, as appropriate;

30 (H) local law enforcement agencies from affected border cities
31 and communities; and

32 (I) appropriate tribal law enforcement agencies.

33 (2) ESTABLISHMENT.—The Secretary may establish BEST units in
34 jurisdictions in which the units can contribute to BEST missions, as
35 appropriate. Before establishing a BEST unit, the Secretary shall con-
36 sider—

37 (A) whether the area in which the BEST unit would be estab-
38 lished is significantly impacted by cross-border threats;

39 (B) the availability of Federal, State, local, tribal, and foreign
40 law enforcement resources to participate in the BEST unit;

1 (C) the extent to which border security threats are having a sig-
 2 nificant harmful impact in the jurisdiction in which the BEST
 3 unit is to be established, and other jurisdictions in the country;
 4 and

5 (D) whether or not an Integrated Border Enforcement Team al-
 6 ready exists in the area in which the BEST unit would be estab-
 7 lished.

8 (3) DUPLICATION OF EFFORTS.—In determining whether to establish
 9 a new BEST unit or to expand an existing BEST unit in a given juris-
 10 diction, the Secretary shall ensure that the BEST unit under consider-
 11 ation does not duplicate the efforts of other existing interagency task
 12 forces or centers within that jurisdiction.

13 (e) OPERATION.—After determining the jurisdictions in which to establish
 14 BEST units under subsection (b)(2), and in order to provide Federal assist-
 15 ance to the jurisdictions, the Secretary may—

16 (1) direct the assignment of Federal personnel to BEST, subject to
 17 the approval of the head of the department or agency that employs
 18 such personnel; and

19 (2) take other actions to assist Federal, State, local, and tribal enti-
 20 ties to participate in BEST, including providing financial assistance, as
 21 appropriate, for operational, administrative, and technological costs as-
 22 sociated with the participation of Federal, State, local, and tribal law
 23 enforcement agencies in BEST

24 (d) REPORT.—Not later than June 6, 2017, and 2018, the Secretary
 25 shall submit a report to Congress that describes the effectiveness of BEST
 26 in enhancing border security and reducing the drug trafficking, arms smug-
 27 gling, illegal alien trafficking and smuggling, violence, and kidnapping along
 28 and across the international borders of the United States, as measured by
 29 crime statistics, including violent deaths, incidents of violence, and drug-re-
 30 lated arrests.

31 **§ 10986. Cyber Crimes Center**

32 (a) IN GENERAL.—

33 (1) ESTABLISHMENT.—The Secretary shall operate, in U.S. Immi-
 34 gration and Customs Enforcement, a Cyber Crimes Center (referred to
 35 in this section as the “Center”).

36 (2) PURPOSE.—The purpose of the Center is to provide investigative
 37 assistance, training, and equipment to support U.S. Immigration and
 38 Customs Enforcement’s domestic and international investigations of
 39 cyber-related crimes.

40 (b) CHILD EXPLOITATION INVESTIGATIONS UNIT

1 (1) IN GENERAL.—The Secretary shall operate, in the Center, a
2 Child Exploitation Investigations Unit (referred to in this subsection as
3 the “CEIU”).

4 (2) FUNCTIONS.—The CEIU—

5 (A) shall coordinate all U.S. Immigration and Customs Enforce-
6 ment child exploitation initiatives, including investigations into—

7 (i) child exploitation;

8 (ii) child pornography;

9 (iii) child victim identification;

10 (iv) traveling child sex offenders; and

11 (v) forced child labor, including the sexual exploitation of
12 minors;

13 (B) shall, among other things, focus on—

14 (i) child exploitation prevention;

15 (ii) investigative capacity building;

16 (iii) enforcement operations; and

17 (iv) training for Federal, State, local, tribal, and foreign
18 law enforcement agency personnel, on request;

19 (C) shall provide training, technical expertise, support, or co-
20 ordination of child exploitation investigations, as needed, to co-
21 operating law enforcement agencies and personnel;

22 (D) shall provide psychological support and counseling services
23 for U.S. Immigration and Customs Enforcement personnel en-
24 gaged in child exploitation prevention initiatives, including making
25 available other existing services to assist employees who are ex-
26 posed to child exploitation material during investigations;

27 (E) may collaborate with the Department of Defense and the
28 National Association to Protect Children for the purpose of the re-
29 cruiting, training, equipping and hiring of wounded, ill, and in-
30 jured veterans and transitioning service members, through the
31 Human Exploitation Rescue Operative (HERO) Child Rescue
32 Corps program; and

33 (F) shall collaborate with other governmental, nongovernmental,
34 and nonprofit entities approved by the Secretary for the sponsor-
35 ship of, and participation in, outreach and training activities.

36 (3) DATA COLLECTION.—The CEIU shall collect and maintain data
37 concerning—

38 (A) the total number of suspects identified by U.S. Immigration
39 and Customs Enforcement;

40 (B) the number of arrests by U.S. Immigration and Customs
41 Enforcement, disaggregated by type, including—

1 (i) the number of victims identified through investigations
2 carried out by U.S. Immigration and Customs Enforcement;
3 and

4 (ii) the number of suspects arrested who were in positions
5 of trust or authority over children;

6 (C) the number of cases opened for investigation by U.S. Immi-
7 gration and Customs Enforcement; and

8 (D) the number of cases resulting in a Federal, State, foreign,
9 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 (c) COMPUTER FORENSICS UNIT.—

4 (1) IN GENERAL.—The Secretary shall operate, in the Center, a
5 Computer Forensics Unit (referred to in this subsection as the
6 “CFU”).

7 (2) FUNCTIONS.—The CFU—

8 (A) shall provide training and technical support in digital
9 forensics to—

10 (i) U.S. Immigration and Customs Enforcement personnel;
11 and

12 (ii) Federal, State, local, tribal, military, and foreign law
13 enforcement agency personnel engaged in the investigation of
14 crimes within their respective jurisdictions, on request and
15 subject to the availability of funds;

16 (B) shall provide computer hardware, software, and forensic li-
17 censes for all computer forensics personnel in U.S. Immigration
18 and Customs Enforcement;

19 (C) shall participate in research and development in the area of
20 digital forensics, in coordination with appropriate components of
21 the Department; and

22 (D) may collaborate with the Department of Defense and the
23 National Association to Protect Children for the purpose of re-
24 cruiting, training, equipping, and hiring wounded, ill, and injured
25 veterans and transitioning service members, through the Human
26 Exploitation Rescue Operative (HERO) Child Rescue Corps pro-
27 gram.

28 (3) COOPERATIVE AGREEMENTS.—The CFU may enter into coopera-
29 tive agreements to accomplish the functions set forth in paragraph (2).

30 (4) ACCEPTANCE OF GIFTS.—

31 (A) IN GENERAL.—The Secretary may accept money and in-
32 kind donations from the Virtual Global Task Force, national lab-
33 oratories, Federal agencies, not-for-profit organizations, and edu-
34 cational institutions to create and expand public awareness cam-
35 paigns in support of the functions of the CFU.

36 (B) EXEMPTION FROM FEDERAL ACQUISITION REGULATION.—
37 Gifts authorized under subparagraph (A) are not subject to the
38 Federal Acquisition Regulation for competition when the services
39 provided by the entities referred to in subparagraph (A) are do-
40 nated or of minimal cost to the Department.

41 (d) CYBER CRIMES UNIT.—

1 (1) IN GENERAL.—The Secretary shall operate, in the Center, a
2 Cyber Crimes Unit (referred to in this subsection as the “CCU”).

3 (2) FUNCTIONS.—The CCU—

4 (A) shall oversee the cyber security strategy and cyber-related
5 operations and programs for U.S. Immigration and Customs En-
6 forcement;

7 (B) shall enhance U.S. Immigration and Customs Enforce-
8 ment’s ability to combat criminal enterprises operating on or
9 through the Internet, with specific focus in the areas of—

10 (i) cyber economic crime;

11 (ii) digital theft of intellectual property;

12 (iii) illicit e-commerce (including hidden marketplaces);

13 (iv) Internet-facilitated proliferation of arms and strategic
14 technology; and

15 (v) cyber-enabled smuggling and money laundering;

16 (C) shall provide training and technical support in cyber inves-
17 tigation to—

18 (i) U.S. Immigration and Customs Enforcement personnel;

19 and

20 (ii) Federal, State, local, tribal, military, and foreign law
21 enforcement agency personnel engaged in the investigation of
22 crimes within their respective jurisdictions, on request and
23 subject to the availability of funds;

24 (D) shall participate in research and development in the area
25 of cyber investigations, in coordination with appropriate compo-
26 nents of the Department; and

27 (E) may recruit participants of the Human Exploitation Rescue
28 Operative (HERO) Child Rescue Corps program for investigative
29 and forensic positions in support of the functions of the CCU.

30 (3) COOPERATIVE AGREEMENTS.—The CCU may enter into coopera-
31 tive agreements to accomplish the functions set forth in paragraph (2).

32 (e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be
33 appropriated to the Secretary such sums as are necessary to carry out this
34 section.

35 **Chapter 111—National Emergency** 36 **Management**

Sec.

11101. Definitions.

11102. Federal Emergency Management Agency.

11103. Authority and responsibilities.

11104. Preparedness programs.

11105. Functions transferred.

11106. Preserving the Federal Emergency Management Agency.

11107. Regional Offices.

- 11108. National Advisory Council.
- 11109. National Integration Center.
- 11110. Credentialing and typing.
- 11111. National Infrastructure Simulation and Analysis Center.
- 11112. Evacuation plans and exercises.
- 11113. Disability Coordinator.
- 11114. National Operations Center.
- 11115. Responsibilities of Chief Medical Officer.
- 11116. Nuclear incident response.
- 11117. Conduct of certain public health-related activities.
- 11118. Use of national private-sector networks in emergency response.
- 11119. Model standards and guidelines for critical infrastructure workers.
- 11120. Guidance and recommendations.
- 11121. Voluntary private-sector preparedness accreditation and certification program.
- 11122. Acceptance of gifts.
- 11123. Integrated public alert and warning system modernization.
- 11124. National planning and education.

1 **§ 11101. Definitions**

2 In this chapter:

3 (1) ADMINISTRATOR.—the term “Administrator” means the Admin-
4 istrator of the Agency.

5 (2) AGENCY.—The term “Agency” means the Federal Emergency
6 Management Agency.

7 (3) CATASTROPHIC INCIDENT.—The term “catastrophic incident”
8 means a natural disaster, act of terrorism, or other man-made disaster
9 that results in extraordinary levels of casualties or damage or disrup-
10 tion severely affecting the population (including mass evacuations), in-
11 frastructure, environment, economy, national morale, or government
12 functions in an area.

13 (4) CREDENTIALLED; CREDENTIALING.—The terms “credentialed”
14 and “credentialing” mean having provided, or providing, respectively,
15 documentation that identifies personnel and authenticates and verifies
16 the qualifications of the personnel by ensuring that the personnel pos-
17 sess a minimum common level of training, experience, physical and
18 medical fitness, and capability appropriate for a particular position in
19 accordance with standards created under section 11110 of this title.

20 (5) FEDERAL COORDINATING OFFICER.—The term “Federal coordi-
21 nating officer” means a Federal coordinating officer as described in
22 section 302 of the Robert T. Stafford Disaster Relief and Emergency
23 Assistance Act (42 U.S.C. 5143).

24 (6) INTEROPERABLE COMMUNICATIONS.—The term “interoperable
25 communications” has the meaning given that term in section 10712(a)
26 of this title.

27 (7) NATIONAL INCIDENT MANAGEMENT SYSTEM.—The term “Na-
28 tional Incident Management System” means a system to enable effec-
29 tive, efficient, and collaborative incident management.

1 (8) NATIONAL RESPONSE PLAN.—The term “National Response
2 Plan” means the National Response Plan or a successor plan prepared
3 under section 11103(a)(6) of this title.

4 (9) NUCLEAR INCIDENT RESPONSE TEAM.—The term “Nuclear Inci-
5 dent Response Team” means a resource that includes—

6 (A) those entities of the Department of Energy that perform
7 nuclear or radiological emergency support functions (including ac-
8 cident response, search response, advisory, and technical oper-
9 ations functions), radiation exposure functions at the medical as-
10 sistance facility known as the Radiation Emergency Assistance
11 Center/Training Site (REAC/TS), radiological assistance func-
12 tions, and related functions; and

13 (B) those entities of the Environmental Protection Agency that
14 perform such support functions (including radiological emergency
15 response functions) and related functions.

16 (10) REGIONAL ADMINISTRATOR.—The term “Regional Adminis-
17 trator” means Regional Administrator appointed under section 11107
18 of this title.

19 (11) REGIONAL OFFICE.—The term “Regional Office” means a Re-
20 gional Office established under section 11107 of this title.

21 (12) RESOURCES.—The term “resources” means personnel and
22 major items of equipment, supplies, and facilities available or poten-
23 tially available for responding to a natural disaster, act of terrorism,
24 or other man-made disaster.

25 (13) SURGE CAPACITY.—The term “surge capacity” means the abil-
26 ity to rapidly and substantially increase the provision of search and res-
27 cue capabilities, food, water, medicine, shelter and housing, medical
28 care, evacuation capacity, staffing (including disaster assistance em-
29 ployees), and other resources necessary to save lives and protect prop-
30 erty during a catastrophic incident.

31 (14) TRIBAL GOVERNMENT.—The term “tribal government” means
32 the government of an entity described in section 10101 of this title.

33 (15) TYPED; TYPING.—The terms “typed” and “typing” mean hav-
34 ing evaluated, or evaluating, respectively, a resource in accordance with
35 standards created under section 11110 of this title.

36 **§ 11102. Federal Emergency Management Agency**

37 (a) MISSION.—

38 (1) PRIMARY MISSION.—The primary mission of the Agency is to re-
39 duce the loss of life and property and protect the Nation from all haz-
40 ards, including natural disasters, acts of terrorism, and other man-
41 made disasters, by leading and supporting the Nation in a risk-based,

1 comprehensive emergency management system of preparedness, protec-
2 tion, response, recovery, and mitigation.

3 (2) SPECIFIC ACTIVITIES.—In support of the primary mission of the
4 Agency, the Administrator shall—

5 (A) lead the Nation’s efforts to prepare for, protect against, re-
6 spond to, recover from, and mitigate against the risk of natural
7 disasters, acts of terrorism, and other man-made disasters, includ-
8 ing catastrophic incidents;

9 (B) partner with State, local, and tribal governments and emer-
10 gency response providers, with other Federal agencies, with the
11 private sector, and with nongovernmental organizations to build a
12 national system of emergency management that can effectively and
13 efficiently utilize the full measure of the Nation’s resources to re-
14 spond to natural disasters, acts of terrorism, and other man-made
15 disasters, including catastrophic incidents;

16 (C) develop a Federal response capability that, when necessary
17 and appropriate, can act effectively and rapidly to deliver assist-
18 ance essential to saving lives or protecting or preserving property
19 or public health and safety in a natural disaster, act of terrorism,
20 or other man-made disaster;

21 (D) integrate the Agency’s emergency preparedness, protection,
22 response, recovery, and mitigation responsibilities to confront ef-
23 fectively the challenges of a natural disaster, act of terrorism, or
24 other man-made disaster;

25 (E) develop and maintain robust Regional Offices that will work
26 with State, local, and tribal governments, emergency response pro-
27 viders, and other appropriate entities to identify and address re-
28 gional priorities;

29 (F) under the leadership of the Secretary, coordinate with the
30 Commandant of the Coast Guard, the Commissioner of U.S. Cus-
31 toms and Border Protection, the Director of Immigration and
32 Customs Enforcement, the National Operations Center, and other
33 agencies and offices in the Department to take full advantage of
34 the substantial range of resources in the Department;

35 (G) provide funding, training, exercises, technical assistance,
36 planning, and other assistance to build tribal, local, State, re-
37 gional, and national capabilities (including communications capa-
38 bilities), necessary to respond to a natural disaster, act of ter-
39 rorism, or other man-made disaster; and

40 (H) develop and coordinate the implementation of a risk-based,
41 all-hazards strategy for preparedness that builds those common

1 capabilities necessary to respond to natural disasters, acts of ter-
2 rorism, and other man-made disasters while also building the
3 unique capabilities necessary to respond to specific types of inci-
4 dents that pose the greatest risk to our Nation.

5 (b) ADMINISTRATOR.—

6 (1) REPORTING.—The Administrator shall report to the Secretary,
7 without being required to report through another official of the Depart-
8 ment.

9 (2) PRINCIPAL ADVISOR ON EMERGENCY MANAGEMENT.—

10 (A) IN GENERAL.—The Administrator is the principal advisor to
11 the President, the Homeland Security Council, and the Secretary
12 for all matters relating to emergency management in the United
13 States.

14 (B) ADVICE AND RECOMMENDATIONS.—

15 (i) RANGE OF OPTIONS.—In presenting advice with respect
16 to a matter to the President, the Homeland Security Council,
17 or the Secretary, the Administrator shall, as the Adminis-
18 trator considers appropriate, inform the President, the Home-
19 land Security Council, or the Secretary, as the case may be,
20 of the range of emergency preparedness, protection, response,
21 recovery, and mitigation options with respect to that matter.

22 (ii) ADVICE ON A PARTICULAR MATTER.—The Adminis-
23 trator, as the principal advisor on emergency management,
24 shall provide advice to the President, the Homeland Security
25 Council, or the Secretary on a particular matter when the
26 President, the Homeland Security Council, or the Secretary
27 requests advice.

28 (iii) RECOMMENDATIONS.—After informing the Secretary,
29 the Administrator may make recommendations to Congress
30 relating to emergency management the Administrator con-
31 siders appropriate.

32 (3) CABINET STATUS.—

33 (A) IN GENERAL.—The President may designate the Adminis-
34 trator to serve as a member of the Cabinet in the event of natural
35 disasters, acts of terrorism, or other man-made disasters.

36 (B) RETENTION OF AUTHORITY.—Nothing in this paragraph
37 shall be construed as affecting the authority of the Secretary
38 under this subtitle.

39 **§ 11103. Authority and responsibilities**

40 (a) IN GENERAL.—The Administrator shall provide Federal leadership
41 necessary to prepare for, protect against, respond to, recover from, or miti-

1 gate against a natural disaster, act of terrorism, or other man-made dis-
2 aster, including—

3 (1) helping to ensure the effectiveness of emergency response pro-
4 viders to terrorist attacks, major disasters, and other emergencies;

5 (2) with respect to the Nuclear Incident Response Team (regardless
6 of whether it is operating as an organizational unit of the Department
7 pursuant to this chapter)—

8 (A) establishing standards and certifying when those standards
9 have been met;

10 (B) conducting joint and other exercises, and training and eval-
11 uating performance; and

12 (C) providing funds to the Department of Energy and the Envi-
13 ronmental Protection Agency, as appropriate, for homeland secu-
14 rity planning, exercises and training, and equipment;

15 (3) providing the Federal Government’s response to terrorist attacks
16 and major disasters, including—

17 (A) managing the response;

18 (B) directing the Domestic Emergency Support Team and
19 (when operating as an organizational unit of the Department pur-
20 suant to this chapter) the Nuclear Incident Response Team;

21 (C) overseeing the Metropolitan Medical Response System; and

22 (D) coordinating other Federal response resources, including re-
23 quiring deployment of the Strategic National Stockpile, in the
24 event of a terrorist attack or major disaster;

25 (4) aiding the recovery from terrorist attacks and major disasters;

26 (5) building a comprehensive national incident management system
27 with Federal, State, and local government personnel, agencies, and au-
28 thorities, to respond to attacks and disasters;

29 (6) consolidating existing Federal Government emergency response
30 plans into a single, coordinated national response plan;

31 (7) helping ensure the acquisition of operable and interoperable com-
32 munications capabilities by Federal, State, local, and tribal govern-
33 ments and emergency response providers;

34 (8) assisting the President in carrying out the functions under the
35 Robert T. Stafford Disaster Relief and Emergency Assistance Act (42
36 U.S.C. 5121 et seq.) and carrying out all functions and authorities
37 given to the Administrator under that Act;

38 (9) carrying out the mission of the Agency to reduce the loss of life
39 and property and protect the Nation from all hazards by leading and
40 supporting the Nation in a risk-based, comprehensive emergency man-
41 agement system of—

1 (A) mitigation, by taking sustained actions to reduce or elimi-
2 nate long-term risks to people and property from hazards and
3 their effects;

4 (B) preparedness, by planning, training, and building the emer-
5 gency management profession to prepare effectively for, mitigate
6 against, respond to, and recover from a hazard;

7 (C) response, by conducting emergency operations to save lives
8 and property through positioning emergency equipment, personnel,
9 and supplies, through evacuating potential victims, through pro-
10 viding food, water, shelter, and medical care to those in need, and
11 through restoring critical public services; and

12 (D) recovery, by rebuilding communities so individuals, busi-
13 nesses, and governments can function on their own, return to nor-
14 mal life, and protect against future hazards;

15 (10) increasing efficiencies, by coordinating efforts relating to pre-
16 paredness, protection, response, recovery, and mitigation;

17 (11) helping to ensure the effectiveness of emergency response pro-
18 viders in responding to a natural disaster, act of terrorism, or other
19 man-made disaster;

20 (12) supervising grant programs administered by the Agency;

21 (13) administering and ensuring the implementation of the National
22 Response Plan, including coordinating and ensuring the readiness of
23 each emergency support function under the National Response Plan;

24 (14) coordinating with the National Advisory Council established
25 under section 11108 of this title;

26 (15) preparing and implementing the plans and programs of the
27 Federal Government for—

28 (A) continuity of operations;

29 (B) continuity of government; and

30 (C) continuity of plans;

31 (16) minimizing, to the extent practicable, overlapping planning and
32 reporting requirements applicable to State, local, and tribal govern-
33 ments and the private sector;

34 (17) maintaining and operating within the Agency the National Re-
35 sponse Coordination Center or its successor;

36 (18) developing a national emergency management system that is ca-
37 pable of preparing for, protecting against, responding to, recovering
38 from, and mitigating against catastrophic incidents;

39 (19) assisting the President in carrying out the functions under the
40 national preparedness goal and the national preparedness system and

1 carrying out all functions and authorities of the Administrator under
2 the national preparedness system;

3 (20) carrying out all authorities of the Federal Emergency Manage-
4 ment Agency and the Directorate of Preparedness of the Department
5 as transferred under section 11105 of this title; and

6 (21) otherwise carrying out the mission of the Agency as described
7 in section 11102(a) of this title.

8 (b) ALL-HAZARDS APPROACH.—In carrying out the responsibilities under
9 this section, the Administrator shall coordinate the implementation of a
10 risk-based, all-hazards strategy that builds those common capabilities nec-
11 essary to prepare for, protect against, respond to, recover from, or mitigate
12 against natural disasters, acts of terrorism, and other man-made disasters,
13 while also building the unique capabilities necessary to prepare for, protect
14 against, respond to, recover from, or mitigate against the risks of specific
15 types of incidents that pose the greatest risk to the Nation.

16 **§ 11104. Preparedness programs**

17 The Administrator is responsible for the radiological emergency prepared-
18 ness program and the chemical stockpile emergency preparedness program.

19 **§ 11105. Functions transferred**

20 (a) IN GENERAL.—Except as provided in subsection (b), there are trans-
21 ferred to the Agency the following:

22 (1) All functions of the Agency, including existing responsibilities for
23 emergency alert systems and continuity of operations and continuity of
24 government plans and programs as constituted on June 1, 2006, in-
25 cluding all of its personnel, assets, components, authorities, grant pro-
26 grams, and liabilities, and including the functions of the former Under
27 Secretary for Federal Emergency Management relating to the Agency.

28 (2) The former Directorate of Preparedness, as constituted on June
29 1, 2006, including all of its functions, personnel, assets, components,
30 authorities, grant programs, and liabilities, and including the functions
31 of the Under Secretary for Preparedness relating to the Directorate.

32 (b) EXCEPTIONS.—The following in the former Directorate of Prepared-
33 ness shall not be transferred:

34 (1) The Office of Infrastructure Protection.

35 (2) The National Communications System.

36 (3) The National Cybersecurity Division.

37 (4) The Office of the Chief Medical Officer.

38 (5) The functions, personnel, assets, components, authorities, and li-
39 abilities of each component described under paragraphs (1) through
40 (4).

1 **§ 11106. Preserving the Federal Emergency Management**
2 **Agency**

3 (a) REORGANIZATION.—Section 10331(b) of this title shall not apply to
4 the Agency, including any function or organizational unit of the Agency.

5 (b) PROHIBITION ON CHANGES TO MISSIONS.—

6 (1) IN GENERAL.—The Secretary may not substantially or signifi-
7 cantly reduce, including through a Joint Task Force established under
8 section 11508 of this title, the authorities, responsibilities, or functions
9 of the Agency or the capability of the Agency to perform those mis-
10 sions, authorities, and responsibilities, except as otherwise specifically
11 provided in an Act enacted after October 4, 2006.

12 (2) CERTAIN TRANSFERS PROHIBITED.—No asset, function, or mis-
13 sion of the Agency may be diverted to the principal and continuing use
14 of another organization, unit, or entity of the Department, including
15 a Joint Task Force established under section 11508 of this title, except
16 for details or assignments that do not reduce the capability of the
17 Agency to perform its missions.

18 (c) REPROGRAMMING AND TRANSFER OF FUNDS.—In reprogramming or
19 transferring funds, the Secretary shall comply with applicable provisions of
20 any Act making appropriations for the Department for any fiscal year relat-
21 ing to the reprogramming or transfer of funds.

22 **§ 11107. Regional Offices**

23 (a) IN GENERAL.—There are in the Agency 10 regional offices, as identi-
24 fied by the Administrator.

25 (b) MANAGEMENT OF REGIONAL OFFICES.—

26 (1) REGIONAL ADMINISTRATOR.—Each Regional Office shall be
27 headed by a Regional Administrator, who shall be appointed by the Ad-
28 ministrator, after consulting with State, local, and tribal government
29 officials in the region. Each Regional Administrator shall report di-
30 rectly to the Administrator and be in the Senior Executive Service.

31 (2) QUALIFICATIONS.—

32 (A) IN GENERAL.—Each Regional Administrator shall be ap-
33 pointed from among individuals who have a demonstrated ability
34 in and knowledge of emergency management and homeland secu-
35 rity.

36 (B) CONSIDERATIONS.—In selecting a Regional Administrator
37 for a Regional Office, the Administrator shall consider the famili-
38 arity of an individual with the geographical area and demographic
39 characteristics of the population served by the Regional Office.

40 (c) RESPONSIBILITIES.—

1 (1) IN GENERAL.—The Regional Administrator shall work in part-
2 nership with State, local, and tribal governments, emergency managers,
3 emergency response providers, medical providers, the private sector,
4 nongovernmental organizations, multijurisdictional councils of govern-
5 ments, and regional planning commissions and organizations in the
6 geographical area served by the Regional Office to carry out the re-
7 sponsibilities of a Regional Administrator under this section.

8 (2) SPECIFIC RESPONSIBILITIES.—The responsibilities of a Regional
9 Administrator include—

10 (A) ensuring effective, coordinated, and integrated regional pre-
11 paredness, protection, response, recovery, and mitigation activities
12 and programs for natural disasters, acts of terrorism, and other
13 man-made disasters (including planning, training, exercises, and
14 professional development);

15 (B) assisting in the development of regional capabilities needed
16 for a national catastrophic response system;

17 (C) coordinating the establishment of effective regional operable
18 and interoperable emergency communications capabilities;

19 (D) staffing and overseeing one or more strike teams within the
20 region under subsection (f), to serve as the focal point of the Fed-
21 eral Government’s initial response efforts for natural disasters,
22 acts of terrorism, and other man-made disasters within that re-
23 gion, and otherwise building Federal response capabilities to re-
24 spond to natural disasters, acts of terrorism, and other man-made
25 disasters within that region;

26 (E) designating an individual responsible for the development of
27 strategic and operational regional plans in support of the National
28 Response Plan;

29 (F) fostering the development of mutual aid and other coopera-
30 tive agreements;

31 (G) identifying critical gaps in regional capabilities to respond
32 to populations with special needs;

33 (H) maintaining and operating a Regional Response Coordina-
34 tion Center or its successor;

35 (I) coordinating with the private sector to help ensure private-
36 sector preparedness for natural disasters, acts of terrorism, and
37 other man-made disasters;

38 (J) assisting State, local, and tribal governments, where appro-
39 priate, to pre-identify and evaluate suitable sites where a multi-
40 jurisdictional incident command system may quickly be established
41 and operated from, if the need for a system arises; and

1 (K) performing any other duties relating to these responsibilities
2 that the Administrator may require.

3 (3) TRAINING AND EXERCISE REQUIREMENTS.—

4 (A) TRAINING.—The Administrator shall require each Regional
5 Administrator to undergo specific training periodically to com-
6 plement the qualifications of the Regional Administrator. The
7 training, as appropriate, shall include training with respect to the
8 National Incident Management System, the National Response
9 Plan, and other subjects determined by the Administrator.

10 (B) EXERCISES.—The Administrator shall require each Re-
11 gional Administrator to participate as appropriate in regional and
12 national exercises.

13 (d) AREA OFFICES.—

14 (1) IN GENERAL.—There is an Area Office for the Pacific and an
15 Area Office for the Caribbean, as components in the appropriate Re-
16 gional Offices.

17 (2) ALASKA.—The Administrator shall establish an Area Office in
18 Alaska, as a component in the appropriate Regional Office.

19 (e) REGIONAL ADVISORY COUNCIL.—

20 (1) ESTABLISHMENT.—Each Regional Administrator shall establish
21 a Regional Advisory Council.

22 (2) NOMINATIONS.—A State, local, or tribal government located in
23 the geographic area served by the Regional Office may nominate offi-
24 cials, including Adjutants General and emergency managers, to serve
25 as members of the Regional Advisory Council for that region.

26 (3) RESPONSIBILITIES.—Each Regional Advisory Council shall—

27 (A) advise the Regional Administrator on emergency manage-
28 ment issues specific to that region;

29 (B) identify geographic, demographic, or other characteristics
30 peculiar to a State, local, or tribal government within the region
31 that might make preparedness, protection, response, recovery, or
32 mitigation more complicated or difficult; and

33 (C) advise the Regional Administrator of weaknesses or defi-
34 ciencies in preparedness, protection, response, recovery, and miti-
35 gation for a State, local, and tribal government within the region
36 of which the Regional Advisory Council is aware.

37 (f) REGIONAL OFFICE STRIKE TEAMS.—

38 (1) IN GENERAL.—In coordination with other relevant Federal agen-
39 cies, each Regional Administrator shall oversee multi-agency strike
40 teams authorized under section 303 of the Robert T. Stafford Disaster

1 Relief and Emergency Assistance Act (42 U.S.C. 5144) that shall con-
2 sist of—

3 (A) a designated Federal coordinating officer;

4 (B) personnel trained in incident management;

5 (C) public affairs, response and recovery, and communications
6 support personnel;

7 (D) a defense coordinating officer;

8 (E) liaisons to other Federal agencies;

9 (F) Other personnel the Administrator or Regional Adminis-
10 trator determines appropriate; and

11 (G) individuals from the agencies with primary responsibility for
12 each of the emergency support functions in the National Response
13 Plan.

14 (2) OTHER DUTIES TO BE CONSISTENT.—The duties of an individual
15 assigned to a Regional Office strike team from another relevant agency
16 when the individual is not functioning as a member of the strike team
17 shall be consistent with the emergency preparedness activities of the
18 agency that employs the individual.

19 (3) LOCATION OF MEMBERS.—The members of each Regional Office
20 strike team, including representatives from agencies other than the De-
21 partment, shall be based primarily within the region that corresponds
22 to that strike team.

23 (4) COORDINATION.—Each Regional Office strike team shall coordi-
24 nate the training and exercises of that strike team with the State, local,
25 and tribal governments and private-sector and nongovernmental entities
26 that the strike team shall support when a natural disaster, act of ter-
27 rorism, or other man-made disaster occurs.

28 (5) PREPAREDNESS.—Each Regional Office strike team shall be
29 trained as a unit on a regular basis and equipped and staffed to be
30 well prepared to respond to natural disasters, acts of terrorism, and
31 other man-made disasters, including catastrophic incidents.

32 (6) AUTHORITIES.—If the Administrator determines that statutory
33 authority is inadequate for the preparedness and deployment of individ-
34 uals in strike teams under this subsection, the Administrator shall re-
35 port to Congress regarding the additional statutory authorities that the
36 Administrator determines are necessary.

37 § 11108. National Advisory Council

38 (a) ESTABLISHMENT.—There is in the Department the National Advisory
39 Council, established as an advisory body under section 10381(a) of this title
40 to ensure effective and ongoing coordination of Federal preparedness, pro-

1 tection, response, recovery, and mitigation for natural disasters, acts of ter-
2 rorism, and other man-made disasters.

3 (b) RESPONSIBILITIES.—

4 (1) IN GENERAL.—The National Advisory Council shall advise the
5 Administrator on all aspects of emergency management. The National
6 Advisory Council shall incorporate State, local, and tribal government
7 and private-sector input in the development and revision of the national
8 preparedness goal, the national preparedness system, the National Inci-
9 dent Management System, the National Response Plan, and other re-
10 lated plans and strategies.

11 (2) CONSULTATION ON GRANTS.—To ensure input from and coordi-
12 nation with State, local, and tribal governments and emergency re-
13 sponse providers, the Administrator shall regularly consult and work
14 with the National Advisory Council on the administration and assess-
15 ment of grant programs administered by the Department, including
16 with respect to the development of program guidance and the develop-
17 ment and evaluation of risk-assessment methodologies, as appropriate.

18 (c) MEMBERSHIP.—

19 (1) IN GENERAL.—The members of the National Advisory Council
20 shall be appointed by the Administrator, and shall, to the extent prac-
21 ticable, represent a geographic (including urban and rural) and sub-
22 stantive cross section of officials, emergency managers, and emergency
23 response providers from State, local, and tribal governments, the pri-
24 vate sector, and nongovernmental organizations, including as appro-
25 priate—

26 (A) members selected from the emergency management field
27 and emergency response providers, including fire service, law en-
28 forcement, hazardous materials response, emergency medical serv-
29 ices, and emergency management personnel, or organizations rep-
30 resenting these individuals;

31 (B) health scientists, emergency and inpatient medical pro-
32 viders, and public health professionals;

33 (C) experts from Federal, State, local, and tribal governments,
34 and the private sector, representing standards-setting and accred-
35 iting organizations, including representatives from the voluntary
36 consensus codes and standards development community, particu-
37 larly those with expertise in the emergency preparedness and re-
38 sponse field;

39 (D) State, local, and tribal government officials with expertise
40 in preparedness, protection, response, recovery, and mitigation, in-
41 cluding Adjutants General;

1 (E) elected State, local, and tribal government executives;

2 (F) experts in public- and private-sector infrastructure protec-
3 tion, cybersecurity, and communications;

4 (G) representatives of individuals with disabilities and other
5 populations with special needs; and

6 (H) other individuals the Administrator determines to be appro-
7 priate.

8 (2) COORDINATION WITH DEPARTMENTS OF HEALTH AND HUMAN
9 SERVICES AND TRANSPORTATION.—In the selection of members of the
10 National Advisory Council who are health or emergency medical serv-
11 ices professionals, the Administrator shall work with the Secretary of
12 Health and Human Services and the Secretary of Transportation.

13 (3) EX OFFICIO MEMBERS.—The Administrator shall designate one
14 or more officers of the Federal Government to serve as ex officio mem-
15 bers of the National Advisory Council.

16 (4) TERM OF OFFICE.—The term of office of each member of the
17 National Advisory Council shall be 3 years.

18 (d) RESPONSE SUBCOMMITTEE.—

19 (1) ESTABLISHMENT.—The Administrator shall establish the Rail-
20 road Emergency Services Preparedness, Operational Needs, and Safety
21 Evaluation Subcommittee (in this subsection referred to as the “RE-
22 SPONSE Subcommittee”).

23 (2) MEMBERSHIP.—Notwithstanding subsection (c), the RE-
24 SPONSE Subcommittee is composed of the following:

25 (A) the Deputy Administrator, Protection and National Pre-
26 paredness of the Federal Emergency Management Agency, or des-
27 ignee.

28 (B) The Chief Safety Officer of the Pipeline and Hazardous
29 Materials Safety Administration, or designee.

30 (C) The Associate Administrator for Hazardous Materials Safe-
31 ty of the Pipeline and Hazardous Materials Safety Administration,
32 or designee.

33 (D) The Director of the Office of Emergency Communications
34 of the Department, or designee.

35 (E) The Director of the Office of Railroad, Pipeline and Haz-
36 arduous Materials Investigations of the National Transportation
37 Safety Board, or designee.

38 (F) The Chief Safety Officer and Associate Administrator for
39 Railroad Safety of the Federal Railroad Administration, or des-
40 ignee.

1 (G) The Assistant Administrator for Security Policy and Indus-
2 try Engagement of the Transportation Security Administration, or
3 designee.

4 (H) The Assistant Commandant for Response Policy of the
5 Coast Guard, or designee.

6 (I) The Assistant Administrator for the Office of Solid Waste
7 and Emergency Response of the Environmental Protection Agen-
8 cy, or designee.

9 (J) Such other qualified individuals as the co-chairpersons shall
10 jointly appoint as soon as practicable from among the following:

11 (i) Members of the National Advisory Council who have the
12 requisite technical knowledge and expertise to address rail
13 emergency response issues, including members for the fol-
14 lowing disciplines:

15 (I) Emergency management and emergency response
16 providers, including fire service, law enforcement, haz-
17 ardous materials response, and emergency medical serv-
18 ices.

19 (II) State, local, and tribal government officials.

20 (ii) Individuals who have the requisite technical knowledge
21 and expertise to serve on the RESPONSE Subcommittee, in-
22 cluding at least 1 representative from each of the following:

23 (I) The rail industry.

24 (II) Rail labor.

25 (III) Persons that offer oil for transportation by rail.

26 (IV) The communications industry.

27 (V) Emergency response providers, including individ-
28 uals nominated by national organizations representing
29 State and local governments and emergency responders.

30 (VI) Emergency response training providers.

31 (VII) Representatives from tribal organizations.

32 (VIII) Technical experts.

33 (IX) Vendors, developers, and manufacturers of sys-
34 tems, facilities, equipment, and capabilities for emer-
35 gency responder services.

36 (iii) Representatives of such other stakeholders and inter-
37 ested and affected parties as the co-chairpersons consider ap-
38 propriate.

39 (3) CO-CHAIRPERSONS.—The members described in subparagraphs
40 (A) and (B) of paragraph (2) shall serve as the co-chairpersons of the
41 RESPONSE Subcommittee.

1 (4) CONSULTATION WITH NONMEMBERS.—The RESPONSE Sub-
2 committee and the program offices for emergency responder training
3 and resources shall consult with other relevant agencies and groups, in-
4 cluding entities engaged in federally funded research and academic in-
5 stitutions engaged in relevant work and research, that are not rep-
6 resented on the RESPONSE Subcommittee to consider new and devel-
7 oping technologies and methods that may be beneficial to preparedness
8 and response to rail hazardous materials incidents.

9 (5) RECOMMENDATIONS.—The RESPONSE Subcommittee shall de-
10 velop recommendations, as appropriate, for improving emergency re-
11 sponder training and resource allocation for hazardous materials inci-
12 dents involving railroads after evaluating the following topics:

13 (A) The quality and application of training for State and local
14 emergency responders relating to rail hazardous materials inci-
15 dents, including training for emergency responders serving small
16 communities near railroads, including the following:

17 (i) Ease of access to relevant training for State and local
18 emergency responders, including an analysis of—

19 (I) the number of individual being trained;

20 (II) the number of individuals who are applying;

21 (III) whether current demand is being met;

22 (IV) current challenges; and

23 (V) projected needs.

24 (ii) Modernization of training course content relating to rail
25 hazardous materials incidents, with a particular focus on fluc-
26 tuations in oil shipments by rail, including regular and ongo-
27 ing evaluation of course opportunities, adaptation to emerging
28 trends, agency and private-sector outreach, effectiveness, and
29 ease of access for State and local emergency responders.

30 (iii) Identification of overlap in training content and identi-
31 fication of opportunities to develop complementary courses
32 and materials among governmental and nongovernmental en-
33 tities.

34 (iv) Online training platforms, train-the-trainer, and mobile
35 training options.

36 (B) The availability and effectiveness of Federal, State, local,
37 and nongovernmental funding levels related to training emergency
38 responders for rail hazardous materials incidents, including emer-
39 gency responders serving small communities near railroads, includ-
40 ing—

41 (i) identifying overlap in resource allocation;

1 (ii) identifying cost-saving measures that can be imple-
2 mented to increase training opportunities;

3 (iii) leveraging government funding with nongovernmental
4 funding to enhance training opportunities and fill existing
5 training gaps;

6 (iv) adaptation of priority settings for agency funding allo-
7 cations in response to emerging trends;

8 (v) historic levels of funding across Federal agencies for
9 rail hazardous materials incident response and training, in-
10 cluding funding provided by the private sector to public enti-
11 ties or in conjunction with Federal programs; and

12 (vi) current funding resources across agencies.

13 (C) The strategy for integrating commodity flow studies, map-
14 ping, and rail and hazardous materials databases for State and
15 local emergency responders and increasing the rate of access to
16 the individual responder in existing or emerging communications
17 technology.

18 (6) REPORT.—

19 (A) IN GENERAL.—Not later than December 16, 2017, the RE-
20 SPONSE Committee shall submit a report to the National Advi-
21 sory Council that—

22 (i) includes the recommendations developed under para-
23 graph (5);

24 (ii) specifies the timeframes for implementing the rec-
25 ommendations that do not require congressional action; and

26 (iii) identifies the recommendations that do require con-
27 gressional action.

28 (B) REVIEW.—Not later than 30 days after receiving the report
29 under subparagraph (A), the National Advisory Council shall
30 begin a review of the report. The National Advisory Council may
31 ask for additional clarification, changes, or other information from
32 the RESPONSE Subcommittee to assist in the approval of the
33 recommendations.

34 (C) RECOMMENDATIONS.—Once the National Advisory Council
35 approves the recommendations of the RESPONSE Subcommittee,
36 the National Advisory Council shall submit the report to—

37 (i) the co-chairpersons of the RESPONSE Subcommittee;

38 (ii) the head of each other agency represented on the RE-
39 SPONSE Subcommittee;

40 (iii) the Committee on Homeland Security and Govern-
41 mental Affairs of the Senate;

1 (iv) the Committee on Commerce, Science, and Transpor-
2 tation of the Senate;

3 (v) the Committee on Homeland Security of the House of
4 Representatives; and

5 (vi) the Committee on Transportation and Infrastructure of
6 the House of Representatives.

7 (7) INTERIM ACTIVITY.—

8 (A) UPDATES AND OVERSIGHT.—After the submission of the re-
9 port by the National Advisory Council under paragraph (6), the
10 Administrator shall—

11 (i) provide annual updates to the congressional committees
12 referred to in paragraph (6)(C) regarding the status of the
13 implementation of the recommendations developed under
14 paragraph (5); and

15 (ii) coordinate the implementation of the recommendations
16 described in paragraph (5)(A)(i), as appropriate.

17 (B) SUNSET.—The requirements of subparagraph (A) shall ter-
18minate on the date that is 2 years after the date of the submission
19of the report required under paragraph (6)(A).

20 (8) TERMINATION.—The RESPONSE Subcommittee shall terminate
21not later than 90 days after the submission of the report required
22under paragraph (6)(C).

23 (e) APPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.—

24 (1) IN GENERAL.—Notwithstanding section 10381(a) of this title
25and subject to paragraph (2), the Federal Advisory Committee Act (5
26U.S.C. App.), including section 10(a), (b), and (d), and section 552b(c)
27of title 5, apply to the National Advisory Council.

28 (2) TERMINATION.—Section 14(a)(2) of the Federal Advisory Com-
29mittee Act (5 U.S.C. App.) does not apply to the National Advisory
30Council.

31 **§ 11109. National Integration Center**

32 (a) IN GENERAL.—There is in the Agency the National Integration Cen-
33ter.

34 (b) RESPONSIBILITIES.—

35 (1) IN GENERAL.—The Administrator and the National Integration
36Center, and in consultation with other Federal departments and agen-
37cies and the National Advisory Council, shall ensure ongoing manage-
38ment and maintenance of the National Incident Management System,
39the National Response Plan, and a successor to the system or plan.

40 (2) REVIEW AND REVISION OF SYSTEM AND PLAN.—The National
41Integration Center shall periodically review, and revise as appropriate,

1 the National Incident Management System and the National Response
2 Plan, including—

3 (A) establishing, in consultation with the Director of the Cor-
4 poration for National and Community Service, a process to better
5 use volunteers and donations;

6 (B) improving the use of Federal, State, local, and tribal re-
7 sources and ensuring the effective use of emergency response pro-
8 viders at emergency scenes; and

9 (C) revising the Catastrophic Incident Annex, finalizing and re-
10 leasing the Catastrophic Incident Supplement to the National Re-
11 sponse Plan, and ensuring that both effectively address response
12 requirements in the event of a catastrophic incident.

13 (e) INCIDENT MANAGEMENT.—

14 (1) IN GENERAL.—

15 (A) NATIONAL RESPONSE PLAN.—The Administrator shall en-
16 sure that the National Response Plan provides for a clear chain
17 of command to lead and coordinate the Federal response to a nat-
18 ural disaster, act of terrorism, or other man-made disaster.

19 (B) ADMINISTRATOR.—The chain of the command specified in
20 the National Response Plan shall provide for a role for—

21 (i) the Administrator consistent with the role of the Admin-
22 istrator as the principal emergency management advisor to
23 the President, the Homeland Security Council, and the Sec-
24 retary under section 11102(b)(2) of this title and the respon-
25 sibility of the Administrator under the Post-Katrina Emer-
26 gency Management Reform Act of 2006 (Public Law 109–
27 295, 120 Stat. 1394), and the amendments made by that
28 Act, relating to natural disasters, acts of terrorism, and other
29 man-made disasters; and

30 (ii) the Federal Coordinating Officer consistent with the re-
31 sponsibilities under section 302(b) of the Robert T. Stafford
32 Disaster Relief and Emergency Assistance Act (42 U.S.C.
33 5143(b)).

34 (2) PRINCIPAL FEDERAL OFFICIAL OR DIRECTOR OF A JOINT TASK
35 FORCE.—The Principal Federal Official (or the successor to the Offi-
36 cial) or a Director of a Joint Task Force established under section
37 11508 of this title shall not—

38 (A) direct or replace the incident command structure established
39 at the incident; or

1 (B) have directive authority over the Senior Federal Law En-
2 forcement Official, Federal Coordinating Officer, or other Federal
3 and State officials.

4 **§ 11110. Credentialing and typing**

5 (a) IN GENERAL.—The Administrator shall enter into a memorandum of
6 understanding with the administrators of the Emergency Management As-
7 sistance Compact, State, local, and tribal governments, and organizations
8 that represent emergency response providers, to collaborate on developing
9 standards for deployment capabilities, including for credentialing and typing
10 of incident management personnel, emergency response providers, and other
11 personnel (including temporary personnel) and resources likely needed to re-
12 spond to natural disasters, acts of terrorism, and other man-made disasters.

13 (b) DISTRIBUTION.—

14 (1) IN GENERAL.—The Administrator shall provide the standards de-
15 veloped under subsection (a), including detailed written guidance, to—

16 (A) each Federal agency that has responsibilities under the Na-
17 tional Response Plan to aid that agency with credentialing and
18 typing incident management personnel, emergency response pro-
19 viders, and other personnel (including temporary personnel) and
20 resources likely needed to respond to a natural disaster, act of ter-
21 rorism, or other man-made disaster; and

22 (B) State, local, and tribal governments, to aid the governments
23 with credentialing and typing of State, local, and tribal incident
24 management personnel, emergency response providers, and other
25 personnel (including temporary personnel) and resources likely
26 needed to respond to a natural disaster, act of terrorism, or other
27 man-made disaster.

28 (2) ASSISTANCE.—The Administrator shall provide expertise and
29 technical assistance to aid Federal, State, local, and tribal government
30 agencies with credentialing and typing incident management personnel,
31 emergency response providers, and other personnel (including tem-
32 porary personnel) and resources likely needed to respond to a natural
33 disaster, act of terrorism, or other man-made disaster.

34 (c) CREDENTIALING AND TYPING OF PERSONNEL.—Each Federal agency
35 with responsibilities under the National Response Plan shall ensure that in-
36 cident management personnel, emergency response providers, and other per-
37 sonnel (including temporary personnel) and resources likely needed to re-
38 spond to a natural disaster, act of terrorism, or other manmade disaster are
39 credentialed and typed under this section.

40 (d) CONSULTATION ON HEALTH CARE STANDARDS.—In developing
41 standards for credentialing health care professionals under this section, the

1 Administrator shall consult with the Secretary of Health and Human Serv-
2 ices.

3 **§ 11111. National Infrastructure Simulation and Analysis**
4 **Center**

5 (a) IN GENERAL.—There is in the Department the National Infrastruc-
6 ture Simulation and Analysis Center established under the Critical Infra-
7 structure Protection Act of 2001 (42 U.S.C. 5195e(d)) which shall serve as
8 a source of national expertise to address critical infrastructure protection
9 and continuity through support for activities related to—

- 10 (1) counterterrorism, threat assessment, and risk mitigation; and
11 (2) a natural disaster, act of terrorism, or other man-made disaster.

12 (b) INFRASTRUCTURE MODELING.—

13 (1) PARTICULAR SUPPORT.—The support provided under subsection
14 (a) includes modeling, simulation, and analysis of the systems and as-
15 sets comprising critical infrastructure, to enhance preparedness, protec-
16 tion, response, recovery, and mitigation activities.

17 (2) RELATIONSHIP WITH OTHER AGENCIES.—Each Federal agency
18 and department with critical infrastructure responsibilities under
19 Homeland Security Presidential Directive–7, or a successor to the Di-
20 rective, shall establish a formal relationship, including an agreement re-
21 garding information sharing, between the elements of the agency or de-
22 partment and the National Infrastructure Simulation and Analysis
23 Center, through the Department.

24 (3) PURPOSE.—The purpose of the relationship under paragraph (2)
25 is to permit each Federal agency and department described in para-
26 graph (2) to take full advantage of the capabilities of the National In-
27 frastructure Simulation and Analysis Center (particularly vulnerability
28 and consequence analysis), consistent with its work load capacity and
29 priorities, for real-time response to reported and projected natural dis-
30 asters, acts of terrorism, and other man-made disasters.

31 (4) RECIPIENT OF CERTAIN SUPPORT.—Modeling, simulation, and
32 analysis provided under this subsection shall be provided to relevant
33 Federal agencies and departments, including Federal agencies and de-
34 partments with critical infrastructure responsibilities under Homeland
35 Security Presidential Directive–7, or a successor to the Directive.

36 **§ 11112. Evacuation plans and exercises**

37 (a) IN GENERAL.—Notwithstanding any other provision of law, and sub-
38 ject to subsection (d), grants made to States or local or tribal governments
39 by the Department through the State Homeland Security Grant Program
40 or the Urban Area Security Initiative may be used to—

1 (1) establish programs for the development and maintenance of mass
2 evacuation plans under subsection (b) in the event of a natural dis-
3 aster, act of terrorism, or other man-made disaster;

4 (2) prepare for the execution of the plans, including the development
5 of evacuation routes and the purchase and stockpiling of necessary sup-
6 plies and shelters; and

7 (3) conduct exercises of the plans.

8 (b) PLAN DEVELOPMENT.—In developing the mass evacuation plans au-
9 thorized under subsection (a), each State, local, or tribal government shall,
10 to the maximum extent practicable—

11 (1) establish incident command and decision-making processes;

12 (2) ensure that State, local, and tribal government plans, including
13 evacuation routes, are coordinated and integrated;

14 (3) identify primary and alternative evacuation routes and methods
15 to increase evacuation capabilities along the routes, such as conversion
16 of two-way traffic to one-way evacuation routes;

17 (4) identify evacuation transportation modes and capabilities, includ-
18 ing the use of mass and public transit capabilities, and coordinating
19 and integrating evacuation plans for all populations including for those
20 individuals located in hospitals, nursing homes, and other institutional
21 living facilities;

22 (5) develop procedures for informing the public of evacuation plans
23 before and during an evacuation, including individuals—

24 (A) with disabilities or other special needs, including the elderly;

25 (B) with limited English proficiency; or

26 (C) who might otherwise have difficulty in obtaining informa-
27 tion; and

28 (6) identify shelter locations and capabilities.

29 (c) ASSISTANCE.—

30 (1) IN GENERAL.—The Administrator may establish guidelines,
31 standards, or requirements determined appropriate to administer this
32 section and to ensure effective mass evacuation planning for State,
33 local, and tribal areas.

34 (2) REQUESTED ASSISTANCE.—The Administrator shall make assist-
35 ance available upon request of a State, local, or tribal government to
36 assist hospitals, nursing homes, and other institutions that house indi-
37 viduals with special needs to establish, maintain, and exercise mass
38 evacuation plans that are coordinated and integrated into the plans de-
39 veloped by that State, local, or tribal government under this section.

40 (d) MULTIPURPOSE FUNDS.—Nothing in this section may be construed
41 to preclude a State, local, or tribal government from using grant funds in

1 a manner that enhances preparedness for a natural or man-made disaster
2 unrelated to an act of terrorism, if the use assists the government in build-
3 ing capabilities for terrorism preparedness.

4 **§ 11113. Disability Coordinator**

5 (a) IN GENERAL.—After consultation with organizations representing in-
6 dividuals with disabilities, the National Council on Disability, and the Inter-
7 agency Coordinating Council on Emergency Preparedness and Individuals
8 with Disabilities, established under Executive Order No. 13347 (July 22,
9 2004, 69 Fed. Reg. 44573), the Administrator shall appoint a Disability
10 Coordinator. The Disability Coordinator shall report directly to the Admin-
11 istrator, in order to ensure that the needs of individuals with disabilities are
12 being properly addressed in emergency preparedness and disaster relief.

13 (b) RESPONSIBILITIES.—The Disability Coordinator is responsible for—

14 (1) providing guidance and coordination on matters related to indi-
15 viduals with disabilities in emergency planning requirements and relief
16 efforts in the event of a natural disaster, act of terrorism, or other
17 man-made disaster;

18 (2) interacting with the staff of the Agency, the National Council on
19 Disability, the Interagency Coordinating Council on Emergency Pre-
20 paredness and Individuals with Disabilities established under Executive
21 Order No. 13347 (July 22, 2004, 69 Fed. Reg. 44573), other agencies
22 of the Federal Government, and State, local, and tribal government au-
23 thorities regarding the needs of individuals with disabilities in emer-
24 gency planning requirements and relief efforts in the event of a natural
25 disaster, act of terrorism, or other man-made disaster;

26 (3) consulting with organizations that represent the interests and
27 rights of individuals with disabilities about the needs of individuals with
28 disabilities in emergency planning requirements and relief efforts in the
29 event of a natural disaster, act of terrorism, or other man-made dis-
30 aster;

31 (4) ensuring the coordination and dissemination of best practices and
32 model evacuation plans for individuals with disabilities;

33 (5) ensuring the development of training materials and a curriculum
34 for training of emergency response providers, State, local, and tribal
35 government officials, and others on the needs of individuals with dis-
36 abilities;

37 (6) promoting the accessibility of telephone hotlines and websites re-
38 garding emergency preparedness, evacuations, and disaster relief;

39 (7) working to ensure that video programming distributors, including
40 broadcasters, cable operators, and satellite television services, make

1 emergency information accessible to individuals with hearing and vision
2 disabilities;

3 (8) ensuring the availability of accessible transportation options for
4 individuals with disabilities in the event of an evacuation;

5 (9) providing guidance and implementing policies to ensure that the
6 rights and wishes of individuals with disabilities regarding post-evacu-
7 ation residency and relocation are respected;

8 (10) ensuring that meeting the needs of individuals with disabilities
9 is included in the components of the national preparedness system es-
10 tablished under section 644 of the Post-Katrina Emergency Manage-
11 ment Reform Act of 2006 (Public Law 109–295, 120 Stat. 1425); and

12 (11) other duties assigned by the Administrator.

13 **§ 11114. National Operations Center**

14 (a) DEFINITION OF SITUATIONAL AWARENESS.—In this section, the term
15 “situational awareness” means information gathered from a variety of
16 sources that, when communicated to emergency managers, decision makers,
17 and other appropriate officials, can form the basis for incident management
18 decisionmaking and steady-state activity.

19 (b) ESTABLISHMENT.—The National Operations Center is the principal
20 operations center for the Department and shall—

21 (1) provide situational awareness and a common operating picture
22 for the entire Federal Government, and for State, local, tribal, and ter-
23 ritorial governments, the private sector, and international partners as
24 appropriate, for events, threats, and incidents involving a natural dis-
25 aster, act of terrorism, or other man-made disaster;

26 (2) ensure that critical terrorism and disaster-related information
27 reaches government decision-makers; and

28 (3) enter into agreements with other Federal operations centers and
29 other homeland security partners, as appropriate, to facilitate the shar-
30 ing of information.

31 (c) STATE AND LOCAL EMERGENCY RESPONDER REPRESENTATION.—

32 (1) ESTABLISHMENT OF EMERGENCY RESPONDER POSITION.—The
33 Secretary shall establish a position, on a rotating basis, for a represent-
34 ative of State and local emergency responders at the National Oper-
35 ations Center established under subsection (b) to ensure the effective
36 sharing of information between the Federal Government and State and
37 local emergency response services.

38 (2) MANAGEMENT.—The Secretary shall manage the position estab-
39 lished under paragraph (1) in accordance with the rules, regulations,
40 and practices that govern other similar rotating positions at the Na-
41 tional Operations Center.

§ 11115. Responsibilities of Chief Medical Officer

The Chief Medical Officer has the primary responsibility in the Department for medical issues related to natural disasters, acts of terrorism, and other man-made disasters, including—

(1) serving as the principal advisor to the Secretary and the Administrator on medical and public health issues;

(2) coordinating the biodefense activities of the Department;

(3) ensuring internal and external coordination of all medical preparedness and response activities of the Department, including training, exercises, and equipment support;

(4) serving as the Department's primary point of contact with the Department of Agriculture, the Department of Defense, the Department of Health and Human Services, the Department of Transportation, the Department of Veterans Affairs, and other Federal departments or agencies, on medical and public health issues;

(5) serving as the Department's primary point of contact for State, local, and tribal governments, the medical community, and others within and outside the Department, with respect to medical and public health matters;

(6) discharging, in coordination with the Under Secretary for Science and Technology, the responsibilities of the Department related to Project Bioshield; and

(7) performing any other duties relating to these responsibilities that the Secretary may require.

§ 11116. Nuclear incident response

(a) IN GENERAL.—At the direction of the Secretary (in connection with an actual or threatened terrorist attack, major disaster, or other emergency in the United States), the Nuclear Incident Response Team shall operate as an organizational unit of the Department. While so operating, the Nuclear Incident Response Team shall be subject to the direction, authority, and control of the Secretary.

(b) RULE OF CONSTRUCTION.—Nothing in this chapter shall be construed to limit the ordinary responsibility of the Secretary of Energy and the Administrator of the Environmental Protection Agency for organizing, training, equipping, and utilizing their respective entities in the Nuclear Incident Response Team, or (subject to the provisions of this chapter) from exercising direction, authority, and control over them when they are not operating as a unit of the Department.

§ 11117. Conduct of certain public health-related activities

(a) IN GENERAL.—With respect to all public health-related activities to improve State, local, and hospital preparedness and response to chemical,

1 biological, radiological, and nuclear and other emerging terrorist threats car-
2 ried out by the Department of Health and Human Services (including the
3 Public Health Service), the Secretary of Health and Human Services shall
4 set priorities and preparedness goals and further develop a coordinated
5 strategy for these activities in collaboration with the Secretary.

6 (b) EVALUATION OF PROGRESS.—In carrying out subsection (a), the Sec-
7 retary of Health and Human Services shall collaborate with the Secretary
8 in developing specific benchmarks and outcome measurements for evaluating
9 progress toward achieving the priorities and goals described in subsection
10 (a).

11 **§ 11118. Use of national private-sector networks in emer-**
12 **gency response**

13 To the maximum extent practicable, the Secretary shall use national pri-
14 vate-sector networks and infrastructure for emergency response to chemical,
15 biological, radiological, nuclear, or explosive disasters, and other major dis-
16 asters.

17 **§ 11119. Model standards and guidelines for critical infra-**
18 **structure workers**

19 (a) IN GENERAL.—In coordination with appropriate national professional
20 organizations, Federal, State, local, and tribal government agencies, and pri-
21 vate-sector and nongovernmental entities, the Administrator shall establish
22 model standards and guidelines for credentialing critical infrastructure
23 workers that may be used by a State to credential critical infrastructure
24 workers that may respond to a natural disaster, act of terrorism, or other
25 man-made disaster.

26 (b) DISTRIBUTION AND ASSISTANCE.—The Administrator shall provide
27 the standards developed under subsection (a), including detailed written
28 guidance, to State, local, and tribal governments, and provide expertise and
29 technical assistance to aid the governments with credentialing critical infra-
30 structure workers that may respond to a natural disaster, act of terrorism,
31 or other man-made disaster.

32 **§ 11120. Guidance and recommendations**

33 (a) IN GENERAL.—Consistent with their responsibilities and authorities
34 under law, as of August 2, 2007, the Administrator and the Assistant Sec-
35 retary for Infrastructure Protection, in consultation with the private sector,
36 may develop guidance or recommendations and identify best practices to as-
37 sist or foster action by the private sector in—

38 (1) identifying potential hazards and assessing risks and impacts;

39 (2) mitigating the impact of a wide variety of hazards, including
40 weapons of mass destruction;

1 (3) managing necessary emergency preparedness and response re-
2 sources;

3 (4) developing mutual aid agreements;

4 (5) developing and maintaining emergency preparedness and re-
5 sponse plans, and associated operational procedures;

6 (6) developing and conducting training and exercises to support and
7 evaluate emergency preparedness and response plans and operational
8 procedures;

9 (7) developing and conducting training programs for security guards
10 to implement emergency preparedness and response plans and oper-
11 ations procedures; and

12 (8) developing procedures to respond to requests for information
13 from the media or the public.

14 (b) ISSUANCE AND PROMOTION.—Any guidance or recommendations de-
15 veloped or best practices identified under subsection (a) shall be—

16 (1) issued through the Administrator; and

17 (2) promoted by the Secretary to the private sector.

18 (c) SMALL BUSINESS CONCERNS.—In developing guidance or rec-
19 ommendations or identifying best practices under subsection (a), the Admin-
20 istrator and the Assistant Secretary for Infrastructure Protection shall take
21 into consideration small business concerns (under the meaning given that
22 term in section 3 of the Small Business Act (15 U.S.C. 632)), including
23 a need for separate guidance or recommendations or best practices, as nec-
24 essary and appropriate.

25 (d) RULE OF CONSTRUCTION.—Nothing in this section may be construed
26 to supersede a requirement established under any other provision of law.

27 **§ 11121. Voluntary private-sector preparedness accredita-**
28 **tion and certification program**

29 (a) ESTABLISHMENT.—

30 (1) IN GENERAL.—The Secretary, acting through the officer des-
31 ignated under paragraph (2), shall establish and implement the vol-
32 untary private-sector preparedness accreditation and certification pro-
33 gram under this section.

34 (2) DESIGNATION OF OFFICER.—The Secretary shall designate an
35 officer responsible for the accreditation and certification program under
36 this section. The officer (in this section referred to as the “designated
37 officer”) shall be one of the following:

38 (A) The Administrator, based on consideration of—

39 (i) the expertise of the Administrator in emergency man-
40 agement and preparedness in the United States; and

1 (ii) the responsibilities of the Administrator as the prin-
 2 cipal advisor to the President for all matters relating to emer-
 3 gency management in the United States.

4 (B) The Assistant Secretary for Infrastructure Protection,
 5 based on consideration of the expertise of the Assistant Secretary
 6 in, and responsibilities for—

- 7 (i) protection of critical infrastructure;
- 8 (ii) risk assessment methodologies; and
- 9 (iii) interacting with the private sector on the issues de-
 10 scribed in clauses (i) and (ii).

11 (C) The Under Secretary for Science and Technology, based on
 12 consideration of the expertise of the Under Secretary in, and re-
 13 sponsibilities associated with, standards.

14 (3) COORDINATION.—In carrying out the accreditation and certifi-
 15 cation program under this section, the designated officer shall coordi-
 16 nate with—

17 (A) the other officers of the Department referred to in para-
 18 graph (2), using the expertise and responsibilities of the officers;
 19 and

20 (B) the Special Assistant to the Secretary for the private sector,
 21 based on consideration of the expertise of the Special Assistant in,
 22 and responsibilities for, interacting with the private sector.

23 (b) VOLUNTARY PRIVATE-SECTOR PREPAREDNESS STANDARDS; VOL-
 24 UNTARY ACCREDITATION AND CERTIFICATION PROGRAM FOR THE PRIVATE
 25 SECTOR.—

26 (1) ACCREDITATION AND CERTIFICATION PROGRAM.—The designated
 27 officer shall—

28 (A) begin supporting the development and updating, as nec-
 29 essary, of voluntary preparedness standards through appropriate
 30 organizations that coordinate or facilitate the development and use
 31 of voluntary consensus standards and voluntary consensus stand-
 32 ards development organizations; and

33 (B) in consultation with representatives of appropriate organiza-
 34 tions that coordinate or facilitate the development and use of vol-
 35 untary consensus standards, appropriate voluntary consensus
 36 standards development organizations, each private-sector advisory
 37 council created under section 10321(4) of this title, appropriate
 38 representatives of State and local governments, including emer-
 39 gency management officials, and appropriate private-sector advi-
 40 sory groups, such as sector coordinating councils and information
 41 sharing and analysis centers—

1 (i) develop and promote a program to certify the prepared-
2 ness of private-sector entities that voluntarily choose to seek
3 certification under the program; and

4 (ii) implement the program under this subsection through
5 an entity with which the designated officer enters into an
6 agreement under paragraph (3)(A), which shall accredit third
7 parties to carry out the certification process under this sec-
8 tion.

9 (2) PROGRAM ELEMENTS.—

10 (A) IN GENERAL.—

11 (i) The program developed and implemented under this
12 subsection shall assess whether a private-sector entity com-
13 plies with voluntary preparedness standards.

14 (ii) In developing the program under this subsection, the
15 designated officer shall develop guidelines for the accredita-
16 tion and certification processes established under this sub-
17 section.

18 (B) STANDARDS.—The designated officer, in consultation with
19 representatives of appropriate organizations that coordinate or fa-
20 cilitate the development and use of voluntary consensus standards,
21 representatives of appropriate voluntary consensus standards de-
22 velopment organizations, each private-sector advisory council cre-
23 ated under section 10321(4) of this title, appropriate representa-
24 tives of State and local governments, including emergency manage-
25 ment officials, and appropriate private-sector advisory groups such
26 as sector coordinating councils and information sharing and anal-
27 ysis centers—

28 (i) shall adopt one or more appropriate voluntary prepared-
29 ness standards that promote preparedness, which may be tai-
30 lored to address the unique nature of various sectors in the
31 private sector, as necessary and appropriate, that shall be
32 used in the accreditation and certification program under this
33 subsection; and

34 (ii) after the adoption of one or more standards under
35 clause (i), may adopt additional voluntary preparedness
36 standards or modify or discontinue the use of voluntary pre-
37 paredness standards for the accreditation and certification
38 program, as necessary and appropriate to promote prepared-
39 ness.

40 (C) SUBMISSION OF RECOMMENDATIONS.—In adopting one or
41 more standards under subparagraph (B), the designated officer

1 may receive recommendations from an entity described in that
2 subparagraph relating to appropriate voluntary preparedness
3 standards, including appropriate sector specific standards, for
4 adoption in the program.

5 (D) SMALL BUSINESS CONCERNS.—The designated officer and
6 an entity with which the designated officer enters into an agree-
7 ment under paragraph (3)(A) shall establish separate classifica-
8 tions and methods of certification for small business concerns
9 (under the meaning given that term in section 3 of the Small
10 Business Act (15 U.S.C. 632)) for the program under this sub-
11 section.

12 (E) CONSIDERATIONS.—In developing and implementing the
13 program under this subsection, the designated officer shall—

14 (i) consider the unique nature of various sectors in the pri-
15 vate sector, including preparedness standards, business con-
16 tinuity standards, or best practices, established—

17 (I) under any other provision of Federal law; or

18 (II) by a sector-specific agency, as defined under
19 Homeland Security Presidential Directive-7; and

20 (ii) coordinate the program, as appropriate, with—

21 (I) other Department private-sector-related programs;

22 and

23 (II) preparedness and business continuity programs in
24 other Federal agencies.

25 (3) ACCREDITATION AND CERTIFICATION PROCESSES.—

26 (A) AGREEMENT.—

27 (i) The designated officer shall enter into one or more
28 agreements with a highly qualified nongovernmental entity
29 with experience or expertise in coordinating and facilitating
30 the development and use of voluntary consensus standards
31 and in managing or implementing accreditation and certifi-
32 cation programs for voluntary consensus standards, or a simi-
33 larly qualified private-sector entity, to carry out accreditations
34 and oversee the certification process under this subsection. An
35 entity entering into an agreement with the designated officer
36 under this clause (in this section referred to as a “selected
37 entity”) shall not perform certifications under this subsection.

38 (ii) A selected entity shall manage the accreditation process
39 and oversee the certification process in accordance with the
40 program established under this subsection and accredit quali-

1 fied third parties to carry out the certification program estab-
2 lished under this subsection.

3 (B) PROCEDURES AND REQUIREMENTS FOR ACCREDITATION
4 AND CERTIFICATION.—

5 (i) COLLABORATION.—A selected entity shall collaborate to
6 develop procedures and requirements for the accreditation
7 and certification processes under this subsection, in accord-
8 ance with the program established under this subsection and
9 guidelines developed under paragraph (2)(A)(ii).

10 (ii) REASONABLE UNIFORMITY; USE.—The procedures and
11 requirements developed under clause (i) shall—

12 (I) ensure reasonable uniformity in accreditation and
13 certification processes if there is more than one selected
14 entity; and

15 (II) be used by a selected entity in conducting accredi-
16 tations and overseeing the certification process under
17 this subsection.

18 (iii) RESOLUTION OF DISAGREEMENT.—A disagreement
19 among selected entities in developing procedures under clause
20 (i) shall be resolved by the designated officer.

21 (C) DESIGNATION.—A selected entity may accredit a qualified
22 third party to carry out the certification process under this sub-
23 section.

24 (D) DISADVANTAGED BUSINESS INVOLVEMENT.—In accrediting
25 qualified third parties to carry out the certification process under
26 this subsection, a selected entity shall ensure, to the extent prac-
27 ticable, that the third parties include qualified small, minority,
28 women-owned, or disadvantaged business concerns when appro-
29 priate. The term “disadvantaged business concern” means a small
30 business that is owned and controlled by socially and economically
31 disadvantaged individuals, as defined in section 124 of title 13,
32 Code of Federal Regulations.

33 (E) TREATMENT OF OTHER CERTIFICATIONS.—At the request
34 of an entity seeking certification, a selected entity may consider,
35 as appropriate, other relevant certifications acquired by the entity
36 seeking certification. If the selected entity determines that the
37 other certifications are sufficient to meet the certification require-
38 ment or aspects of the certification requirement under this section,
39 the selected entity may give credit to the entity seeking certifi-
40 cation, as appropriate, to avoid unnecessarily duplicative certifi-
41 cation requirements.

1 (F) THIRD PARTIES.—To be accredited under subparagraph
2 (C), a third party shall—

3 (i) demonstrate that the third party has the ability to cer-
4 tify private-sector entities in accordance with the procedures
5 and requirements developed subparagraph (B);

6 (ii) agree to perform certifications in accordance with the
7 procedures and requirements;

8 (iii) agree not to have a beneficial interest in or direct or
9 indirect control over—

10 (I) a private-sector entity for which that third party
11 conducts a certification under this subsection; or

12 (II) an organization that provides preparedness con-
13 sulting services to private-sector entities;

14 (iv) agree not to have any other conflict of interest with re-
15 spect to a private-sector entity for which the third party con-
16 ducts a certification under this subsection;

17 (v) maintain liability insurance coverage at policy limits in
18 accordance with the requirements developed under subpara-
19 graph (B); and

20 (vi) enter into an agreement with the selected entity ac-
21 crediting that third party to protect proprietary information
22 of a private-sector entity obtained under this subsection.

23 (G) MONITORING.—

24 (i) ENSURE COMPLIANCE.—The designated officer and an
25 selected entity shall regularly monitor and inspect the oper-
26 ations of a third party conducting certifications under this
27 subsection to ensure that the third party is complying with
28 the procedures and requirements established under subpara-
29 graph (B) and all other applicable requirements.

30 (ii) PROCEDURES OR REQUIREMENTS NOT MET.—If the
31 designated officer or a selected entity determines that a third
32 party is not meeting the procedures or requirements estab-
33 lished under subparagraph (B), the selected entity shall—

34 (I) revoke the accreditation of that third party to con-
35 duct certifications under this subsection; and

36 (II) review the certification conducted by that third
37 party, as necessary and appropriate.

38 (4) ANNUAL REVIEW.—

39 (A) IN GENERAL.—The designated officer, in consultation with
40 representatives of appropriate organizations that coordinate or fa-
41 cilitate the development and use of voluntary consensus standards,

1 appropriate voluntary consensus standards development organiza-
 2 tions, appropriate representatives of State and local governments,
 3 including emergency management officials, and each private-sector
 4 advisory council created under section 10321(4) of this title, shall
 5 annually review the voluntary accreditation and certification pro-
 6 gram established under this subsection to ensure the effectiveness
 7 of the program (including the operations and management of the
 8 program by a selected entity and the selected entity's inclusion of
 9 qualified disadvantaged business concerns under paragraph
 10 (3)(D)) and make improvements and adjustments to the program
 11 as necessary and appropriate.

12 (B) REVIEW OF STANDARDS.—Each review under subparagraph
 13 (A) shall include an assessment of the voluntary preparedness
 14 standard or standards used in the program under this subsection.

15 (5) VOLUNTARY PARTICIPATION.—Certification under this subsection
 16 shall be voluntary for a private-sector entity.

17 (6) PUBLIC LISTING.—The designated officer shall maintain and
 18 make public a listing of any private-sector entity certified as being in
 19 compliance with the program established under this subsection, if that
 20 private-sector entity consents to the listing.

21 (c) RULE OF CONSTRUCTION.—Nothing in this section may be construed
 22 as—

23 (1) a requirement to replace preparedness, emergency response, or
 24 business continuity standards, requirements, or best practices estab-
 25 lished—

26 (A) under any other provision of federal law; or

27 (B) by a sector-specific agency, as those agencies are defined
 28 under Homeland Security Presidential Directive–7; or

29 (2) exempting a private-sector entity seeking certification or meeting
 30 certification requirements under subsection (b) from compliance with
 31 all applicable statutes, regulations, directives, policies, and industry
 32 codes of practice.

33 § 11122. Acceptance of gifts

34 (a) AUTHORITY.—The Secretary may accept and use gifts of property,
 35 both real and personal, and may accept gifts of services, including from
 36 guest lecturers, for otherwise authorized activities of the Center for Domes-
 37 tic Preparedness that are related to efforts to prevent, prepare for, protect
 38 against, or respond to a natural disaster, act of terrorism, or other man-
 39 made disaster, including the use of a weapon of mass destruction.

1 (b) PROHIBITION.—The Secretary may not accept a gift under this sec-
2 tion if the Secretary determines that the use of the property or services
3 would compromise the integrity or appearance of integrity of—

4 (1) a program of the Department; or

5 (2) an individual involved in a program of the Department.

6 (c) REPORT.—

7 (1) IN GENERAL.—The Secretary shall submit to the Committee on
8 Homeland Security of the House of Representatives and the Committee
9 on Homeland Security and Governmental Affairs of the Senate an an-
10 nual report disclosing—

11 (A) gifts that were accepted under this section during the year
12 covered by the report;

13 (B) how the gifts contribute to the mission of the Center for
14 Domestic Preparedness; and

15 (C) the amount of Federal savings that were generated from the
16 acceptance of the gifts.

17 (2) PUBLICATION.—Each report required under paragraph (1) shall
18 be made publicly available.

19 **§ 11123. Integrated public alert and warning system mod-**
20 **ernization**

21 (a) IN GENERAL.—To provide timely and effective warnings regarding
22 natural disasters, acts of terrorism, and other man-made disasters or
23 threats to public safety, the Administrator shall—

24 (1) modernize the integrated public alert and warning system of the
25 United States (in this section referred to as the “public alert and warn-
26 ing system”) to help ensure that under all conditions the President
27 and, except to the extent the public alert and warning system is in use
28 by the President, Federal agencies and State, tribal, and local govern-
29 ments can alert and warn the civilian population in areas endangered
30 by natural disasters, acts of terrorism, and other man-made disasters
31 or threats to public safety; and

32 (2) implement the public alert and warning system to disseminate
33 timely and effective warnings regarding natural disasters, acts of ter-
34 rorism, and other man-made disasters or threats to public safety.

35 (b) IMPLEMENTATION REQUIREMENTS.—In carrying out subsection (a),
36 the Administrator shall—

37 (1) establish or adopt, as appropriate, common alerting and warning
38 protocols, standards, terminology, and operating procedures for the
39 public alert and warning system;

40 (2) include in the public alert and warning system the capability to
41 adapt the distribution and content of communications on the basis of

1 geographic location, risks, and multiple communication systems and
2 technologies, as appropriate and to the extent technically feasible;

3 (3) include in the public alert and warning system the capability to
4 alert, warn, and provide equivalent information to individuals with dis-
5 abilities, individuals with access and functional needs, and individuals
6 with limited-English proficiency, to the extent technically feasible;

7 (4) ensure that training, tests, and exercises are conducted for the
8 public alert and warning system, including by—

9 (A) incorporating the public alert and warning system into other
10 training and exercise programs of the Department, as appropriate;

11 (B) establishing and integrating into the National Incident
12 Management System a comprehensive and periodic training pro-
13 gram to instruct and educate Federal, State, tribal, and local gov-
14 ernment officials in the use of the Common Alerting Protocol en-
15 abled Emergency Alert System; and

16 (C) conducting, not less than once every 3 years, periodic na-
17 tionwide tests of the public alert and warning system;

18 (5) to the extent practicable, ensure that the public alert and warn-
19 ing system is resilient and secure and can withstand acts of terrorism
20 and other external attacks;

21 (6) conduct public education efforts so that State, tribal, and local
22 governments, private entities, and the people of the United States rea-
23 sonably understand the functions of the public alert and warning sys-
24 tem and how to access, use, and respond to information from the public
25 alert and warning system through a general market awareness cam-
26 paign;

27 (7) consult, coordinate, and cooperate with the appropriate private-
28 sector entities and Federal, State, tribal, and local governmental au-
29 thorities, including the Regional Administrators and emergency re-
30 sponse providers;

31 (8) consult and coordinate with the Federal Communications Com-
32 mission, taking into account rules and regulations promulgated by the
33 Federal Communications Commission; and

34 (9) coordinate with and consider the recommendations of the Inte-
35 grated Public Alert and Warning System Subcommittee established
36 under section 2(b) of the Integrated Public Alert and Warning System
37 Modernization Act of 2015 (Public Law 114–143, 130 Stat. 329).

38 (c) SYSTEM REQUIREMENTS.—The public alert and warning system
39 shall—

40 (1) to the extent determined appropriate by the Administrator, incor-
41 porate multiple communications technologies;

1 (2) be designed to adapt to, and incorporate, future technologies for
2 communicating directly with the public;

3 (3) to the extent technically feasible, be designed—

4 (A) to provide alerts to the largest portion of the affected popu-
5 lation feasible, including nonresident visitors and tourists, individ-
6 uals with disabilities, individuals with access and functional needs,
7 and individuals with limited-English proficiency; and

8 (B) to improve the ability of remote areas to receive alerts;

9 (4) promote local and regional public and private partnerships to en-
10 hance community preparedness and response;

11 (5) provide redundant alert mechanisms where practicable so as to
12 reach the greatest number of people; and

13 (6) to the extent feasible, include a mechanism to ensure the protec-
14 tion of individual privacy.

15 (d) USE OF SYSTEM.—Except to the extent necessary for testing the pub-
16 lic alert and warning system, the public alert and warning system shall not
17 be used to transmit a message that does not relate to a natural disaster,
18 act of terrorism, or other man-made disaster or threat to public safety.

19 (e) PERFORMANCE REPORTS.—

20 (1) IN GENERAL.—Not later than April 11, 2017, and 2018, the Ad-
21 ministrator shall make available on the public website of the Agency
22 a performance report, which shall—

23 (A) establish performance goals for the implementation of the
24 public alert and warning system by the Agency;

25 (B) describe the performance of the public alert and warning
26 system, including—

27 (i) the type of technology used for alerts and warnings
28 issued under the system;

29 (ii) the measures taken to alert, warn, and provide equiva-
30 lent information to individuals with disabilities, individuals
31 with access and functional needs, and individuals with lim-
32 ited-English proficiency; and

33 (iii) the training, tests, and exercises performed and the
34 outcomes obtained by the Agency;

35 (C) identify significant challenges to the effective operation of
36 the public alert and warning system and any plans to address the
37 challenges;

38 (D) identify other necessary improvements to the system; and

39 (E) provide an analysis comparing the performance of the public
40 alert and warning system with the performance goals established
41 under subparagraph (A).

1 (2) SUBMISSION TO CONGRESS.—The Administrator shall submit to
 2 the Committee on Homeland Security and Governmental Affairs and
 3 the Committee on Commerce, Science, and Transportation of the Sen-
 4 ate and the Committee on Transportation and Infrastructure and the
 5 Committee on Homeland Security of the House of Representatives each
 6 report required under paragraph (1).

7 **§ 11124. National planning and education**

8 The Secretary shall, to the extent practicable—

9 (1) include in national planning frameworks the threat of an EMP
 10 or GMD event; and

11 (2) conduct outreach to educate owners and operators of critical in-
 12 frastructure, emergency planners, and emergency response providers at
 13 all levels of government regarding threats of EMP and GMD.

14 **Chapter 113—Transportation Security**
 15 **Administration**

Subchapter I—General

Sec.

- 11301. Functions.
- 11302. National emergency responsibilities.
- 11303. Management of security information.
- 11304. View of National Transportation Safety Board.
- 11305. Acquisitions.
- 11306. Transfers of funds.
- 11307. Regulations.
- 11308. Personnel and services.
- 11309. Personnel management system.
- 11310. Authority of Inspector General.
- 11311. Law enforcement powers.
- 11312. Authority to exempt.
- 11313. Nondisclosure of security activities.
- 11314. Transportation security strategic planning.
- 11315. Transportation Security Information Sharing Plan.
- 11316. Enforcement of certain regulations and orders of the Secretary.
- 11317. Registered traveler fee.
- 11318. Enhanced security measures.
- 11319. Performance management system.
- 11320. Voluntary provision of emergency services.
- 11321. Disposition of unclaimed money and clothing.

Subchapter II—Acquisition Improvements

- 11331. Definitions.
- 11332. Technology investment plan.
- 11333. Acquisition justification and reports and certification.
- 11334. Baseline establishment and reports.
- 11335. Inventory utilization.
- 11336. Small business contracting goals.
- 11337. Consistency with Federal Acquisition Regulation and Department policies and direc-
 tives.

16 **Subchapter I—General**

17 **§ 11301. Functions**

18 (a) FUNCTIONS.—The Administrator of the Transportation Security Ad-
 19 ministration (in this chapter referred to as the “Administrator”), is respon-
 20 sible for security in all modes of transportation, including—

1 (1) carrying out chapter 409 of this title and related research and
2 development activities; and

3 (2) security responsibilities over other modes of transportation that
4 were exercised by the Department of Transportation prior to March 1,
5 2003.

6 (b) SCREENING OPERATIONS.—The Administrator shall—

7 (1) be responsible for day-to-day Federal security screening oper-
8 ations for passenger air transportation and intrastate air transpor-
9 tation under sections 40911 and 40953 of this title;

10 (2) develop standards for the hiring and retention of security screen-
11 ing personnel;

12 (3) train and test security screening personnel; and

13 (4) be responsible for hiring and training personnel to provide secu-
14 rity screening at all airports in the United States where screening is
15 required under section 40911 of this title, in consultation with the Sec-
16 retary of Transportation and the heads of other appropriate Federal
17 agencies and departments.

18 (c) ADDITIONAL DUTIES AND POWERS.—In addition to carrying out the
19 functions specified in subsections (a) and (b), the Administrator shall—

20 (1) receive, assess, and distribute intelligence information related to
21 transportation security;

22 (2) assess threats to transportation;

23 (3) develop policies, strategies, and plans for dealing with threats to
24 transportation security;

25 (4) make other plans related to transportation security, including co-
26 ordinating countermeasures with appropriate departments, agencies,
27 and instrumentalities of the United States Government;

28 (5) serve as the primary liaison for transportation security to the in-
29 telligence and law enforcement communities;

30 (6) on a day-to-day basis, manage and provide operational guidance
31 to the field security resources of the Transportation Security Adminis-
32 tration, including Federal Security Managers as provided by section
33 40951 of this title;

34 (7) enforce security-related regulations and requirements;

35 (8) identify and undertake research and development activities nec-
36 essary to enhance transportation security;

37 (9) inspect, maintain, and test security facilities, equipment, and sys-
38 tems;

39 (10) ensure the adequacy of security measures for the transportation
40 of cargo;

1 (11) oversee the implementation, and ensure the adequacy, of secu-
2 rity measures at airports and other transportation facilities;

3 (12) require background checks for airport security screening per-
4 sonnel, individuals with access to secure areas of airports, and other
5 transportation security personnel;

6 (13) work in conjunction with the Administrator of the Federal Avia-
7 tion Administration with respect to actions or activities that may affect
8 aviation safety or air carrier operations;

9 (14) work with the International Civil Aviation Organization and ap-
10 propriate aeronautic authorities of foreign governments under section
11 40917 of this title, to address security concerns on passenger flights
12 by foreign air carriers in foreign air transportation; and

13 (15) carry out other duties, and exercise other powers, relating to
14 transportation security the Administrator considers appropriate, to the
15 extent authorized by law.

16 **§ 11302. National emergency responsibilities**

17 (a) IN GENERAL.—The Administrator, during a national emergency, has
18 the following responsibilities:

19 (1) To coordinate domestic transportation, including aviation, rail,
20 and other surface transportation, and maritime transportation (includ-
21 ing port security).

22 (2) To coordinate and oversee the transportation-related responsibil-
23 ities of other departments and agencies of the Federal Government
24 other than the Department of Defense and the military departments.

25 (3) To coordinate and provide notice to other departments and agen-
26 cies of the Federal Government, and appropriate agencies of State and
27 local governments, including departments and agencies for transpor-
28 tation, law enforcement, and border control, about threats to transpor-
29 tation.

30 (4) To carry out other duties, and exercise other powers, relating to
31 transportation during a national emergency, that the Secretary shall
32 prescribe.

33 (b) AUTHORITY OF OTHER DEPARTMENTS AND AGENCIES.—The author-
34 ity of the Administrator under this section shall not supersede the authority
35 of another department or agency of the Federal Government under law with
36 respect to transportation or transportation-related matters, whether or not
37 during a national emergency.

38 (c) CIRCUMSTANCES.—The Secretary shall prescribe the circumstances
39 constituting a national emergency for purposes of this section.

1 **§ 11303. Management of security information**

2 In consultation with the Transportation Security Oversight Board, the
3 Administrator shall—

4 (1) enter into memoranda of understanding with Federal agencies or
5 other entities to share or otherwise cross-check as necessary data on
6 individuals identified on Federal agency databases who may pose a risk
7 to transportation or national security;

8 (2) establish procedures for notifying the Administrator of the Fed-
9 eral Aviation Administration, appropriate State and local law enforce-
10 ment officials, and airport or airline security officers of the identity of
11 individuals known to pose, or suspected of posing, a risk of air piracy
12 or terrorism or a threat to airline or passenger safety;

13 (3) in consultation with other appropriate Federal agencies and air
14 carriers, establish policies and procedures requiring air carriers—

15 (A) to use information from government agencies to identify in-
16 dividuals on passenger lists who may be a threat to civil aviation
17 or national security; and

18 (B) if such an individual is identified, notify appropriate law en-
19 forcement agencies, prevent the individual from boarding an air-
20 craft, or take other appropriate action with respect to that indi-
21 vidual; and

22 (4) consider requiring passenger air carriers to share passenger lists
23 with appropriate Federal agencies for the purpose of identifying indi-
24 viduals who may pose a threat to aviation safety or national security.

25 **§ 11304. View of National Transportation Safety Board**

26 In taking an action under this section that could affect safety, the Admin-
27 istrator shall give great weight to the timely views of the National Transpor-
28 tation Safety Board.

29 **§ 11305. Acquisitions**

30 (a) IN GENERAL.—The Administrator may—

31 (1) acquire (by purchase, lease, condemnation, or otherwise) real
32 property, or an interest in the property, in and outside the continental
33 United States, that the Administrator considers necessary;

34 (2) acquire (by purchase, lease, condemnation, or otherwise) and to
35 construct, repair, operate, and maintain personal property (including
36 office space and patents), or an interest in the property, in and outside
37 the continental United States, that the Administrator considers nec-
38 essary;

39 (3) lease to others the real and personal property and to provide by
40 contract or otherwise for necessary facilities for the welfare of Trans-

1 portation Security Administration employees and to acquire, maintain,
2 and operate equipment for these facilities;

3 (4) acquire services, including personal services the Secretary deter-
4 mines necessary, and to acquire (by purchase, lease, condemnation, or
5 otherwise) and to construct, repair, operate, and maintain research and
6 testing sites and facilities; and

7 (5) in cooperation with the Administrator of the Federal Aviation
8 Administration, utilize the research and development facilities of the
9 Federal Aviation Administration.

10 (b) TITLE.—Title to property or an interest in property acquired under
11 this section shall be held by the Government of the United States.

12 (c) CHARGE FOR LEASE OF REAL AND PERSONAL PROPERTY.—Notwith-
13 standing section 3302 of title 31, the Administrator may impose a reason-
14 able charge for the lease of real and personal property to Transportation
15 Security Administration employees and for use by Transportation Security
16 Administration employees and may credit amounts received to the appro-
17 priation or fund initially charged for operating and maintaining the prop-
18 erty. The amounts are available, without fiscal year limitation, for expendi-
19 ture for property management, operation, protection, construction, repair,
20 alteration, and related activities.

21 **§ 11306. Transfers of funds**

22 The Administrator may accept transfers of unobligated balances and un-
23 expended balances of funds appropriated to other Federal agencies (as the
24 term “agency” is defined in section 551(1) of title 5) to carry out functions
25 transferred, on or after November 19, 2001, by law to the Administrator.

26 **§ 11307. Regulations**

27 (a) IN GENERAL.—The Administrator may issue, rescind, and revise reg-
28 ulations as necessary to carry out the functions of the Transportation Secu-
29 rity Administration.

30 (b) EMERGENCY PROCEDURES.—

31 (1) IN GENERAL.—Notwithstanding any other provision of law or ex-
32 ecutive order (including an executive order requiring a cost-benefit
33 analysis), if the Administrator determines that a regulation or security
34 directive must be issued immediately in order to protect transportation
35 security, the Administrator shall issue the regulation or security direc-
36 tive without providing notice or an opportunity for comment and with-
37 out prior approval of the Secretary.

38 (2) REVIEW BY TRANSPORTATION SECURITY OVERSIGHT BOARD.—A
39 regulation or security directive issued under this subsection shall be
40 subject to review by the Transportation Security Oversight Board es-
41 tablished under section 10320 of this title. A regulation or security di-

1 rective issued under this subsection shall remain effective for a period
2 not to exceed 90 days unless ratified or disapproved by the Board or
3 rescinded by the Secretary.

4 (e) FACTORS TO CONSIDER.—In determining whether to issue, rescind,
5 or revise a regulation under this chapter, the Administrator shall consider,
6 as a factor in the final determination, whether the costs of the regulation
7 are excessive in relation to the enhancement of security the regulation will
8 provide. The Administrator may waive requirements for an analysis that es-
9 timates the number of lives that will be saved by the regulation and the
10 monetary value of lives if the Administrator determines that it is not fea-
11 sible to make an estimate.

12 (d) AIRWORTHINESS OBJECTIONS BY FEDERAL AVIATION ADMINISTRA-
13 TION.—

14 (1) IN GENERAL.—The Administrator shall not take an aviation se-
15 curity action under this title if the Administrator of the Federal Avia-
16 tion Administration notifies the Administrator that the action could ad-
17 versely affect the airworthiness of an aircraft.

18 (2) REVIEW BY ADMINISTRATOR.—Notwithstanding paragraph (1),
19 the Administrator may take an aviation security action, after receiving
20 a notification concerning the action from the Administrator of the Fed-
21 eral Aviation Administration under paragraph (1), if the Secretary sub-
22 sequently approves the action.

23 **§ 11308. Personnel and services**

24 (a) AUTHORITY OF ADMINISTRATOR.—In carrying out the functions of
25 the Transportation Security Administration, the Administrator has the same
26 authority as is provided to the Administrator of the Federal Aviation Ad-
27 ministration under subsections (l) and (m) of section 106 of title 49.

28 (b) AUTHORITY OF AGENCY HEADS.—The head of a Federal agency shall
29 have the same authority to provide services, supplies, equipment, personnel,
30 and facilities to the Secretary as the head has to provide services, supplies,
31 equipment, personnel, and facilities to the Administrator of the Federal
32 Aviation Administration under section 106(m) of title 49.

33 **§ 11309. Personnel management system**

34 (a) IN GENERAL.—The personnel management system established by the
35 Administrator of the Federal Aviation Administration under section 40122
36 of title 49 applies to employees of the Transportation Security Administra-
37 tion

38 (b) MODIFICATIONS.—Subject to the requirements of section 40122 of
39 title 49, the Administrator may make modifications to the personnel man-
40 agement system with respect to such employees as the Administrator con-
41 siders appropriate.

1 **§ 11310. Authority of Inspector General**

2 The Transportation Security Administration is subject to the Inspector
3 General Act of 1978 (5 U.S.C. App.) and other laws relating to the author-
4 ity of the Inspector General of the Department.

5 **§ 11311. Law enforcement powers**

6 (a) IN GENERAL.—The Administrator may designate an employee of the
7 Transportation Security Administration or other Federal agency to serve as
8 a law enforcement officer.

9 (b) POWERS.—While engaged in official duties of the Transportation Se-
10 curity Administration as required to fulfill the responsibilities under this
11 section, a law enforcement officer designated under paragraph (1) may—

12 (1) carry a firearm;

13 (2) make an arrest without a warrant for any offense against the
14 United States committed in the presence of the officer, or for any fel-
15 ony cognizable under the laws of the United States if the officer has
16 probable cause to believe that the person to be arrested has committed
17 or is committing the felony; and

18 (3) seek and execute warrants for arrest or seizure of evidence issued
19 under the authority of the United States upon probable cause that a
20 violation has been committed.

21 (c) GUIDELINES ON EXERCISE OF AUTHORITY.—The authority provided
22 by this section shall be exercised in accordance with guidelines prescribed
23 by the Administrator, in consultation with the Attorney General, and shall
24 include adherence to the Attorney General’s policy on use of deadly force.

25 (d) REVOCATION OR SUSPENSION OF AUTHORITY.—The powers author-
26 ized by this section may be rescinded or suspended should the Attorney
27 General determine that the Administrator has not complied with the guide-
28 lines prescribed in paragraph (3) and conveys the determination in writing
29 to the Secretary and the Administrator.

30 **§ 11312. Authority to exempt**

31 The Administrator may grant an exemption from a regulation prescribed
32 in carrying out this chapter if the Administrator determines that the exemp-
33 tion is in the public interest.

34 **§ 11313. Nondisclosure of security activities**

35 (a) IN GENERAL.—Notwithstanding section 552 of title 5, the Adminis-
36 trator shall prescribe regulations prohibiting the disclosure of information
37 obtained or developed in carrying out security under authority of chapter
38 409 of this title or the Aviation and Transportation Security Act (Public
39 Law 107–71, 115 Stat. 597) if the Administrator decides that disclosing the
40 information would—

41 (1) be an unwarranted invasion of personal privacy;

1 (2) reveal a trade secret or privileged or confidential commercial or
2 financial information; or

3 (3) be detrimental to the security of transportation.

4 (b) AVAILABILITY OF INFORMATION TO CONGRESS.—Subsection (a) does
5 not authorize information to be withheld from a committee of Congress au-
6 thorized to have the information.

7 (c) LIMITATION ON TRANSFERABILITY OF DUTIES.—Except as otherwise
8 provided by law, the Administrator may not transfer a duty or power under
9 this section to another department, agency, or instrumentality of the United
10 States.

11 (d) LIMITATIONS.—Nothing in this section, or any other provision of law,
12 shall be construed to authorize the designation of information as sensitive
13 security information (as defined in section 1520.5 of title 49, Code of Fed-
14 eral Regulations)—

15 (1) to conceal a violation of law, inefficiency, or administrative error;

16 (2) to prevent embarrassment to a person, organization, or agency;

17 (3) to restrain competition; or

18 (4) to prevent or delay the release of information that does not re-
19 quire protection in the interest of transportation security, including
20 basic scientific research information not clearly related to transpor-
21 tation security.

22 **§ 11314. Transportation security strategic planning**

23 (a) IN GENERAL.—The Secretary shall develop, prepare, implement, and
24 update, as needed—

25 (1) a National Strategy for Transportation Security; and

26 (2) transportation modal security plans addressing security risks, in-
27 cluding threats, vulnerabilities, and consequences, for aviation, railroad,
28 ferry, highway, maritime, pipeline, public transportation, over-the-road
29 bus, and other transportation infrastructure assets.

30 (b) ROLE OF SECRETARY OF TRANSPORTATION.—The Secretary shall
31 work jointly with the Secretary of Transportation in developing, revising,
32 and updating the documents required by paragraph (1).

33 (c) CONTENTS OF NATIONAL STRATEGY FOR TRANSPORTATION SECU-
34 RITY.—The National Strategy for Transportation Security shall include the
35 following:

36 (1) An identification and evaluation of the transportation assets in
37 the United States that, in the interests of national security and com-
38 merce, must be protected from attack or disruption by terrorist or
39 other hostile forces, including modal security plans for aviation, bridge
40 and tunnel, commuter rail and ferry, highway, maritime, pipeline, rail,

1 mass transit, over-the-road bus, and other public transportation infra-
2 structure assets that could be at risk of attack or disruption.

3 (2) The development of risk-based priorities, based on risk assess-
4 ments conducted or received by the Secretary (including assessments
5 conducted under the Implementing Recommendations of the 9/11 Com-
6 mission Act of 2007 (Public Law 110–53, 121 Stat. 266)), across all
7 transportation modes and realistic deadlines for addressing security
8 needs associated with those assets referred to in paragraph (1).

9 (3) The most appropriate, practical, and cost-effective means of de-
10 fending those assets against threats to their security.

11 (4) A forward-looking strategic plan that sets forth the agreed upon
12 roles and missions of Federal, State, regional, local, and tribal authori-
13 ties and establishes mechanisms for encouraging cooperation and par-
14 ticipation by private-sector entities, including nonprofit employee labor
15 organizations, in the implementation of the plan.

16 (5) A comprehensive delineation of prevention, response, and recov-
17 ery responsibilities and issues regarding threatened and executed acts
18 of terrorism within the United States and threatened and executed acts
19 of terrorism outside the United States to the extent the acts affect
20 United States transportation systems.

21 (6) A prioritization of research and development objectives that sup-
22 port transportation security needs, giving a higher priority to research
23 and development directed toward protecting vital transportation assets.
24 Transportation security research and development projects shall be
25 based, to the extent practicable, on the prioritization. Nothing in the
26 preceding sentence shall be construed to require the termination of a
27 research or development project initiated by the Secretary or the Sec-
28 retary of Transportation before August 3, 2007.

29 (7) A 3- and 10-year budget for Federal transportation security pro-
30 grams that will achieve the priorities of the National Strategy for
31 Transportation Security.

32 (8) Methods for linking the individual transportation modal security
33 plans and the programs contained therein, and a plan for addressing
34 the security needs of intermodal transportation.

35 (9) Transportation modal security plans described in subsection
36 (a)(2), including operational recovery plans to expedite, to the max-
37 imum extent practicable, the return to operation of an adversely af-
38 fected transportation system following a major terrorist attack on that
39 system or other incident. These plans shall be coordinated with the re-
40 sumption of trade protocols required under section 30502 of this title

1 and the National Maritime Transportation Security Plan required
2 under section 70103(a) of title 46.

3 (d) SUBMISSIONS OF PLANS TO CONGRESS.—

4 (1) DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEES.—

5 In this subsection, the term “appropriate congressional committees”
6 means the Committee on Transportation and Infrastructure and the
7 Committee on Homeland Security of the House of Representatives and
8 the Committee on Commerce, Science, and Transportation, the Com-
9 mittee on Homeland Security and Governmental Affairs, and the Com-
10 mittee on Banking, Housing, and Urban Affairs of the Senate.

11 (2) BIENNIAL STRATEGY REPORT.—The Secretary shall submit the
12 National Strategy for Transportation Security, including the transpor-
13 tation modal security plans and any revisions to the National Strategy
14 for Transportation Security and the transportation modal security
15 plans, to appropriate congressional committees not less frequently than
16 April 1 of each even-numbered year.

17 (3) PERIODIC PROGRESS REPORT.—

18 (A) REQUIREMENT FOR REPORT.—Each year, in conjunction
19 with the submission of the budget to Congress under section
20 1105(a) of title 31, the Secretary shall submit to the appropriate
21 congressional committees an assessment of the progress made on
22 implementing the National Strategy for Transportation Security,
23 including the transportation modal security plans.

24 (B) CONTENT.—Each progress report submitted under this
25 paragraph shall include, at a minimum, the following:

26 (i) Recommendations for improving and implementing the
27 National Strategy for Transportation Security and the trans-
28 portation modal and intermodal security plans that the Sec-
29 retary of Homeland Security, in consultation with the Sec-
30 retary of Transportation, considers appropriate.

31 (ii) An accounting of all grants for transportation security,
32 including grants and contracts for research and development,
33 awarded by the Secretary in the most recent fiscal year and
34 a description of how the grants accomplished the goals of the
35 National Strategy for Transportation Security.

36 (iii) An accounting of all—

37 (I) funds requested in the President’s budget sub-
38 mitted pursuant to section 1105 of title 31 for the most
39 recent fiscal year for transportation security, by mode;

40 (II) personnel working on transportation security by
41 mode, including the number of contractors; and

1 (III) information on the turnover in the previous year
2 among senior staff of the Department, including compo-
3 nent agencies, working on transportation security issues.
4 The information shall include the number of employees
5 who have permanently left the office, agency, or area in
6 which they worked, and the amount of time that they
7 worked for the Department.

8 (C) WRITTEN EXPLANATION OF TRANSPORTATION SECURITY
9 ACTIVITIES NOT DELINEATED IN THE NATIONAL STRATEGY FOR
10 TRANSPORTATION SECURITY.—At the end of each fiscal year, the
11 Secretary shall submit to the appropriate congressional committees
12 a written explanation of a Federal transportation security activity
13 that is inconsistent with the National Strategy for Transportation
14 Security, including the amount of funds to be expended for the ac-
15 tivity and the number of personnel involved.

16 (4) CLASSIFIED MATERIAL.—Any part of the National Strategy for
17 Transportation Security, or any part of the transportation modal secu-
18 rity plans, that involves information that is properly classified under
19 criteria established by Executive order shall be submitted to the appro-
20 priate congressional committees separately in a classified format.

21 (e) PRIORITY STATUS.—

22 (1) IN GENERAL.—The National Strategy for Transportation Secu-
23 rity shall be the governing document for Federal transportation secu-
24 rity efforts.

25 (2) OTHER PLANS AND REPORTS.—The National Strategy for Trans-
26 portation Security shall include, as an integral part or as an appen-
27 dix—

28 (A) the current National Maritime Transportation Security Plan
29 under section 70103 of title 46;

30 (B) the report required by section 40956 of this title;

31 (C) transportation modal security plans required under this
32 chapter;

33 (D) the transportation sector specific plan required under
34 Homeland Security Presidential Directive–7; and

35 (E) another transportation security plan or report that the Sec-
36 retary determines appropriate for inclusion.

37 (f) COORDINATION.—In carrying out the responsibilities under this sec-
38 tion, the Secretary, in coordination with the Secretary of Transportation,
39 shall consult, as appropriate, with Federal, State, and local agencies, tribal
40 governments, private-sector entities (including nonprofit employee labor or-
41 ganizations), institutions of higher learning, and other entities.

1 (g) PLAN DISTRIBUTION.—The Secretary shall make available and appro-
2 priately publicize an unclassified version of the National Strategy for Trans-
3 portation Security, including its component transportation modal security
4 plans, to Federal, State, regional, local and tribal authorities, transportation
5 system owners or operators, private-sector stakeholders, including nonprofit
6 employee labor organizations representing transportation employees, institu-
7 tions of higher learning, and other appropriate entities.

8 **§ 11315. 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 11314 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, acting through the Ad-
26 ministrator and in consultation with the program manager of the informa-
27 tion sharing environment established under section 11708 of this title, the
28 Secretary of Transportation, and public and private stakeholders, shall es-
29 tablish a Transportation Security Information Sharing Plan. In establishing
30 the Plan, the Secretary shall gather input on the development of the Plan
31 from private and public stakeholders and the program manager of the infor-
32 mation sharing environment established under section 11708 of this title.

33 (c) PURPOSE OF PLAN.—The Plan shall promote 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 40508 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 within the Department
7 that has the primary authority, or has been delegated the authority by
8 the 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 11708 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, not later than Decem-
20 ber 31 each year, submit to the appropriate congressional committees, a re-
21 port containing the Plan.

22 (g) COMPTROLLER GENERAL SURVEY AND REPORT.—

23 (1) BIENNIAL SURVEY.—

24 (A) IN GENERAL.—The Comptroller General shall conduct a bi-
25 ennial survey of the satisfaction of recipients of transportation in-
26 telligence reports disseminated under the Plan.

27 (B) INFORMATION SOUGHT.—The survey conducted under sub-
28 paragraph (A) shall seek information about the quality, speed, reg-
29 ularity, and classification of the transportation security informa-
30 tion products disseminated by the Department to public and pri-
31 vate stakeholders.

32 (2) REPORT.—The Comptroller General shall, each even-numbered
33 year, submit to the appropriate congressional committees, a report on
34 the results of the survey conducted under paragraph (1). The Comp-
35 troller General shall also provide a copy of the report to the Secretary.

36 (h) SECURITY CLEARANCES.—The Secretary shall, to the greatest extent
37 practicable, take steps to expedite the security clearances needed for des-
38 ignated public and private stakeholders to receive and obtain access to clas-
39 sified information distributed under this section, as appropriate.

1 (i) CLASSIFICATION OF MATERIAL.—The Secretary, to the greatest extent
 2 practicable, shall provide designated public and private stakeholders with
 3 transportation security information in an unclassified format.

4 (j) STAKEHOLDER SEMIANNUAL REPORT.—

5 (1) IN GENERAL.—Except as provided in paragraph (2), the Sec-
 6 retary shall provide a semiannual report to the appropriate congres-
 7 sional committees that includes—

8 (A) the number of public and private stakeholders who were
 9 provided with each report on the Plan;

10 (B) a description of the measures the Secretary has taken,
 11 under subsection (g) or otherwise, to ensure proper treatment and
 12 security for classified information to be shared with the public and
 13 private stakeholders under the Plan; and

14 (C) an explanation of the reason for the denial of transportation
 15 security information to a stakeholder who had previously received
 16 the information.

17 (2) WHEN REPORT NOT REQUIRED.—The Secretary is not required
 18 to provide a semiannual report under paragraph (1) if no stakeholders
 19 have been added to or removed from the group of persons with whom
 20 transportation security information is shared under the plan since the
 21 end of the period covered by the last preceding semiannual report.

22 **§ 11316. Enforcement of certain regulations and orders of**
 23 **the Secretary**

24 (a) DEFINITIONS.—In this section:

25 (1) PERSON.—The term “person” does not include—

26 (A) the United States Postal Service; or

27 (B) the Department of Defense.

28 (2) SMALL BUSINESS CONCERN.—The term “small business concern”
 29 has the meaning given the term in section 3 of the Small Business Act
 30 (15 U.S.C. 632).

31 (b) APPLICABILITY OF SECTION.—

32 (1) IN GENERAL.—This section applies to the enforcement of regula-
 33 tions prescribed, and orders issued, by the Secretary under a provision
 34 of chapter 701 of title 46 or under a provision of title 49 other than
 35 a provision of former chapter 449 (in this section referred to as an
 36 “applicable provision of title 49”).

37 (2) VIOLATIONS OF FORMER CHAPTER 449 OF TITLE 49.—The pen-
 38 alties under chapter 125 of title 18 and chapter 182 of title 28 apply
 39 to violations of regulations prescribed and orders issued by the Sec-
 40 retary under former chapter 449 of title 49.

41 (3) NON-APPLICABILITY TO CERTAIN VIOLATIONS.—

1 (A) IN GENERAL.—Subsections (c) through (f) do not apply to
2 violations of regulations prescribed, and orders issued, by the Sec-
3 retary under a provision of title 49—

4 (i) involving the transportation of personnel or shipments
5 of materials by contractors where the Department of Defense
6 has assumed control and responsibility;

7 (ii) by a member of the armed forces of the United States
8 when performing official duties; or

9 (iii) by a civilian employee of the Department of Defense
10 when performing official duties.

11 (B) ALTERNATIVE PENALTIES.—Violations described in clause
12 (i), (ii), or (iii) of subparagraph (A) shall be subject to penalties
13 as determined by the Secretary of Defense or the designee of the
14 Secretary of Defense.

15 (c) CIVIL PENALTY.—

16 (1) IN GENERAL.—A person is liable to the United States Govern-
17 ment for a civil penalty of not more than \$10,000 for a violation of
18 a regulation prescribed, or order issued, by the Secretary under an ap-
19 plicable provision of title 49.

20 (2) REPEAT VIOLATIONS.—A separate violation occurs under this
21 subsection for each day the violation continues.

22 (d) ADMINISTRATIVE IMPOSITION OF CIVIL PENALTIES.—

23 (1) IN GENERAL.—The Secretary may impose a civil penalty for a
24 violation of a regulation prescribed, or order issued, under an applica-
25 ble provision of title 49. The Secretary shall give written notice of the
26 finding of a violation and the penalty.

27 (2) SCOPE OF CIVIL ACTION.—In a civil action to collect a civil pen-
28 alty imposed by the Secretary under this section, a court may not re-
29 examine issues of liability or the amount of the penalty.

30 (3) JURISDICTION.—The district courts of the United States shall
31 have exclusive jurisdiction of civil actions to collect a civil penalty im-
32 posed by the Secretary under this section if—

33 (A) the amount in controversy is more than—

34 (i) \$400,000, if the violation was committed by a person
35 other than an individual or small business concern; or

36 (ii) \$50,000 if the violation was committed by an individual
37 or small business concern;

38 (B) the action is in rem or another action in rem based on the
39 same violation has been brought; or

40 (C) another action has been brought for an injunction based on
41 the same violation.

1 (4) MAXIMUM PENALTY.—The maximum civil penalty the Secretary
2 administratively may impose under this subsection is—

3 (A) \$400,000, if the violation was committed by a person other
4 than an individual or small business concern; or

5 (B) \$50,000, if the violation was committed by an individual or
6 small business concern.

7 (5) NOTICE AND OPPORTUNITY TO REQUEST HEARING.—Before im-
8 posing a penalty under this chapter, the Secretary shall provide to the
9 person against whom the penalty is to be imposed—

10 (A) written notice of the proposed penalty; and

11 (B) the opportunity to request a hearing on the proposed pen-
12 alty, if the Secretary receives the request not later than 30 days
13 after the date on which the person receives notice.

14 (e) COMPROMISE AND SETOFF.—

15 (1) COMPROMISE.—The Secretary may compromise the amount of a
16 civil penalty imposed under this section.

17 (2) SETOFF.—The United States Government may deduct the
18 amount of a civil penalty imposed or compromised under this section
19 from amounts it owes the person liable for the penalty.

20 (f) INVESTIGATIONS AND PROCEEDINGS.—Subchapter IV of chapter 409
21 of this title applies to investigations and proceedings brought under this sec-
22 tion to the same extent that chapter 461 of title 49 applies to investigations
23 and proceedings brought with respect to aviation security duties designated
24 to be carried out by the Secretary.

25 (g) ENFORCEMENT TRANSPARENCY.—

26 (1) IN GENERAL.—The Secretary shall, not later than December 31
27 each year—

28 (A) provide an annual summary to the public of all enforcement
29 actions taken by the Secretary under this section; and

30 (B) include in each summary the docket number of each en-
31 forcement action, the type of alleged violation, the penalty or pen-
32 alties proposed, and the final assessment amount of each penalty.

33 (2) ELECTRONIC AVAILABILITY.—Each summary under this sub-
34 section shall be made available to the public by electronic means.

35 (3) RELATIONSHIP TO FREEDOM OF INFORMATION ACT AND PRIVACY
36 ACT.—Nothing in this subsection shall be construed to require disclo-
37 sure of information or records that are exempt from disclosure under
38 section 552 or 552a of title 5.

39 **§ 11317. Registered traveler fee**

40 Notwithstanding section 553 of title 5, the Secretary shall impose a fee
41 for a registered traveler program undertaken by the Department by notice

1 in the Federal Register, and may modify the fee from time to time by notice
2 in the Federal Register. Fees shall not exceed the aggregate costs associated
3 with the program, shall be credited to the Transportation Security Adminis-
4 tration registered traveler fee account, and are available until expended.

5 **§ 11318. Enhanced security measures**

6 (a) IN GENERAL.—The Administrator may take the following actions:

7 (1) Require effective 911 emergency call capability for telephones
8 serving passenger aircraft and passenger trains.

9 (2) Establish a uniform system of identification for all State and
10 local law enforcement personnel for use in obtaining permission to
11 carry weapons in aircraft cabins and in obtaining access to a secured
12 area of an airport, if otherwise authorized to carry the weapons.

13 (3) Establish requirements to implement trusted passenger programs
14 and use available technologies to expedite the security screening of pas-
15 sengers who participate in the programs, thereby allowing security
16 screening personnel to focus on those passengers who should be subject
17 to more extensive screening.

18 (4) In consultation with the Commissioner of the Food and Drug
19 Administration, develop alternative security procedures under which a
20 medical product to be transported on a flight of an air carrier would
21 not be subject to an inspection that would irreversibly damage the
22 product.

23 (5) Provide for the use of technologies, including wireless and wire
24 line data technologies, to enable the private and secure communication
25 of threats to aid in the screening of passengers and other individuals
26 on airport property who are identified on any State or Federal security-
27 related data base for the purpose of having an integrated response co-
28 ordination of various authorized airport security forces.

29 (6) In consultation with the Administrator of the Federal Aviation
30 Administration, consider whether to require all pilot licenses to incor-
31 porate a photograph of the license holder and appropriate biometric im-
32 prints.

33 (7) Provide for the use of voice stress analysis, biometric, or other
34 technologies to prevent a person who might pose a danger to air safety
35 or security from boarding the aircraft of an air carrier or foreign air
36 carrier in air transportation or intrastate air transportation.

37 (8) Provide for the use of technology that will permit enhanced in-
38 stant communications and information between airborne passenger air-
39 craft and appropriate individuals or facilities on the ground.

40 (9) Require that air carriers provide flight attendants with a dis-
41 creet, hands-free, wireless method of communicating with the pilots.

1 (b) ANNUAL REPORT.—Until the Administrator has implemented or de-
 2 cided not to take each of the actions specified in subsection (a), the Admin-
 3 istrator shall transmit to Congress by May 19 each year a report on the
 4 progress of the Administrator in evaluating and taking the actions, includ-
 5 ing legislative recommendations that the Secretary may have for enhancing
 6 transportation security.

7 **§ 11319. Performance management system**

8 (a) ESTABLISHING A FAIR AND EQUITABLE SYSTEM FOR MEASURING
 9 STAFF PERFORMANCE.—The Administrator shall establish a performance
 10 management system that strengthens the organization’s effectiveness by
 11 providing for the establishment of goals and objectives for managers, em-
 12 ployees, and organizational performance consistent with the performance
 13 plan.

14 (b) ESTABLISHING MANAGEMENT ACCOUNTABILITY FOR MEETING PER-
 15 FORMANCE GOALS.—

16 (1) ADMINISTRATOR.—Each year, the Secretary and the Adminis-
 17 trator shall enter into an annual performance agreement that shall set
 18 forth organizational and individual performance goals for the Adminis-
 19 trator.

20 (2) SENIOR MANAGERS.—Each year, the Administrator and each
 21 senior manager who reports to the Administrator shall enter into an
 22 annual performance agreement that sets forth organization and indi-
 23 vidual goals for those managers. All other employees hired under the
 24 authority of the Transportation Security Administration shall enter
 25 into an annual performance agreement that sets forth organization and
 26 individual goals for those employees.

27 (c) PERFORMANCE-BASED SERVICE CONTRACTING.—To the extent con-
 28 tracts are used to implement the Aviation and Transportation Security Act
 29 (Public Law 107–71, 115 Stat. 597), the Administrator shall, to the extent
 30 practical, maximize the use of performance-based service contracts. These
 31 contracts should be consistent with guidelines published by the Office of
 32 Federal Procurement Policy.

33 **§ 11320. Voluntary provision of emergency services**

34 (a) PROGRAM FOR PROVISION OF VOLUNTARY SERVICES.—

35 (1) PROGRAM.—The Administrator shall carry out a program to per-
 36 mit qualified law enforcement officers, firefighters, and emergency med-
 37 ical technicians to provide emergency services on commercial air flights
 38 during emergencies.

39 (2) REQUIREMENTS.—The Administrator shall establish require-
 40 ments for qualifications of providers of voluntary services under the

1 program under paragraph (1), including training requirements, that
2 the Administrator considers appropriate.

3 (3) CONFIDENTIALITY OF REGISTRY.—If as part of the program
4 under paragraph (1), the Administrator requires or permits registra-
5 tion of law enforcement officers, firefighters, or emergency medical
6 technicians who are willing to provide emergency services on commer-
7 cial flights during emergencies, the Administrator shall take appro-
8 priate actions to ensure that the registry is available only to appro-
9 priate airline personnel and otherwise remains confidential.

10 (4) CONSULTATION.—The Administrator shall consult with appro-
11 priate representatives of the commercial airline industry, and organiza-
12 tions representing community-based law enforcement, firefighters, and
13 emergency medical technicians, in carrying out the program under
14 paragraph (1), including the actions taken under paragraph (3).

15 (b) EXEMPTION FROM LIABILITY.—An individual is not liable for dam-
16 ages in an action brought in a Federal or State court that arises from an
17 act or omission of the individual in providing or attempting to provide as-
18 sistance in the case of an in-flight emergency in an aircraft of an air carrier
19 if the individual meets qualifications as the Administrator prescribes for
20 purposes of this section.

21 (c) EXCEPTION.—The exemption under subsection (b) shall not apply in
22 a case in which an individual provides, or attempts to provide, assistance
23 described in subsection (b) in a manner that constitutes gross negligence
24 or willful misconduct.

25 **§ 11321. Disposition of unclaimed money and clothing**

26 (a) IN GENERAL.—

27 (1) DISPOSITION OF UNCLAIMED MONEY.—Notwithstanding section
28 3302 of title 31, unclaimed money recovered at an airport security
29 checkpoint—

30 (A) shall be retained by the Transportation Security Adminis-
31 tration; and

32 (B) shall remain available until expended for the purpose of pro-
33 viding civil aviation security as required in this chapter.

34 (2) DISPOSITION OF UNCLAIMED CLOTHING.—

35 (A) IN GENERAL.—In disposing of unclaimed clothing recovered
36 at any airport security checkpoint, the Administrator shall make
37 every reasonable effort, in consultation with the Secretary of Vet-
38 erans Affairs, to transfer the clothing to the local airport authority
39 or other local authorities for donation to charity, including local
40 veterans organizations or other local charitable organizations for
41 distribution to homeless or needy veterans and veteran families.

1 (B) AGREEMENTS.—In implementing paragraph (1), the Ad-
2 ministrators may enter into agreements with airport authorities.

3 (C) OTHER CHARITABLE ARRANGEMENTS.—Nothing in this
4 subsection prevents an airport or the Transportation Security Ad-
5 ministration from donating unclaimed clothing to a charitable or-
6 ganization of their choosing.

7 (D) LIMITATION.—Nothing in this subsection creates a cost to
8 the Government.

9 (b) ANNUAL REPORT.—The Administrator shall transmit annually to the
10 Committee on Transportation and Infrastructure of the House of Rep-
11 resentatives; the Committee on Appropriations of the House of Representa-
12 tives; the Committee on Commerce, Science and Transportation of the Sen-
13 ate; and the Committee on Appropriations of the Senate, a report that con-
14 tains a detailed description of the amount of unclaimed money recovered in
15 total and at each individual airport, and specifies how the unclaimed money
16 is being used to provide civil aviation security.

17 **Subchapter II—Acquisition Improvements**

18 **§ 11331. Definitions**

19 In this subchapter:

20 (1) PLAN.—The term “Plan” means the strategic 5-year technology
21 investment plan the Administrator develops under section 11332 of this
22 title.

23 (2) SECURITY-RELATED TECHNOLOGY.—The term “security-related
24 technology” means any technology that assists the Transportation Se-
25 curity Administration in the prevention of, or defense against, threats
26 to United States transportation systems, including threats to people,
27 property, and information.

28 **§ 11332. Technology investment plan**

29 (a) IN GENERAL.—The Administrator—

30 (1) shall develop and submit to Congress a strategic 5-year tech-
31 nology investment plan that may include a classified addendum to re-
32 port sensitive transportation security risks, technology vulnerabilities,
33 or other sensitive security information; and

34 (2) to the extent possible, shall publish the Plan in an unclassified
35 format in the public domain after it is approved by the Secretary.

36 (b) CONSULTATION.—The Administrator shall develop the Plan in con-
37 sultation with—

- 38 (1) the Under Secretary for Management;
39 (2) the Under Secretary for Science and Technology;
40 (3) the Chief Information Officer; and

1 (4) the aviation stakeholder advisory committee established by the
2 Administrator.

3 (c) CONTENTS.—The Plan shall include—

4 (1) an analysis of transportation security risks and the associated ca-
5 pability gaps that would be best addressed by security-related tech-
6 nology, including consideration of the most recent quadrennial home-
7 land security review under section 11506 of this title;

8 (2) a set of security-related technology acquisition needs that—

9 (A) is prioritized based on risk and associated capability gaps
10 identified under paragraph (1); and

11 (B) includes planned technology programs and projects with de-
12 fined objectives, goals, timelines, and measures;

13 (3) an analysis of current and forecast trends in domestic and inter-
14 national passenger travel;

15 (4) an identification of currently deployed security-related tech-
16 nologies that are at or near the end of their lifecycles;

17 (5) an identification of test, evaluation, modeling, and simulation ca-
18 pabilities, including target methodologies, rationales, and timelines nec-
19 essary to support the acquisition of the security-related technologies ex-
20 pected to meet the needs under paragraph (2);

21 (6) an identification of opportunities for public-private partnerships,
22 small and disadvantaged company participation, intragovernment col-
23 laboration, university centers of excellence, and national laboratory
24 technology transfer;

25 (7) an identification of the Transportation Security Administration’s
26 acquisition workforce needs for the management of planned security-
27 related technology acquisitions, including consideration of leveraging
28 acquisition expertise of other Federal agencies;

29 (8) an identification of the security resources, including information
30 security resources, that will be required to protect security-related tech-
31 nology from physical or cyber theft, diversion, sabotage, or attack;

32 (9) an identification of initiatives to streamline the Transportation
33 Security Administration’s acquisition process and provide greater pre-
34 dictability and clarity to small, medium, and large businesses, including
35 the timelines for testing and evaluation;

36 (10) an assessment of the impact to commercial aviation passengers;

37 (11) a strategy for consulting airport management, air carrier rep-
38 resentatives, and Federal security directors when an acquisition will
39 lead to the removal of equipment at airports, and how the strategy for
40 consulting with those officials of the relevant airports will address po-

1 tential negative impacts on commercial passengers or airport oper-
2 ations; and

3 (12) in consultation with the National Institute of Standards and
4 Technology, an identification of security-related technology interface
5 standards, in existence or if implemented, that could promote more
6 interoperable passenger, baggage, and cargo screening systems.

7 (d) LEVERAGING THE PRIVATE SECTOR.—To the extent practicable, and
8 in a manner that is consistent with fair and equitable practices, the Plan
9 shall—

10 (1) leverage emerging technology trends and research and develop-
11 ment investment trends in the public and private sectors;

12 (2) incorporate private-sector input, including from the aviation in-
13 dustry stakeholder advisory committee established by the Adminis-
14 trator, through requests for information, industry days, and other inno-
15 vative means consistent with the Federal Acquisition Regulation; and

16 (3) in consultation with the Under Secretary for Science and Tech-
17 nology, identify technologies in existence or in development that, with
18 or without adaptation, are expected to be suitable to meeting mission
19 needs.

20 (e) DISCLOSURE.—The Administrator shall include with the Plan a list
21 of nongovernment persons that contributed to the writing of the Plan.

22 (f) UPDATE AND REPORT.—Beginning 2 years after the date the Plan
23 is submitted to Congress under subsection (a), and biennially afterwards,
24 the Administrator shall submit to Congress—

25 (1) an update of the Plan; and

26 (2) a report on the extent to which each security-related technology
27 the Transportation Security Administration has acquired since the last
28 issuance or update of the Plan is consistent with the planned tech-
29 nology programs and projects identified under subsection (c)(2) for
30 that security-related technology.

31 **§ 11333. Acquisition justification and reports and certifi-**
32 **cation**

33 (a) ACQUISITION JUSTIFICATION.—Before the Transportation Security
34 Administration implements any security-related technology acquisition, the
35 Administrator, in accordance with the Department’s policies and directives,
36 shall determine whether the acquisition is justified by conducting an anal-
37 ysis that includes—

38 (1) an identification of the scenarios and level of risk to transpor-
39 tation security from those scenarios that would be addressed by the se-
40 curity-related technology acquisition;

41 (2) an assessment of how the proposed acquisition aligns to the Plan;

1 (3) a comparison of the total expected lifecycle cost against the total
2 expected quantitative and qualitative benefits to transportation secu-
3 rity;

4 (4) an analysis of alternative security solutions, including policy or
5 procedure solutions, to determine if the proposed security-related tech-
6 nology acquisition is the most effective and cost-efficient solution based
7 on cost-benefit considerations;

8 (5) an assessment of the potential privacy and civil liberties implica-
9 tions of the proposed acquisition that includes, to the extent prac-
10 ticable, consultation with organizations that advocate for the protection
11 of privacy and civil liberties;

12 (6) a determination that the proposed acquisition is consistent with
13 fair information practice principles issued by the Privacy Officer of the
14 Department;

15 (7) confirmation that there are no significant risks to human health
16 or safety posed by the proposed acquisition; and

17 (8) an estimate of the benefits to commercial aviation passengers.

18 (b) REPORTS AND CERTIFICATION.—

19 (1) IN GENERAL.—Not later than the end of the 30-day period pre-
20 ceeding the award by the Transportation Security Administration of a
21 contract for any security-related technology acquisition exceeding
22 \$30,000,000, the Administrator shall submit to the Committee on
23 Commerce, Science, and Transportation of the Senate and the Com-
24 mittee on Homeland Security of the House of Representatives—

25 (A) the results of the comprehensive acquisition justification
26 under subsection (a); and

27 (B) a certification by the Administrator that the benefits to
28 transportation security justify the contract cost.

29 (2) REDUCTION DUE TO IMMINENT TERRORIST THREAT.—If there is
30 a known or suspected imminent threat to transportation security, the
31 Administrator—

32 (A) may reduce the 30-day period under paragraph (1) to 5
33 days to rapidly respond to the threat; and

34 (B) shall immediately notify the Committee on Commerce,
35 Science, and Transportation of the Senate and the Committee on
36 Homeland Security of the House of Representatives of the known
37 or suspected imminent threat.

38 **§ 11334. Baseline establishment and reports**

39 (a) BASELINE REQUIREMENTS.—

40 (1) IN GENERAL.—Before the Transportation Security Administra-
41 tion implements any security-related technology acquisition, the appro-

1 appropriate acquisition official of the Department shall establish and docu-
2 ment a set of formal baseline requirements. The requirements shall—

3 (A) include the estimated costs (including lifecycle costs), sched-
4 ule, and performance milestones for the planned duration of the
5 acquisition;

6 (B) identify the acquisition risks and a plan for mitigating those
7 risks; and

8 (C) assess the personnel necessary to manage the acquisition
9 process, manage the ongoing program, and support training and
10 other operations as necessary.

11 (2) FEASIBILITY.—In establishing the performance milestones under
12 paragraph (1)(A), the appropriate acquisition official of the Depart-
13 ment, to the extent possible and in consultation with the Under Sec-
14 retary for Science and Technology, shall ensure that achieving those
15 milestones is technologically feasible.

16 (3) TEST AND EVALUATION PLAN.—The Administrator, in consulta-
17 tion with the Under Secretary for Science and Technology, shall de-
18 velop a test and evaluation plan that describes—

19 (A) the activities that are expected to be required to assess ac-
20 quired technologies against the performance milestones established
21 under paragraph (1)(A);

22 (B) the necessary and cost-effective combination of laboratory
23 testing, field testing, modeling, simulation, and supporting analysis
24 to ensure that the technologies meet the Transportation Security
25 Administration’s mission needs;

26 (C) an efficient planning schedule to ensure that test and eval-
27 uation activities are completed without undue delay; and

28 (D) if commercial aviation passengers are expected to interact
29 with the security-related technology, methods that could be used
30 to ensure passenger acceptance of and familiarization with the se-
31 curity-related technology.

32 (4) VERIFICATION AND VALIDATION.—The appropriate acquisition
33 official of the Department—

34 (A) subject to subparagraph (B), shall utilize independent re-
35 views to verify and validate the performance milestones and cost
36 estimates developed under paragraph (1) for a security-related
37 technology that pursuant to section 11332(c)(2) of this title has
38 been identified as a high priority need in the most recent Plan;
39 and

40 (B) shall ensure that the use of independent reviewers does not
41 unduly delay the schedule of any acquisition.

1 (5) STREAMLINING ACCESS FOR INTERESTED VENDORS.—The Ad-
 2 ministrator shall establish a streamlined process for an interested ven-
 3 dor of a security-related technology to request and receive appropriate
 4 access to the baseline requirements and test and evaluation plans that
 5 are necessary for the vendor to participate in the acquisition process
 6 for that technology.

7 (b) REVIEW OF BASELINE REQUIREMENTS AND DEVIATION; REPORT.—

8 (1) REVIEW.—

9 (A) IN GENERAL.—The appropriate acquisition official of the
 10 Department shall review and assess each implemented acquisition
 11 to determine if the acquisition is meeting the baseline require-
 12 ments established under subsection (a).

13 (B) ASSESSMENT.—The review shall include an assessment of
 14 whether—

15 (i) the planned testing and evaluation activities have been
 16 completed; and

17 (ii) the results of that testing and evaluation demonstrate
 18 that the performance milestones are technologically feasible.

19 (2) REPORT.—Not later than 30 days after making a finding de-
 20 scribed in clause (i) or (ii) of subparagraph (A), the Administrator
 21 shall submit a report to the Committee on Commerce, Science, and
 22 Transportation of the Senate and the Committee on Homeland Secu-
 23 rity of the House of Representatives that includes—

24 (A) the results of any assessment that finds that—

25 (i) the actual or planned costs exceed the baseline costs by
 26 more than 10 percent;

27 (ii) the actual or planned schedule for delivery has been de-
 28 layed by more than 180 days; or

29 (iii) there is a failure to meet any performance milestone
 30 that directly impacts security effectiveness;

31 (B) the cause for the excessive costs, delay, or failure; and

32 (C) a plan for corrective action.

33 **§ 11335. Inventory utilization**

34 (a) USE OF EXISTING INVENTORY.—Before the procurement of addi-
 35 tional quantities of equipment to fulfill a mission need, the Administrator,
 36 to the extent practicable, shall utilize any existing units in the Transpor-
 37 tation Security Administration's inventory to meet that need.

38 (b) TRACKING OF INVENTORY.—

39 (1) IN GENERAL.—The Administrator shall establish a process for
 40 tracking—

1 (A) the location of security-related technology in the inventory
2 under subsection (a);

3 (B) the utilization status of security-related technology in the
4 inventory under subsection (a); and

5 (C) the quality of security-related equipment in the inventory
6 under subsection (a).

7 (2) INTERNAL CONTROLS.—The Administrator shall implement in-
8 ternal controls to ensure up-to-date accurate data on security-related
9 technology owned, deployed, and in use.

10 (e) LOGISTICS MANAGEMENT.—

11 (1) IN GENERAL.—The Administrator shall establish logistics prin-
12 ciples for managing inventory in an effective and efficient manner.

13 (2) LIMITATION ON JUST-IN-TIME LOGISTICS.—The Administrator
14 may not use just-in-time logistics if doing so—

15 (A) would inhibit necessary planning for large-scale delivery of
16 equipment to airports or other facilities; or

17 (B) would unduly diminish surge capacity for response to a ter-
18 rorist threat.

19 **§ 11336. Small business contracting goals**

20 Not later than March 18 of each year, the Administrator shall submit to
21 the Committee on Commerce, Science, and Transportation of the Senate
22 and the Committee on Homeland Security of the House of Representative
23 a report that includes—

24 (1) the Transportation Security Administration’s performance record
25 with respect to meeting its published small-business contracting goals
26 during the preceding fiscal year;

27 (2) if the goals described in paragraph (1) were not met or the
28 Transportation Security Administration’s performance was below the
29 published small-business contracting goals of the Department—

30 (A) a list of challenges, including deviations from the Transpor-
31 tation Security Administration’s subcontracting plans, and factors
32 that contributed to the level of performance during the preceding
33 fiscal year;

34 (B) an action plan, with benchmarks, for addressing each of the
35 challenges identified in subparagraph (A) that—

36 (i) is prepared after consultation with the Secretary of De-
37 fense and the heads of Federal departments and agencies
38 that achieved their published goals for prime contracting with
39 small and minority-owned businesses, including small and dis-
40 advantaged businesses, in prior fiscal years; and

(ii) identifies policies and procedures that could be incorporated by the Transportation Security Administration in furtherance of achieving the Administration’s published goal for the contracting; and

(3) a status report on the implementation of the action plan that was developed in the preceding fiscal year in accordance with paragraph (2)(B), if the plan was required.

§ 11337. Consistency with Federal Acquisition Regulation and Department policies and directives

The Administration shall execute the responsibilities set forth in this subchapter in a manner consistent with, and not duplicative of, the Federal Acquisition Regulation and the Department’s polices and directives.

Chapter 115—Management

Sec.

- 11501. Under Secretary for Management.
- 11502. Chief Financial Officer.
- 11503. Chief Information Officer.
- 11504. Chief Human Capital Officer.
- 11505. Officer for Civil Rights and Civil Liberties.
- 11506. Quadrennial homeland security review.
- 11507. Interoperable communications.
- 11508. Joint Task Forces.
- 11509. Office of Strategy, Policy, and Plans.

§ 11501. Under Secretary for Management

(a) DEFINITION OF INTEROPERABLE COMMUNICATIONS.—In this section, the term “interoperable communications” means the ability of emergency response providers and relevant Federal, State, and local government agencies to communicate with each other as necessary, through a dedicated public safety network utilizing information technology systems and radio communications systems, and to exchange voice, data, and video with one another on demand, in real time, as necessary.

(b) IN GENERAL.—The Under Secretary for Management serves as the Chief Management Officer and principal advisor to the Secretary on matters relating to the management of the Department, including management integration and transformation in support of homeland security operations and programs. The Secretary, acting through the Under Secretary for Management, is responsible for the management and administration of the Department, including the following:

- (1) The budget, appropriations, expenditures of funds, accounting, and finance.
- (2) Procurement.
- (3) Human resources and personnel.
- (4) Information technology and communications systems, including policies and directives to achieve and maintain interoperable communications among the components of the Department.

- 1 (5) Facilities, property, equipment, and other material resources.
- 2 (6) Security for personnel, information technology and communica-
- 3 tions systems, facilities, property, equipment, and other material re-
- 4 sources.
- 5 (7) Strategic management planning and annual performance plan-
- 6 ning and identification and tracking of performance measures relating
- 7 to the responsibilities of the Department.
- 8 (8) Grants and other assistance for management programs.
- 9 (9) The management integration and transformation in each func-
- 10 tional management discipline of the Department, including information
- 11 technology, financial management, acquisition management, and human
- 12 capital management, to ensure an efficient and orderly consolidation of
- 13 functions and personnel in the Department, including—
- 14 (A) the development of centralized data sources and connectivity
- 15 of information systems to the greatest extent practicable to en-
- 16 hance program visibility, transparency, and operational effective-
- 17 ness and coordination;
- 18 (B) the development of standardized and automated manage-
- 19 ment information to manage and oversee programs and make in-
- 20 formed decisions to improve the efficiency of the Department;
- 21 (C) the development of effective program management and reg-
- 22 ular oversight mechanisms, including clear roles and processes for
- 23 program governance, sharing of best practices, and access to time-
- 24 ly, reliable, and evaluated data on all acquisitions and investments;
- 25 and
- 26 (D) the overall supervision, including the conduct of internal au-
- 27 dits and management analyses, of the programs and activities of
- 28 the Department, including establishment of oversight procedures
- 29 to ensure a full and effective review of the efforts by components
- 30 of the Department to implement policies and procedures of the
- 31 Department for management integration and transformation.
- 32 (10) The development of a transition and succession plan, before De-
- 33 cember 1 of each year in which a Presidential election is held, to guide
- 34 the transition of Department functions to a new Presidential adminis-
- 35 tration, and making the plan available to the next Secretary and Under
- 36 Secretary for Management and to the congressional homeland security
- 37 committees.
- 38 (11) Reporting to the Government Accountability Office every 6
- 39 months to demonstrate measurable, sustainable progress made in im-
- 40 plementing the corrective action plans of the Department to address
- 41 the designation of the management functions of the Department on the

1 bi-annual high risk list of the Government Accountability Office, until
2 the Comptroller General of the United States submits to the appro-
3 priate congressional committees written notification of removal of the
4 high-risk designation.

5 (12) The conduct of internal audits and management analyses of the
6 programs and activities of the Department.

7 (13) Any other management duties that the Secretary may des-
8 ignate.

9 (c) WAIVERS FOR CONDUCTING BUSINESS WITH SUSPENDED OR
10 DEBARRED CONTRACTORS.—Not later than 5 days after the date on which
11 the Chief Procurement Officer or Chief Financial Officer of the Department
12 issues a waiver of the requirement that an agency not engage in business
13 with a contractor or other recipient of funds listed as a party suspended
14 or debarred from receiving contracts, grants, or other types of Federal as-
15 sistance in the System for Award Management maintained by the General
16 Services Administration, or any successor, the Under Secretary for Manage-
17 ment shall submit to the congressional homeland security committees and
18 the Inspector General of the Department notice of the waiver and an expla-
19 nation of the finding by the Under Secretary that a compelling reason exists
20 for the waiver.

21 (d) APPOINTMENT AND EVALUATION.—The Under Secretary for Manage-
22 ment—

23 (1) is appointed by the President, by and with the advice and con-
24 sent of the Senate, from among individuals who have—

25 (A) extensive executive level leadership and management experi-
26 ence in the public or private sector;

27 (B) strong leadership skills;

28 (C) a demonstrated ability to manage large and complex organi-
29 zations; and

30 (D) a proven record in achieving positive operational results;

31 (2) shall enter into an annual performance agreement with the Sec-
32 retary that shall set forth measurable individual and organizational
33 goals; and

34 (3) is subject to an annual performance evaluation by the Secretary,
35 who shall determine as part of each evaluation whether the Under Sec-
36 retary for Management has made satisfactory progress toward achiev-
37 ing the goals set out in the performance agreement required under
38 paragraph (2).

39 (e) SYSTEM FOR AWARD MANAGEMENT CONSULTATION.—The Under
40 Secretary for Management shall require that all Department contracting
41 and grant officials consult the System for Award Management (or successor

1 system) as maintained by the General Services Administration prior to
2 awarding a contract or grant or entering into other transactions to ascertain
3 whether the selected contractor is excluded from receiving Federal contracts,
4 certain subcontracts, and certain types of Federal financial and non-finan-
5 cial assistance and benefits.

6 **§ 11502. Chief Financial Officer**

7 (a) IN GENERAL.—The Chief Financial Officer shall—

8 (1) perform functions as specified in chapter 9 of title 31; and

9 (2) report to the Under Secretary for Management with respect to
10 those functions described in paragraph (1) and other responsibilities
11 that may be assigned.

12 (b) PROGRAM ANALYSIS AND EVALUATION FUNCTION.—

13 (1) ESTABLISHMENT OF OFFICE OF PROGRAM ANALYSIS AND EVAL-
14 UATION.—The Secretary shall establish an Office of Program Analysis
15 and Evaluation (in this section referred to as the “Office”) in the De-
16 partment.

17 (2) RESPONSIBILITIES.—The Office shall—

18 (A) analyze and evaluate plans, programs, and budgets of the
19 Department in relation to United States homeland security objec-
20 tives, projected threats, vulnerability assessments, estimated costs,
21 resource constraints, and the most recent homeland security strat-
22 egy developed under section 10386(b)(2) of this title;

23 (B) develop and perform analyses and evaluations of alternative
24 plans, programs, personnel levels, and budget submissions for the
25 Department in relation to United States homeland security objec-
26 tives, projected threats, vulnerability assessments, estimated costs,
27 resource constraints, and the most recent homeland security strat-
28 egy developed under section 10386(b)(2) of this title;

29 (C) establish policies for, and oversee the integration of, the
30 planning, programming, and budgeting system of the Department;

31 (D) review and ensure that the Department meets performance-
32 based budget requirements established by the Office of Manage-
33 ment and Budget;

34 (E) provide guidance for, and oversee the development of, the
35 Future Years Homeland Security Program of the Department, as
36 specified under section 10386 of this title;

37 (F) ensure that the costs of Department programs, including
38 classified programs, are presented accurately and completely;

39 (G) oversee the preparation of the annual performance plan for
40 the Department and the program and performance section of the

1 annual report on program performance for the Department, con-
2 sistent with sections 1115 and 1116, respectively, of title 31;

3 (H) provide leadership in developing and promoting improved
4 analytical tools and methods for analyzing homeland security plan-
5 ning and the allocation of resources; and

6 (I) perform other responsibilities delegated by the Secretary
7 consistent with an effective program analysis and evaluation func-
8 tion.

9 (3) DIRECTOR OF PROGRAM ANALYSIS AND EVALUATION.—There is
10 a Director of Program Analysis and Evaluation. The Director—

11 (A) is a principal staff assistant to the Chief Financial Officer
12 of the Department for program analysis and evaluation; and

13 (B) shall report to an official no lower than the Chief Financial
14 Officer.

15 (4) REORGANIZATION.—

16 (A) IN GENERAL.—The Secretary may allocate or reallocate the
17 functions of the Office, or discontinue the Office, under section
18 10331(b)(1) of this title.

19 (B) EXEMPTION FROM LIMITATIONS.—Section 10331(b)(2) of
20 this title does not apply to an action by the Secretary under this
21 paragraph.

22 (e) NOTIFICATION REGARDING TRANSFER OR REPROGRAMMING OF
23 FUNDS.—In a case in which appropriations available to the Department or
24 an officer of the Department are transferred or reprogrammed and notice
25 of the transfer or reprogramming is submitted to Congress (including an
26 officer, office, or committee of Congress), the Chief Financial Officer shall
27 simultaneously submit the notice to the Committee on Homeland Security
28 and the Committee on Oversight and Government Reform of the House of
29 Representatives, and to the Committee on Homeland Security and Govern-
30 mental Affairs of the Senate.

31 § 11503. Chief Information Officer

32 (a) IN GENERAL.—The Chief Information Officer shall report to the Sec-
33 retary, or to another official of the Department, as the Secretary may di-
34 rect.

35 (b) GEOSPATIAL INFORMATION FUNCTIONS.—

36 (1) DEFINITIONS.—In this subsection:

37 (A) GEOSPATIAL INFORMATION.—The term “geospatial infor-
38 mation” means graphical or digital data depicting natural or man-
39 made physical features, phenomena, or boundaries of the earth
40 and information related thereto, including surveys, maps, charts,
41 remote sensing data, and images.

1 (B) GEOSPATIAL TECHNOLOGY.—The term “geospatial tech-
2 nology” means technology utilized by analysts, specialists, sur-
3 veyors, photogrammetrists, hydrographers, geodesists, cartog-
4 raphers, architects, or engineers for the collection, storage, re-
5 trieval, or dissemination of geospatial information, including

- 6 (i) global satellite surveillance systems;
7 (ii) global position systems;
8 (iii) geographic information systems;
9 (iv) mapping equipment;
10 (v) geocoding technology; and
11 (vi) remote sensing devices.

12 (2) OFFICE OF GEOSPATIAL MANAGEMENT.—

13 (A) ESTABLISHMENT.—There is in the Office of the Chief In-
14 formation Officer the Office of Geospatial Management.

15 (B) GEOSPATIAL INFORMATION OFFICER.—

16 (i) IN GENERAL.—The Geospatial Information Officer ad-
17 ministers the Office of Geospatial Management. The
18 Geospatial Information Officer is appointed by the Secretary.
19 The Geospatial Information Officer serves under the direction
20 of the Chief Information Officer.

21 (ii) ASSISTS CHIEF INFORMATION OFFICER.—The
22 Geospatial Information Officer assists the Chief Information
23 Officer in carrying out all functions under this section and in
24 coordinating the geospatial information needs of the Depart-
25 ment.

26 (C) COORDINATION OF GEOSPATIAL INFORMATION.—The Chief
27 Information Officer shall establish and carry out a program to
28 provide for the efficient use of geospatial information, which shall
29 include—

- 30 (i) providing necessary geospatial information to implement
31 the critical infrastructure protection programs;
32 (ii) providing leadership and coordination in meeting the
33 geospatial information requirements of those responsible for
34 planning, prevention, mitigation, assessment, and response to
35 emergencies, critical infrastructure protection, and other
36 functions of the Department; and
37 (iii) coordinating with users of geospatial information with-
38 in the Department to ensure interoperability and prevent un-
39 necessary duplication.

40 (D) RESPONSIBILITIES.—In carrying out this subsection, the
41 responsibilities of the Chief Information Officer include—

1 (i) coordinating the geospatial information needs and ac-
2 tivities of the Department;

3 (ii) implementing standards, as adopted by the Director of
4 the Office of Management and Budget under the processes
5 established under section 216 of the E-Government Act of
6 2002 (Public Law 107-347, 44 U.S.C. 3501 note), to facili-
7 tate the interoperability of geospatial information pertaining
8 to homeland security among all users of the information in—

9 (I) the Department;

10 (II) State and local government; and

11 (III) the private sector;

12 (iii) coordinating with the Federal Geographic Data Com-
13 mittee and carrying out the responsibilities of the Department
14 pursuant to Office of Management and Budget Circular A-16
15 and Executive Order 12906 (59 Fed. Reg. 17671, 43 U.S.C.
16 1457 note); and

17 (iv) making recommendations to the Secretary and the Ex-
18 ecutive Director of the Office for State and Local Government
19 Coordination and Preparedness on awarding grants to—

20 (I) fund the creation of geospatial data; and

21 (II) execute information sharing agreements regarding
22 geospatial data with State, local, and tribal governments.

23 (3) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to
24 be appropriated such sums as may be necessary to carry out this sub-
25 section for each fiscal year.

26 **§ 11504. Chief Human Capital Officer**

27 (a) REPORTING AUTHORITY.—The Chief Human Capital Officer of the
28 Department shall report directly to the Under Secretary for Management.

29 (b) RESPONSIBILITIES.—In addition to the responsibilities set forth in
30 chapter 14 of title 5 and other applicable law, the Chief Human Capital Of-
31 ficer of the Department shall—

32 (1) develop and implement strategic workforce planning policies that
33 are consistent with Government-wide leading principles and in line with
34 Department strategic human capital goals and priorities, taking into
35 account the special requirements of members of the armed forces serv-
36 ing in the Coast Guard;

37 (2) develop performance measures to provide a basis for monitoring
38 and evaluating Department-wide strategic workforce planning efforts;

39 (3) develop, improve, and implement policies, including compensation
40 flexibilities available to Federal agencies where appropriate, to recruit,

1 hire, train, and retain the workforce of the Department, in coordination
2 with all components of the Department;

3 (4) identify methods for managing and overseeing human capital
4 programs and initiatives, in coordination with the head of each compo-
5 nent of the Department;

6 (5) develop a career path framework and create opportunities for
7 leader development in coordination with all components of the Depart-
8 ment;

9 (6) lead the efforts of the Department for managing employee re-
10 sources, including training and development opportunities, in coordina-
11 tion with each component of the Department;

12 (7) work to ensure the Department is implementing human capital
13 programs and initiatives and effectively educating each component of
14 the Department about these programs and initiatives;

15 (8) identify and eliminate unnecessary and duplicative human capital
16 policies and guidance;

17 (9) provide input concerning the hiring and performance of the Chief
18 Human Capital Officer or comparable official in each component of the
19 Department; and

20 (10) ensure that all employees of the Department are informed of
21 their rights and remedies under chapters 12 and 23 of title 5.

22 (c) COMPONENT STRATEGIES.—

23 (1) IN GENERAL.— Each component of the Department shall, in co-
24 ordination with the Chief Human Capital Officer of the Department,
25 develop a 5-year workforce strategy for the component that will support
26 the goals, objectives, and performance measures of the Department for
27 determining the proper balance of Federal employees and private labor
28 resources.

29 (2) STRATEGY REQUIREMENTS.— In developing the strategy re-
30 quired under paragraph (1), each component shall consider the effect
31 on human resources associated with creating additional Federal full-
32 time equivalent positions, converting private contractors to Federal em-
33 ployees, or relying on the private sector for goods and services.

34 (d) ANNUAL SUBMISSION.— Not later than 90 days after the date on
35 which the Secretary submits the annual budget justification for the Depart-
36 ment, the Secretary shall submit to the congressional homeland security
37 committees a report that includes a table, delineated by component with ac-
38 tual and enacted amounts, including—

39 (1) information on the progress in the Department of fulfilling the
40 workforce strategies developed under subsection (c);

1 (2) the number of on-board staffing for Federal employees from the
2 prior fiscal year;

3 (3) 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 (4) the number of full-time equivalent personnel identified under the
8 Intergovernmental Personnel Act of 1970 (42 U.S.C. 4701 et seq.).

9 (e) LIMITATION.— Nothing in this section overrides or otherwise affects
10 the requirements specified in section 10312 of this title.

11 **§ 11505. 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, poli-
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 **§ 11506. Quadrennial homeland security review**

6 (a) REQUIREMENT.—

7 (1) QUADRENNIAL REVIEWS REQUIRED.—In fiscal year 2017, 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, and the Director of National In-
23 telligence;

24 (B) key officials of the Department, including the Under Sec-
25 retary for Strategy, Policy, and Plans; and

26 (C) other relevant governmental and nongovernmental entities,
27 including State, local, and tribal government officials, members of
28 Congress, private-sector representatives, academics, and other pol-
29 icy experts.

30 (4) RELATIONSHIP WITH FUTURE YEARS HOMELAND SECURITY PRO-
31 GRAM.—The Secretary shall ensure that each review conducted under
32 this section is coordinated with the Future Years Homeland Security
33 Program required under section 10386 of this title.

34 (b) CONTENTS OF REVIEW.—In each quadrennial homeland security re-
35 view, the Secretary shall—

36 (1) delineate and update, as appropriate, the national homeland se-
37 curity strategy, consistent with appropriate national and Department
38 strategies, strategic plans, and Homeland Security Presidential Direc-
39 tives, including the National Strategy for Homeland Security, the Na-
40 tional Response Plan, and the Department Security Strategic Plan;

1 (2) outline and prioritize the full range of the critical homeland secu-
2 rity mission areas of the Nation;

3 (3) describe the interagency cooperation, preparedness of Federal re-
4 sponse assets, infrastructure, budget plan, and other elements of the
5 homeland security program and policies of the Nation associated with
6 the national homeland security strategy, required to execute success-
7 fully the full range of missions called for in the national homeland se-
8 curity strategy described in paragraph (1) and the homeland security
9 mission areas outlined under paragraph (2);

10 (4) identify the budget plan required to provide sufficient resources
11 to successfully execute the full range of missions called for in the na-
12 tional homeland security strategy described in paragraph (1) and the
13 homeland security mission areas outlined under paragraph (2);

14 (5) include an assessment of the organizational alignment of the De-
15 partment with the national homeland security strategy referred to in
16 paragraph (1) and the homeland security mission areas outlined under
17 paragraph (2); and

18 (6) review and assess the effectiveness of the mechanisms of the De-
19 partment for executing the process of turning the requirements devel-
20 oped in the quadrennial homeland security review into an acquisition
21 strategy and expenditure plan in the Department.

22 (e) REPORTING.—

23 (1) IN GENERAL.—Not later than December 31 of the year in which
24 a quadrennial homeland security review is conducted, the Secretary
25 shall submit to Congress a report regarding that quadrennial homeland
26 security review.

27 (2) CONTENTS OF REPORT.—Each report submitted under para-
28 graph (1) shall include—

29 (A) the results of the quadrennial homeland security review;

30 (B) a description of the threats to the assumed or defined na-
31 tional homeland security interests of the Nation that were exam-
32 ined for the purposes of that review;

33 (C) the national homeland security strategy, including a
34 prioritized list of the critical homeland security missions of the
35 Nation;

36 (D) a description of the interagency cooperation, preparedness
37 of Federal response assets, infrastructure, budget plan, and other
38 elements of the homeland security program and policies of the Na-
39 tion associated with the national homeland security strategy, re-
40 quired to execute successfully the full range of missions called for
41 in the applicable national homeland security strategy referred to

1 in subsection (b)(1) and the homeland security mission areas out-
2 lined under subsection (b)(2);

3 (E) an assessment of the organizational alignment of the De-
4 partment with the applicable national homeland security strategy
5 referred to in subsection (b)(1) and the homeland security mission
6 areas outlined under subsection (b)(2), including the Department's
7 organizational structure, management systems, budget and ac-
8 counting systems, human resources systems, procurement systems,
9 and physical and technical infrastructure;

10 (F) a discussion of the status of cooperation among Federal
11 agencies in the effort to promote national homeland security;

12 (G) a discussion of the status of cooperation between the Fed-
13 eral Government and State, local, and tribal governments in pre-
14 venting terrorist attacks and preparing for emergency response to
15 threats to national homeland security;

16 (H) an explanation of underlying assumptions used in con-
17 ducting the review; and

18 (I) any other matter the Secretary considers appropriate.

19 (3) PUBLIC AVAILABILITY.—The Secretary shall, consistent with the
20 protection of national security and other sensitive matters, make each
21 report submitted under paragraph (1) publicly available on the Internet
22 website of the Department.

23 (d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be
24 appropriated such sums as may be necessary to carry out this section.

25 **§ 11507. Interoperable communications**

26 (a) DEFINITION OF INTEROPERABLE COMMUNICATIONS.—The term
27 “interoperable communications” has the same meaning given that term in
28 section 10712(a) of this title.

29 (b) APPLICATION.—Subsections (c) through (e) shall apply only with re-
30 spect to the interoperable communications capabilities in the Department
31 and components of the Department to communicate with the Department.

32 (c) STRATEGY FOR ACHIEVING AND MAINTAINING INTEROPERABLE COM-
33 MUNICATIONS AMONG THE COMPONENTS OF THE DEPARTMENT.—The
34 Under Secretary for Management shall submit to the Committee on Home-
35 land Security of the House of Representatives and the Committee on Home-
36 land Security and Governmental Affairs of the Senate a strategy, which
37 shall be updated as necessary, for achieving and sustaining interoperable
38 communications among the components of the Department, including for
39 daily operations, planned events, and emergencies, with corresponding mile-
40 stones, that includes the following:

1 (1) An assessment of interoperability gaps in radio communications
2 among the components of the Department, as of July 6, 2015.

3 (2) Information on efforts and activities, including current and
4 planned policies, directives, and training, of the Department since No-
5 vember 1, 2012, to achieve and maintain interoperable communications
6 among the components of the Department, and planned efforts and ac-
7 tivities of the Department to achieve and maintain the interoperable
8 communications.

9 (3) An assessment of obstacles and challenges to achieving and
10 maintaining interoperable communications among the components of
11 the Department.

12 (4) Information on, and an assessment of, the adequacy of mecha-
13 nisms available to the Under Secretary for Management to enforce and
14 compel compliance with interoperable communications policies and di-
15 rectives of the Department.

16 (5) Guidance provided to the components of the Department to im-
17 plement interoperable communications policies and directives of the De-
18 partment.

19 (6) The total amount of funds expended by the Department since
20 November 1, 2012, and projected future expenditures, to achieve inter-
21 operable communications, including on equipment, infrastructure, and
22 maintenance.

23 (7) Dates on which Department-wide interoperability is projected to
24 be achieved for voice, data, and video communications, respectively, and
25 interim milestones that correspond to the achievement of each of those
26 modes of communications.

27 (d) SUPPLEMENTAL MATERIAL.—Together with the strategy required
28 under subsection (c), the Under Secretary for Management shall submit 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 information on—

32 (1) any intra-agency effort or task force that has been delegated cer-
33 tain responsibilities by the Under Secretary for Management relating
34 to achieving and maintaining interoperable communications among the
35 components of the Department by the dates referred to in subsection
36 (c)(7); and

37 (2) who in each component is responsible for implementing policies
38 and directives issued by the Under Secretary for Management to
39 achieve and maintain the interoperable communications.

40 (e) REPORT.—Not later than 100 days after the date on which the strat-
41 egy required under subsection (c) is submitted, and every 2 years afterwards

1 for 6 years, the Under Secretary for Management shall submit to the Com-
2 mittee on Homeland Security of the House of Representatives and the Com-
3 mittee on Homeland Security and Governmental Affairs of the Senate a re-
4 port on the status of efforts to implement the strategy required under sub-
5 section (e), including the following:

6 (1) Progress on each interim milestone referred to in subsection
7 (e)(7) toward achieving and maintaining interoperable communications
8 among the components of the Department.

9 (2) Information on any policies, directives, guidance, and training es-
10 tablished by the Under Secretary for Management.

11 (3) An assessment of the level of compliance, adoption, and partici-
12 pation among the components of the Department with the policies, di-
13 rectives, guidance, and training established by the Under Secretary for
14 Management to achieve and maintain interoperable communications
15 among the components.

16 (4) Information on any additional resources or authorities needed by
17 the Under Secretary for Management.

18 **§ 11508. Joint Task Forces**

19 (a) DEFINITION OF SITUATIONAL AWARENESS.—In this section, the term
20 “situational awareness” means knowledge and unified understanding of un-
21 lawful cross-border activity, including—

22 (1) threats and trends concerning illicit trafficking and unlawful
23 crossings;

24 (2) the ability to forecast future shifts in the threats and trends;

25 (3) the ability to evaluate the threats and trends at a level sufficient
26 to create actionable plans; and

27 (4) the operational capability to conduct continuous and integrated
28 surveillance of the air, land, and maritime borders of the United
29 States.

30 (b) ESTABLISHMENT.—The Secretary may establish and operate depart-
31 mental Joint Task Forces to conduct joint operations using personnel and
32 capabilities of the Department for the purposes specified in subsection (d).

33 (c) DIRECTOR, DEPUTY DIRECTORS, AND STAFF.—

34 (1) DIRECTOR.—

35 (A) APPOINTMENT.—Each Joint Task Force shall be headed by
36 a Director, appointed by the President, for a term of not more
37 than 2 years. The Secretary shall submit to the President rec-
38 ommendations for the appointment after consulting with the heads
39 of the components of the Department with membership on any
40 Joint Task Force. A Director shall be—

1 (i) a current senior official of the Department with not less
2 than 1 year of significant leadership experience at the De-
3 partment; or

4 (ii) if no suitable candidate is available at the Department,
5 an individual with—

6 (I) not less than 1 year of significant leadership experi-
7 ence in a Federal agency since the establishment of the
8 Department; and

9 (II) a demonstrated ability in knowledge of, and sig-
10 nificant experience working on, the issues to be ad-
11 dressed by the Joint Task Force.

12 (B) EXTENSION.—The Secretary may extend the appointment
13 of a Director of a Joint Task Force for not more than 2 years
14 if the Secretary determines that the extension is in the best inter-
15 est of the Department.

16 (2) DEPUTY DIRECTORS.—For each Joint Task Force, the Secretary
17 shall appoint a Deputy Director, who shall be an official of a different
18 component or office of the Department than the Director.

19 (3) STAFF.—Each Joint Task Force shall have a staff, composed of
20 officials from the relevant components and offices of the Department,
21 to assist the Director in carrying out the mission and responsibilities
22 of the Joint Task Force.

23 (d) PURPOSES.—

24 (1) IN GENERAL.—Subject to paragraph (2), the purposes referred
25 to in subsection (b) are or relate to the following:

26 (A) Securing the land and maritime borders of the United
27 States.

28 (B) Homeland security crises.

29 (C) Establishing regionally based operations.

30 (2) LIMITATION.—

31 (A) IN GENERAL.—The Secretary may not establish a Joint
32 Task Force for any major disaster or emergency declared under
33 the Robert T. Stafford Disaster Relief and Emergency Assistance
34 Act (42 U.S.C. 5121 et seq.) or an incident for which the Federal
35 Emergency Management Agency has primary responsibility for
36 management of the response under chapter 111 of this title, in-
37 cluding section 11103(a)(3)(A), unless the responsibilities of the
38 Joint Task Force—

39 (i) do not include operational functions relating to incident
40 management, including coordination of operations; and

1 (ii) are consistent with the requirements of paragraphs (1)
2 and (2)(A) of section 11102(b) and section 11109 of this title
3 and section 302 of the Robert T. Stafford Disaster Relief and
4 Emergency Assistance Act (42 U.S.C. 5143).

5 (B) RESPONSIBILITIES AND FUNCTIONS OF AGENCY AND AD-
6 MINISTRATOR NOT REDUCED.—Nothing in this section may be
7 construed to reduce the responsibilities or functions of the Federal
8 Emergency Management Agency or the Administrator of the Fed-
9 eral Emergency Management Agency under chapter 111 of this
10 title or any other provision of law, including the diversion of an
11 asset, function, or mission from the Federal Emergency Manage-
12 ment Agency or the Administrator of the Federal Emergency
13 Management Agency pursuant to section 11106 of this title.

14 (e) RESPONSIBILITIES.—The Director of a Joint Task Force, subject to
15 the oversight, direction, and guidance of the Secretary, shall—

16 (1) when the Joint Task Force is established for the purpose re-
17 ferred to in subsection (d)(1)(A), maintain situational awareness in the
18 areas of responsibility of the Joint Task Force, as determined by the
19 Secretary;

20 (2) provide operational plans and requirements for standard oper-
21 ating procedures and contingency operations in the areas of responsi-
22 bility of the Joint Task Force, as determined by the Secretary;

23 (3) plan and execute joint task force activities in the areas of respon-
24 sibility of the Joint Task Force, as determined by the Secretary;

25 (4) set and accomplish strategic objectives through integrated oper-
26 ational planning and execution;

27 (5) exercise operational direction over personnel and equipment from
28 components and offices of the Department allocated to the Joint Task
29 Force to accomplish the objectives of the Joint Task Force;

30 (6) when the Joint Task Force is established for the purpose re-
31 ferred to in subsection (d)(1)(A), establish operational and investigative
32 priorities in the areas of responsibility of the Joint Task Force, as de-
33 termined by the Secretary;

34 (7) coordinate with foreign governments and other Federal, State,
35 and local agencies, as appropriate, to carry out the mission of the Joint
36 Task Force; and

37 (8) carry out other duties and powers the Secretary determines ap-
38 propriate.

39 (f) PERSONNEL AND RESOURCES.—

40 (1) TEMPORARY ALLOCATION.—The Secretary, on request of the Di-
41 rector of a Joint Task Force and giving appropriate consideration of

1 risk to the other primary missions of the Department, may allocate to
2 the Joint Task Force on a temporary basis personnel and equipment
3 of components and offices of the Department.

4 (2) COST NEUTRALITY.—A Joint Task Force may not require more
5 resources than would have otherwise been required by the Department
6 to carry out the duties assigned to the Joint Task Force if the Joint
7 Task Force had not been established.

8 (3) LOCATION OF OPERATIONS.—In establishing a location of oper-
9 ations for a Joint Task Force, the Secretary shall, to the extent prac-
10 ticable, use existing facilities that integrate efforts of components of
11 the Department and State, local, tribal, or territorial law enforcement
12 or military entities.

13 (4) CONSIDERATION OF IMPACT.—When reviewing requests for allo-
14 cation of component personnel and equipment under paragraph (1), the
15 Secretary shall consider the impact of the allocation on the ability of
16 the donating component or office to carry out the primary missions of
17 the Department, and in the case of the Coast Guard, the missions spec-
18 ified in section 10312 of this title.

19 (5) LIMITATION.—Personnel and equipment of the Coast Guard allo-
20 cated under this subsection may be used only to carry out operations
21 and investigations relating to the missions specified in section 10312
22 of this title.

23 (6) REPORT.—The Secretary, at the time the budget of the Presi-
24 dent for a fiscal year is submitted to Congress under section 1105(a)
25 of title 31, shall submit to the Committee on Homeland Security and
26 the Committee on Transportation and Infrastructure of the House of
27 Representatives and the Committee on Homeland Security and Govern-
28 mental Affairs and the Committee on Commerce, Science, and Trans-
29 portation of the Senate a report on the total funding, personnel, and
30 other resources that each component or office of the Department allo-
31 cated under this subsection to each Joint Task Force to carry out the
32 mission of the Joint Task Force during the fiscal year immediately pre-
33 ceding each report, and a description of the degree to which the re-
34 sources drawn from each component or office impact the primary mis-
35 sion of the component or office.

36 (g) COMPONENT RESOURCE AUTHORITY.—As directed by the Secretary—

37 (1) each Director of a Joint Task Force shall be provided sufficient
38 resources from relevant components and offices of the Department and
39 the authority necessary to carry out the missions and responsibilities
40 of the Joint Task Force required under this section;

1 (2) the resources referred to in paragraph (1) shall be under the
2 operational authority, direction, and control of the Director of the Joint
3 Task Force to which the resources are assigned; and

4 (3) the personnel and equipment of each Joint Task Force shall re-
5 main under the administrative direction of the head of the component
6 or office of the Department that provided the personnel or equipment.

7 (h) ESTABLISHMENT OF PERFORMANCE METRICS.—The Secretary
8 shall—

9 (1) establish outcome-based and other appropriate performance
10 metrics to evaluate the effectiveness of each Joint Task Force;

11 (2) not later than 120 days after December 23, 2016, and 120 days
12 after the establishment of a new Joint Task Force, as appropriate, sub-
13 mit to the Committee on Homeland Security and the Committee on
14 Transportation and Infrastructure of the House of Representatives and
15 the Committee on Homeland Security and Governmental Affairs and
16 the Committee on Commerce, Science, and Transportation of the Sen-
17 ate the metrics established under paragraph (1); and

18 (3) not later than January 31 of each year, submit to each com-
19 mittee specified in paragraph (2) a report that contains the evaluation
20 described in paragraph (1).

21 (i) JOINT DUTY TRAINING PROGRAM.—

22 (1) IN GENERAL.—The Secretary shall—

23 (A) establish a joint duty training program in the Department
24 for the purposes of—

25 (i) enhancing coordination in the Department; and

26 (ii) promoting workforce professional development; and

27 (B) tailor the joint duty training program to improve joint oper-
28 ations as part of the Joint Task Forces.

29 (2) ELEMENTS.—The joint duty training program established under
30 paragraph (1) shall address, at a minimum, the following topics:

31 (A) National security strategy.

32 (B) Strategic and contingency planning.

33 (C) Command and control of operations under joint command.

34 (D) International engagement.

35 (E) The homeland security enterprise.

36 (F) Interagency collaboration.

37 (G) Leadership.

38 (H) Specific subject matters relevant to the Joint Task Force,
39 including matters relating to the missions specified in section
40 10312 of this title, to which the joint duty training program is as-
41 signed.

1 (3) TRAINING REQUIRED.—

2 (A) DIRECTORS AND DEPUTY DIRECTORS.—Except as provided
3 in subparagraphs (C) and (D), an individual shall complete the
4 joint duty training program before being appointed Director or
5 Deputy Director of a Joint Task Force.

6 (B) STAFF.—Each official serving on the staff of a Joint Task
7 Force shall complete the joint duty training program in the 1st
8 year of assignment to the Joint Task Force.

9 (C) EXCEPTION.—Subparagraph (A) does not apply to the 1st
10 Director or Deputy Director appointed to a Joint Task Force on
11 or after December 23, 2016.

12 (D) WAIVER.—The Secretary may waive the application of sub-
13 paragraph (A) if the Secretary determines that the waiver is in
14 the interest of homeland security or necessary to carry out the
15 mission for which a Joint Task Force was established.

16 (j) NOTIFICATION OF JOINT TASK FORCE FORMATION.—

17 (1) IN GENERAL.—Not later than 90 days before establishing a Joint
18 Task Force under this section, the Secretary shall submit to the major-
19 ity leader of the Senate, the minority leader of the Senate, The Speak-
20 er of the House of Representatives, the majority leader of the House
21 of Representatives, the minority leader of the House of Representa-
22 tives, the Committee on Homeland Security and the Committee on
23 Transportation and Infrastructure of the House of Representatives,
24 and the Committee on Homeland Security and Governmental Affairs
25 and the Committee on Commerce, Science, and Transportation of the
26 Senate a notification regarding the establishment.

27 (2) WAIVER AUTHORITY.—The Secretary may waive the requirement
28 under paragraph (1) in the event of an emergency circumstance that
29 imminently threatens the protection of human life or property.

30 (k) REVIEW.—Not later than January 31, 2018, and January 31, 2021,
31 the Inspector General of the Department shall submit to the Committee on
32 Homeland Security and the Committee on Transportation and Infrastruc-
33 ture of the House of Representatives and the Committee on Homeland Se-
34 curity and Governmental Affairs and the Committee on Commerce, Science,
35 and Transportation of the Senate a review of the Joint Task Forces estab-
36 lished under this section. The reviews shall include—

37 (1) an assessment of the effectiveness of the structure of each Joint
38 Task Force; and

39 (2) recommendations for enhancements to the structure to strength-
40 en the effectiveness of each Joint Task Force.

1 (l) JOINT DUTY ASSIGNMENT PROGRAM.—After establishing the joint
2 duty training program under subsection (i), the Secretary shall establish a
3 joint duty assignment program in the Department for the purposes of en-
4 hancing coordination in the Department and promoting workforce profes-
5 sional development.

6 (m) SUNSET.—This section expires on September 30, 2022.

7 **§ 11509. Office of Strategy, Policy, and Plans**

8 (a) IN GENERAL.—The Under Secretary for Strategy, Policy, and Plans
9 is the principal policy advisor to the Secretary.

10 (b) FUNCTIONS.—The Under Secretary for Strategy, Policy, and Plans
11 shall—

12 (1) lead, conduct, and coordinate Department-wide policy develop-
13 ment and implementation and strategic planning;

14 (2) develop and coordinate policies to promote and ensure quality,
15 consistency, and integration for the programs, components, offices, and
16 activities across the Department;

17 (3) develop and coordinate strategic plans and long-term goals of the
18 Department with risk-based analysis and planning to improve oper-
19 ational mission effectiveness, including consultation with the Secretary
20 regarding the quadrennial homeland security review under section
21 11506 of this title;

22 (4) manage Department leadership councils and provide analytics
23 and support to the councils;

24 (5) manage international coordination and engagement for the De-
25 partment;

26 (6) review and incorporate, as appropriate, external stakeholder feed-
27 back into Department policy; and

28 (7) carry out such other responsibilities as the Secretary determines
29 appropriate.

30 (c) COORDINATION BY DEPARTMENT COMPONENTS.—To ensure consist-
31 ency with the policy priorities of the Department, the head of each compo-
32 nent of the Department shall coordinate with the Office of Strategy, Policy,
33 and Plans in establishing or modifying policies or strategic planning guid-
34 ance with respect to each component.

35 (d) HOMELAND SECURITY STATISTICS AND JOINT ANALYSIS.—

36 (1) HOMELAND SECURITY STATISTICS.—The Under Secretary for
37 Strategy, Policy, and Plans shall—

38 (A) establish standards of reliability and validity for statistical
39 data collected and analyzed by the Department;

1 (B) be provided by the heads of all components of the Depart-
 2 ment with statistical data maintained by the Department regard-
 3 ing the operations of the Department.

4 (C) conduct or oversee analysis and reporting of the data by the
 5 Department as required by law or as directed by the Secretary;
 6 and

7 (D) ensure the accuracy of metrics and statistical data provided
 8 to Congress.

9 (2) TRANSFER OF RESPONSIBILITIES.—There shall be transferred to
 10 the Under Secretary for Strategy, Policy, and Plans the maintenance
 11 of all immigration statistical information of U.S. Customs and Border
 12 Protection, U.S. Immigration and Customs Enforcement, and U.S.
 13 Citizenship and Immigration Services, which shall include information
 14 and statistics of the type contained in the publication entitled “Year-
 15 book of Immigration Statistics” prepared by the Office of Immigration
 16 Statistics, including region-by-region statistics on the aggregate num-
 17 ber of applicants and petitions filed by an alien (or filed on behalf of
 18 an alien) and denied, and the reasons for the denial, disaggregated by
 19 category of denial and application or petition type.

20 (e) LIMITATION.—Nothing in this section overrides or otherwise affects
 21 the requirements specified in section 10312 of this title.

22 **Chapter 117—Coordination With Other** 23 **Entities**

Sec.

11701. Responsibilities of Office for State and Local Government Coordination.

11702. Responsibilities of Office for National Capital Region Coordination.

11703. Joint Interagency Task Force.

11704. Coordination with Department of Health and Human Services under the Public
 Health Service Act.

11705. Aviation security.

11706. Investigation of violent acts, shootings, and mass killings.

11707. Facilitating homeland security information sharing procedures.

11708. Information sharing.

11709. Prevention of international child abduction.

11710. Limitation of liability.

24 **§ 11701. Responsibilities of Office for State and Local Gov-** 25 **ernment Coordination**

26 The Office for State and Local Government Coordination oversees and co-
 27 ordinates departmental programs for and relationships with State and local
 28 governments. The Office shall—

29 (1) coordinate the activities of the Department relating to State and
 30 local government;

31 (2) assess, and advocate for, the resources needed by State and local
 32 government to implement the national strategy for combating ter-
 33 rorism;

1 (3) provide State and local government with regular information, re-
2 search, and technical support to assist local efforts at securing the
3 homeland; and

4 (4) develop a process for receiving meaningful input from State and
5 local government to assist the development of the national strategy for
6 combating terrorism and other homeland security activities.

7 **§ 11702. Responsibilities of Office for National Capital Re-**
8 **gion Coordination**

9 (a) IN GENERAL.—The Office for National Capital Region Coordination
10 oversees and coordinates Federal programs for and relationships with State,
11 local, and regional authorities in the National Capital Region, as defined
12 under section 2674(f)(2) of title 10.

13 (b) COOPERATION WITH NATIONAL CAPITAL REGION OFFICIALS.—The
14 Secretary shall cooperate with the Mayor of the District of Columbia, the
15 Governors of Maryland and Virginia, and other State, local, and regional
16 officers in the National Capital Region to integrate the District of Colum-
17 bia, Maryland, and Virginia into the planning, coordination, and execution
18 of the activities of the Federal Government for the enhancement of domestic
19 preparedness against the consequences of terrorist attacks.

20 (c) RESPONSIBILITIES.—The Office for National Capital Region Coordi-
21 nation shall—

22 (1) coordinate the activities of the Department relating to the Na-
23 tional Capital Region, including cooperation with the Office for State
24 and Local Government Coordination;

25 (2) assess, and advocate for, the resources needed by State, local,
26 and regional authorities in the National Capital Region to implement
27 efforts to secure the homeland;

28 (3) provide State, local, and regional authorities in the National Cap-
29 ital Region with regular information, research, and technical support
30 to assist the efforts of State, local, and regional authorities in the Na-
31 tional Capital Region in securing the homeland;

32 (4) develop a process for receiving meaningful input from State,
33 local, and regional authorities and the private sector in the National
34 Capital Region to assist in the development of the homeland security
35 plans and activities of the Federal Government;

36 (5) coordinate with Federal agencies in the National Capital Region
37 on terrorism preparedness, to ensure adequate planning, information
38 sharing, training, and execution of the Federal role in domestic pre-
39 paredness activities;

40 (6) coordinate with Federal, State, local, and regional agencies, and
41 the private sector in the National Capital Region on terrorism pre-

1 (3) POTENTIAL PUBLIC HEALTH EMERGENCY.—In cases involving,
 2 or potentially involving, a public health emergency, but in which no de-
 3 termination of an emergency by the Secretary of Health and Human
 4 Services under section 319(a) of the Public Health Service Act (42
 5 U.S.C. 247d(a)) has been made, all relevant agencies, including the De-
 6 partment, the Department of Justice, and the Federal Bureau of Inves-
 7 tigation, shall keep the Secretary of Health and Human Services and
 8 the Director of the Centers for Disease Control and Prevention fully
 9 and currently informed.

10 **§ 11705. Aviation security**

11 (a) CONSULTATION WITH FEDERAL AVIATION ADMINISTRATION.—The
 12 Secretary and other officials in the Department shall consult with the Ad-
 13 ministrator of the Federal Aviation Administration before taking an action
 14 that might affect aviation safety, air carrier operations, aircraft airworthi-
 15 ness, or the use of airspace. The Secretary shall establish a liaison office
 16 in the Department to consult with the Administrator of the Federal Avia-
 17 tion Administration.

18 (b) LIMITATIONS ON STATUTORY CONSTRUCTION.—

19 (1) GRANT OF AUTHORITY.—Nothing in this subtitle may be con-
 20 strued to vest in the Secretary or another official in the Department
 21 authority over transportation security that is not vested in the Admin-
 22 istrator of the Transportation Security Administration, or that was not
 23 vested in the Secretary of Transportation under chapter 449 of title
 24 49 on November 24, 2002.

25 (2) OBLIGATION OF AIP FUNDS.—Nothing in this subtitle may be
 26 construed to authorize the Secretary or any other official in the De-
 27 partment to obligate amounts made available under section 48103 of
 28 title 49.

29 **§ 11706. Investigation of violent acts, shootings, and mass**
 30 **killings**

31 (a) DEFINITIONS.—In this section:

32 (1) MASS KILLINGS.—The term “mass killings” means 3 or more
 33 killings in a single incident.

34 (2) PLACE OF PUBLIC USE.—The term “place of public use” has the
 35 meaning given the term under section 2332f(e)(6) of title 18.

36 (b) PROVIDING ASSISTANCE.—At the request of an appropriate law en-
 37 forcement official of a State or political subdivision, the Secretary, through
 38 deployment of the Secret Service or U.S. Immigration and Customs En-
 39 forcement, may assist in the investigation of violent acts and shootings oc-
 40 curring in a place of public use, and in the investigation of mass killings
 41 and attempted mass killings. Any assistance provided by the Secretary

1 under this subsection shall be presumed to be within the scope of a Federal
2 office or of Federal employment.

3 **§ 11707. Facilitating homeland security information sharing**
4 **procedures**

5 (a) DEFINITIONS.—In this section:

6 (1) HOMELAND SECURITY INFORMATION.—The term “homeland se-
7 curity information” means information possessed by a Federal, State,
8 or local agency that—

9 (A) relates to the threat of terrorist activity;

10 (B) relates to the ability to prevent, interdict, or disrupt ter-
11 rorist activity;

12 (C) would improve the identification or investigation of a sus-
13 pected terrorist or terrorist organization; or

14 (D) would improve the response to a terrorist act.

15 (2) INTELLIGENCE COMMUNITY.—The term “intelligence commu-
16 nity” has the meaning given the term in section 3(4) of the National
17 Security Act of 1947 (50 U.S.C. 3003(4)).

18 (3) STATE AND LOCAL PERSONNEL.—The term “State and local per-
19 sonnel” means any of the following persons involved in the prevention
20 of, preparation for, or response to terrorist attack:

21 (A) State Governors, mayors, and other locally elected officials.

22 (B) State and local law enforcement personnel and firefighters.

23 (C) Public health and medical professionals.

24 (D) Regional, State, and local emergency management agency
25 personnel, including State adjutant generals.

26 (E) Other appropriate emergency response agency personnel.

27 (F) Employees of private-sector entities that affect critical in-
28 frastructure, cyber, economic, or public health security, as des-
29 ignated by the Federal Government in procedures developed under
30 this section.

31 (b) PROCEDURES FOR DETERMINING EXTENT OF SHARING OF HOME-
32 LAND SECURITY INFORMATION.—

33 (1) ESTABLISHMENT OF PROCEDURES.—The President shall pre-
34 scribe and implement procedures under which relevant Federal agen-
35 cies—

36 (A) share relevant and appropriate homeland security informa-
37 tion with other Federal agencies, including the Department, and
38 appropriate State and local personnel;

39 (B) identify and safeguard homeland security information that
40 is sensitive but unclassified; and

1 (C) to the extent the information is in classified form, determine
2 whether, how, and to what extent to remove classified information,
3 as appropriate, and with which personnel it may be shared after
4 the information is removed.

5 (2) APPLICABILITY.—The President shall ensure that the procedures
6 apply to all agencies of the Federal Government.

7 (3) NO CHANGE IN SUBSTANTIVE REQUIREMENTS.—The procedures
8 shall not change the substantive requirements for the classification and
9 safeguarding of classified information.

10 (4) NO CHANGE IN PROTECTIVE AUTHORITIES.—The procedures
11 shall not change the requirements and authorities to protect sources
12 and methods.

13 (e) PROCEDURES FOR SHARING OF HOMELAND SECURITY INFORMA-
14 TION.—

15 (1) IN GENERAL.—Under procedures prescribed by the President, all
16 appropriate agencies, including the intelligence community, shall,
17 through information sharing systems, share homeland security informa-
18 tion with Federal agencies and appropriate State and local personnel
19 to the extent the information may be shared, as determined under sub-
20 section (b), together with assessments of the credibility of the informa-
21 tion.

22 (2) SYSTEM CAPABILITIES.—Each information sharing system
23 through which information is shared under paragraph (1) shall—

24 (A) have the capability to transmit unclassified or classified in-
25 formation, though the procedures and recipients for each capa-
26 bility may differ;

27 (B) have the capability to restrict delivery of information to
28 specified subgroups by geographic location, type of organization,
29 position of a recipient within an organization, or a recipient's need
30 to know the information;

31 (C) be configured to allow the efficient and effective sharing of
32 information; and

33 (D) be accessible to appropriate State and local personnel.

34 (3) USE CONDITIONS.—The procedures prescribed under paragraph
35 (1) shall establish conditions on the use of information shared under
36 paragraph (1)—

37 (A) to limit the re-dissemination of the information to ensure
38 that the information is not used for an unauthorized purpose;

39 (B) to ensure the security and confidentiality of the informa-
40 tion;

1 (C) to protect the constitutional and statutory rights of individ-
2 uals who are subjects of the information; and

3 (D) to provide data integrity through the timely removal and
4 destruction of obsolete or erroneous names and information.

5 (4) INCLUSION OF EXISTING SYSTEMS.—The procedures prescribed
6 under paragraph (1) shall ensure, to the greatest extent practicable,
7 that the information sharing system through which information is
8 shared under that paragraph include existing information sharing sys-
9 tems, including the National Law Enforcement Telecommunications
10 System, the Regional Information Sharing System, and the Terrorist
11 Threat Warning System of the Federal Bureau of Investigation.

12 (5) AGENCY ACCESS.—Each appropriate Federal agency, as deter-
13 mined by the President, shall have access to each information sharing
14 system through which information is shared under paragraph (1), and
15 shall therefore have access to all information, as appropriate, shared
16 under that paragraph.

17 (6) SHARING INFORMATION.—The procedures prescribed under para-
18 graph (1) shall ensure that appropriate State and local personnel are
19 authorized to use the information sharing systems—

20 (A) to access information shared with the personnel; and

21 (B) to share, with others who have access to the information
22 sharing systems, the homeland security information of their own
23 jurisdictions, which shall be marked appropriately as pertaining to
24 potential terrorist activity.

25 (7) ASSESSMENT AND INTEGRATION OF INFORMATION.—Under pro-
26 cedures prescribed jointly by the Director of National Intelligence and
27 the Attorney General, each appropriate Federal agency, as determined
28 by the President, shall review and assess the information shared under
29 paragraph (6) and integrate the information with existing intelligence.

30 (d) SHARING OF CLASSIFIED INFORMATION AND SENSITIVE BUT UN-
31 CLASSIFIED INFORMATION WITH STATE AND LOCAL PERSONNEL.—

32 (1) IN GENERAL.—The President shall prescribe procedures under
33 which Federal agencies may, to the extent the President considers nec-
34 essary, share with appropriate State and local personnel homeland se-
35 curity information that remains classified or otherwise protected after
36 the determinations prescribed under the procedures set forth in sub-
37 section (b) are made.

38 (2) TRAINING PROGRAM.—

39 (A) ESTABLISHMENT.—The Secretary shall establish a program
40 to provide appropriate training to officials described in subpara-
41 graph (B) in order to assist the officials in—

1 (i) identifying sources of potential terrorist threats through
2 the methods the Secretary determines are appropriate;

3 (ii) reporting information relating to the potential terrorist
4 threats to the appropriate Federal agencies in the appropriate
5 form and manner;

6 (iii) assuring that all reported information is systematically
7 submitted to and passed on by the Department for use by ap-
8 propriate Federal agencies; and

9 (iv) understanding the mission and roles of the intelligence
10 community to promote more effective information sharing
11 among Federal, State, and local officials and representatives
12 of the private sector to prevent terrorist attacks against the
13 United States.

14 (B) TRAINING COVERAGE.—The officials referred to in subpara-
15 graph (A) are officials of State and local government agencies and
16 representatives of private-sector entities with responsibilities relat-
17 ing to the oversight and management of first responders, counter-
18 terrorism activities, or critical infrastructure.

19 (C) CONSULTATION WITH ATTORNEY GENERAL.—The Secretary
20 shall consult with the Attorney General to ensure that the training
21 program established in subparagraph (A) does not duplicate the
22 training program established in section 908 of the USA PA-
23 TRIOT Act (Public Law 107–56, 28 U.S.C. 509 note).

24 (D) OTHER CONSULTATION.—The Secretary shall carry out this
25 paragraph in consultation with the Director of National Intel-
26 ligence and the Attorney General.

27 (e) RESPONSIBLE OFFICIALS.—For each affected Federal agency, the
28 head of the agency shall designate an official to administer this subtitle with
29 respect to the agency.

30 (f) FEDERAL CONTROL OF INFORMATION.—Under procedures prescribed
31 under this section, information obtained by a State or local government
32 from a Federal agency under this section shall remain under the control of
33 the Federal agency, and a State or local law authorizing or requiring a gov-
34 ernment to disclose information shall not apply to the information.

35 (g) CONSTRUCTION.—Nothing in this subtitle shall be construed as au-
36 thORIZING a department, bureau, agency, officer, or employee of the Federal
37 Government to request, receive, or transmit to another Government entity
38 or any Government personnel, or transmit to a State or local entity or State
39 or local personnel otherwise authorized by the Homeland Security Act of
40 2002 (Public Law 107–296, 116 Stat. 2135) to receive homeland security
41 information, information collected by the Federal Government solely for sta-

1 tistical purposes in violation of any other provision of law relating to the
2 confidentiality of the information.

3 (h) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be
4 appropriated such sums as may be necessary to carry out this section.

5 **§ 11708. Information sharing**

6 (a) DEFINITIONS.—In this section:

7 (1) HOMELAND SECURITY INFORMATION.—The term “homeland se-
8 curity information” has the meaning given the term in section
9 11707(a) of this title.

10 (2) INFORMATION SHARING COUNCIL.—The term “Information Shar-
11 ing Council” means the Information Sharing Council established by
12 Executive Order 13388 (Oct. 25, 2005, 70 F.R. 62023), or any suc-
13 cessor body designated by the President, and referred to under sub-
14 section (e).

15 (3) INFORMATION SHARING ENVIRONMENT; ISE.—The terms “infor-
16 mation sharing environment” and “ISE” mean an approach that facili-
17 tates the sharing of terrorism and homeland security information,
18 which may include any method determined necessary and appropriate
19 for carrying out this section.

20 (4) PROGRAM MANAGER.—The term “program manager” means the
21 program manager designated under subsection (d).

22 (5) TERRORISM INFORMATION.—The term “terrorism informa-
23 tion”—

24 (A) means all information, whether collected, produced, or dis-
25 tributed by intelligence, law enforcement, military, homeland secu-
26 rity, or other activities relating to—

27 (i) the existence, organization, capabilities, plans, inten-
28 tions, vulnerabilities, means of finance or material support, or
29 activities of foreign or international terrorist groups or indi-
30 viduals, or of domestic groups or individuals involved in
31 transnational terrorism;

32 (ii) threats posed by the groups or individuals to the
33 United States, United States persons, or United States inter-
34 ests, or to those of other nations;

35 (iii) communications of or by the groups or individuals; or

36 (iv) other groups or individuals reasonably believed to be
37 assisting or associated with the groups or individuals; and

38 (B) includes weapons of mass destruction information.

39 (6) WEAPONS OF MASS DESTRUCTION INFORMATION.—The term
40 “weapons of mass destruction information” means information that
41 could reasonably be expected to assist in the development, proliferation,

1 or use of a weapon of mass destruction (including a chemical, biologi-
2 cal, radiological, or nuclear weapon) that could be used by a terrorist
3 or a terrorist organization against the United States, including infor-
4 mation about the location of a stockpile of nuclear materials that could
5 be exploited for use in a weapon that could be used by a terrorist or
6 a terrorist organization against the United States.

7 (b) INFORMATION SHARING ENVIRONMENT.—

8 (1) ESTABLISHMENT.—The President shall—

9 (A) create an information sharing environment for the sharing
10 of terrorism information in a manner consistent with national se-
11 curity and with applicable legal standards relating to privacy and
12 civil liberties;

13 (B) designate the organizational and management structures
14 that will be used to operate and manage the ISE; and

15 (C) determine and enforce the policies, directives, and rules that
16 will govern the content and usage of the ISE.

17 (2) ATTRIBUTES.—The President shall, through the structures de-
18 scribed in subparagraphs (B) and (C) of paragraph (1), ensure that
19 the ISE provides and facilitates the means for sharing terrorism infor-
20 mation among all appropriate Federal, State, local, and tribal entities,
21 and the private sector through the use of policy guidelines and tech-
22 nologies. The President shall, to the greatest extent practicable, ensure
23 that the ISE provides the functional equivalent of, or otherwise sup-
24 ports, a decentralized, distributed, and coordinated environment that—

25 (A) connects existing systems, where appropriate, provides no
26 single points of failure, and allows users to share information
27 among agencies, between levels of government, and, as appro-
28 priate, with the private sector;

29 (B) ensures direct and continuous online electronic access to in-
30 formation;

31 (C) facilitates the availability of information in a form and man-
32 ner that facilitates its use in analysis, investigations, and oper-
33 ations;

34 (D) builds upon existing systems capabilities currently in use
35 across the Government;

36 (E) employs an information access management approach that
37 controls access to data rather than just systems and networks,
38 without sacrificing security;

39 (F) facilitates the sharing of information at and across all levels
40 of security;

1 (G) provides directory services, or the functional equivalent, for
2 locating people and information;

3 (H) incorporates protections for individuals' privacy and civil
4 liberties;

5 (I) incorporates strong mechanisms to enhance accountability
6 and facilitate oversight, including audits, authentication, and ac-
7 cess controls;

8 (J) integrates the information within the scope of the informa-
9 tion sharing environment, including information in legacy tech-
10 nologies;

11 (K) integrates technologies, including all legacy technologies,
12 through Internet-based services, consistent with appropriate secu-
13 rity protocols and safeguards, to enable connectivity among re-
14 quired users at the Federal, State, and local levels;

15 (L) allows the full range of analytic and operational activities
16 without the need to centralize information within the scope of the
17 information sharing environment;

18 (M) permits analysts to collaborate both independently and in
19 a group (commonly known as "collective and noncollective collabo-
20 ration"), and across multiple levels of national security informa-
21 tion and controlled unclassified information;

22 (N) provides a resolution process that enables changes by au-
23 thorized officials regarding rules and policies for the access, use,
24 and retention of information within the scope of the information
25 sharing environment; and

26 (O) incorporates continuous, real-time, and immutable audit ca-
27 pabilities, to the maximum extent practicable.

28 (e) GUIDELINES AND REQUIREMENTS.—The President shall—

29 (1) leverage all ongoing efforts consistent with establishing the ISE
30 and issue guidelines for acquiring, accessing, sharing, and using infor-
31 mation, including guidelines to ensure that information is provided in
32 its most shareable form, such as by using tearlines to separate out data
33 from the sources and methods by which the data are obtained;

34 (2) in consultation with the Privacy and Civil Liberties Oversight
35 Board established under section 1061 of the Intelligence Reform and
36 Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee), issue guidelines
37 that—

38 (A) protect privacy and civil liberties in the development and
39 use of the ISE; and

40 (B) shall be made public, unless nondisclosure is clearly nec-
41 essary to protect national security; and

1 (3) require the heads of Federal departments and agencies to pro-
2 mote a culture of information sharing by—

3 (A) reducing disincentives to information sharing, including
4 over-classification of information and unnecessary requirements
5 for originator approval, consistent with applicable laws and regula-
6 tions; and

7 (B) providing affirmative incentives for information sharing.

8 (d) PROGRAM MANAGER.—

9 (1) DESIGNATION.—The President shall designate an individual as
10 the program manager responsible for information sharing across the
11 Federal Government. The individual designated as the program man-
12 ager shall serve as program manager until removed from service or re-
13 placed by the President (at the President's sole discretion). The pro-
14 gram manager, in consultation with the head of an affected department
15 or agency, shall have and exercise government-wide authority over the
16 sharing of information within the scope of the information sharing en-
17 vironment, including homeland security information, terrorism informa-
18 tion, and weapons of mass destruction information, by all Federal de-
19 partments, agencies, and components, irrespective of the Federal de-
20 partment, agency, or component in which the program manager may
21 be administratively located, except as otherwise expressly provided by
22 law.

23 (2) DUTIES AND RESPONSIBILITIES.—

24 (A) IN GENERAL.—The program manager shall, in consultation
25 with the Information Sharing Council—

26 (i) plan for and oversee the implementation of, and man-
27 age, the ISE;

28 (ii) assist in the development of policies, as appropriate, to
29 foster the development and proper operation of the ISE;

30 (iii) consistent with the direction and policies issued by the
31 President, the Director of National Intelligence, and the Di-
32 rector of the Office of Management and Budget, issue govern-
33 ment-wide procedures, guidelines, instructions, and functional
34 standards, as appropriate, for the management, development,
35 and proper operation of the ISE;

36 (iv) identify and resolve information sharing disputes be-
37 tween Federal departments, agencies, and components; and

38 (v) assist, monitor, and assess the implementation of the
39 ISE by Federal departments and agencies to ensure adequate
40 progress, technological consistency, and policy compliance;
41 and regularly report the findings to Congress.

1 (B) CONTENT OF POLICIES, PROCEDURES, GUIDELINES, RULES,
2 AND STANDARDS.—The policies, procedures, guidelines, rules, and
3 standards under clauses (ii) and (iii) of subparagraph (A) shall—

4 (i) take into account the varying missions and security re-
5 quirements of agencies participating in the ISE;

6 (ii) address development, implementation, and oversight of
7 technical standards and requirements;

8 (iii) take into account ongoing and planned efforts that
9 support development, implementation, and management of
10 the ISE;

11 (iv) address and facilitate information sharing between and
12 among departments and agencies of the intelligence commu-
13 nity, the Department of Defense, the homeland security com-
14 munity, and the law enforcement community;

15 (v) address and facilitate information sharing between Fed-
16 eral departments and agencies and State, tribal, and local
17 governments;

18 (vi) address and facilitate, as appropriate, information
19 sharing between Federal departments and agencies and the
20 private sector;

21 (vii) address and facilitate, as appropriate, information
22 sharing between Federal departments and agencies with for-
23 eign partners and allies; and

24 (viii) ensure the protection of privacy and civil liberties.

25 (e) INFORMATION SHARING COUNCIL.—

26 (1) ESTABLISHMENT.—There is in the Department the Information
27 Sharing Council that assists the President and the program manager
28 in their duties under this section. The Information Sharing Council
29 serves until removed from service or replaced by the President (at the
30 sole discretion of the President) with a successor body.

31 (2) SPECIFIC DUTIES.—In assisting the President and the program
32 manager in their duties under this section, the Information Sharing
33 Council shall—

34 (A) advise the President and the program manager in devel-
35 oping policies, procedures, guidelines, roles, and standards nec-
36 essary to establish, implement, and maintain the ISE;

37 (B) work to ensure coordination among the Federal depart-
38 ments and agencies participating in the ISE in the establishment,
39 implementation, and maintenance of the ISE;

40 (C) identify and, as appropriate, recommend the consolidation
41 and elimination of current programs, systems, and processes used

1 by Federal departments and agencies to share information, and
2 recommend, as appropriate, the redirection of existing resources to
3 support the ISE;

4 (D) identify gaps, if any, between existing technologies, pro-
5 grams, and systems used by Federal departments and agencies to
6 share information and the parameters of the proposed information
7 sharing environment;

8 (E) recommend solutions to address gaps identified under sub-
9 paragraph (D);

10 (F) recommend means by which the ISE can be extended to
11 allow interchange of information between Federal departments and
12 agencies and appropriate authorities of State and local govern-
13 ments;

14 (G) assist the program manager in identifying and resolving in-
15 formation sharing disputes between Federal departments, agen-
16 cies, and components;

17 (H) identify appropriate personnel for assignment to the pro-
18 gram manager to support staffing needs identified by the program
19 manager; and

20 (I) recommend whether or not, and by which means, the ISE
21 should be expanded so as to allow future expansion encompassing
22 other relevant categories of information.

23 (3) CONSULTATION.—In performing its duties, the Information
24 Sharing Council shall consider input from persons and entities outside
25 the Federal Government having significant experience and expertise in
26 policy, technical matters, and operational matters relating to the ISE.

27 (4) INAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.—The
28 Information Sharing Council (including a subsidiary group of the
29 Council) is not subject to the requirements of the Federal Advisory
30 Committee Act (5 U.S.C. App.).

31 (5) DETAILEES.—On a request by the Director of National Intel-
32 ligence, the departments and agencies represented on the Information
33 Sharing Council shall detail to the program manager, on a reimburs-
34 able basis, appropriate personnel identified under paragraph (2)(H).

35 (f) PERFORMANCE MANAGEMENT REPORTS.—

36 (1) IN GENERAL.—Not later than June 30 each year, the President
37 shall submit to Congress a report on the state of the ISE and of infor-
38 mation sharing across the Federal Government.

39 (2) CONTENT.—Each report under this subsection shall include—

40 (A) a progress report on the extent to which the ISE has been
41 implemented, including how the ISE has fared on the performance

1 measures and whether the performance goals set in the preceding
2 year have been met;

3 (B) objective system-wide performance goals for the following
4 year;

5 (C) an accounting of how much was spent on the ISE in the
6 preceding year;

7 (D) actions taken to ensure that procurement of and invest-
8 ments in systems and technology are consistent with the imple-
9 mentation plan for the ISE;

10 (E) the extent to which all terrorism watch lists are available
11 for combined searching in real time through the ISE and whether
12 there are consistent standards for placing individuals on, and re-
13 moving individuals from, the watch lists, including the availability
14 of processes for correcting errors;

15 (F) the extent to which State, tribal, and local officials are par-
16 ticipating in the ISE;

17 (G) the extent to which private-sector data, including informa-
18 tion from owners and operators of critical infrastructure, is incor-
19 porated in the ISE, and the extent to which individuals and enti-
20 ties outside the government are receiving information through the
21 ISE;

22 (H) the measures taken by the Federal government to ensure
23 the accuracy of information in the ISE, in particular the accuracy
24 of information about individuals;

25 (I) an assessment of the privacy and civil liberties protections
26 of the ISE, including actions taken in the preceding year to imple-
27 ment or enforce privacy and civil liberties protections; and

28 (J) an assessment of the security protections used in the ISE.

29 (g) AGENCY RESPONSIBILITIES.—The head of each department or agency
30 that possesses or uses intelligence or terrorism information, operates a sys-
31 tem in the ISE, or otherwise participates (or expects to participate) in the
32 ISE shall—

33 (1) ensure full department or agency compliance with information
34 sharing policies, procedures, guidelines, rules, and standards estab-
35 lished under subsections (b) and (f);

36 (2) ensure the provision of adequate resources for systems and ac-
37 tivities supporting operation of and participation in the ISE;

38 (3) ensure full department or agency cooperation in the development
39 of the ISE to implement government-wide information sharing; and

1 (4) submit, at the request of the President or the program manager,
2 reports on the implementation of the requirements of the ISE within
3 the department or agency.

4 (h) ADDITIONAL POSITIONS.—The program manager may hire not more
5 than 40 full-time employees to assist the program manager in—

6 (1) activities associated with the implementation of the information
7 sharing environment, including

8 (A) implementing the requirements under subsection (b)(2); and

9 (B) any additional implementation initiatives to enhance and ex-
10 pedite the creation of the information sharing environment; and

11 (2) identifying and resolving information sharing disputes between
12 Federal departments, agencies, and components under subsection
13 (d)(2)(A)(iv).

14 **§ 11709. Prevention of international child abduction**

15 (a) PROGRAM ESTABLISHED.—The Secretary, through the Commissioner
16 of U.S. Customs and Border Protection, in coordination with the Secretary
17 of State, the Attorney General, and the Director of the Federal Bureau of
18 Investigation, shall establish a program that—

19 (1) seeks to prevent a child (as defined in section 1204(b)(1) of title
20 18) from departing from the territory of the United States if a parent
21 or legal guardian of the child presents a court order from a court of
22 competent jurisdiction prohibiting the removal of the child from the
23 United States to a U.S. Customs and Border Protection Officer in suf-
24 ficient time to prevent the departure for the duration of the court
25 order; and

26 (2) leverages other existing authorities and processes to address the
27 wrongful removal and return of a child.

28 (b) INTERAGENCY COORDINATION.—

29 (1) IN GENERAL.—The Secretary of State shall convene and chair
30 an interagency working group to prevent international parental child
31 abduction. The group shall be composed of presidentially appointed,
32 Senate confirmed officials from—

33 (A) the Department of State;

34 (B) the Department of Homeland Security, including U.S. Cus-
35 toms and Border Protection and U.S. Immigration and Customs
36 Enforcement; and

37 (C) the Department of Justice, including the Federal Bureau of
38 Investigation.

39 (2) DEPARTMENT OF DEFENSE.—The Secretary of Defense shall
40 designate an official in the Department of Defense—

1 (A) to coordinate with the Department of State on international
2 child abduction issues; and

3 (B) to oversee activities designed to prevent or resolve inter-
4 national child abduction cases relating to active duty military serv-
5 ice members.

6 **§ 11710. Limitation of liability**

7 A person who has completed a security awareness training course ap-
8 proved by or operated under a cooperative agreement with the Department,
9 who is enrolled in a program recognized or acknowledged by an Information
10 Sharing and Analysis Center and who reports a situation, activity or inci-
11 dent pursuant to that program to an appropriate authority, shall not be lia-
12 ble for damages in an action brought in a Federal or State court which re-
13 sult from an act or omission unless the person is guilty of gross negligence
14 or willful misconduct.

15 **Chapter 119—Homeland Security Council**

Sec.

11901. Establishment.

11902. Membership.

11903. Functions and activities.

11904. Staff.

11905. Joint meetings with National Security Council.

16 **§ 11901. Establishment**

17 There is in the Executive Office of the President the Homeland Security
18 Council to advise the President on homeland security matters.

19 **§ 11902. Membership**

20 (a) MEMBERS.—The members of the Homeland Security Council are the
21 following:

22 (1) The President.

23 (2) The Vice President.

24 (3) The Secretary.

25 (4) The Attorney General.

26 (5) The Secretary of Defense.

27 (6) Other individuals who may be designated by the President.

28 (b) ATTENDANCE OF CHAIRMAN OF JOINT CHIEFS OF STAFF AT MEET-
29 INGS.—The Chairman of the Joint Chiefs of Staff (or, in the absence of
30 the Chairman, the Vice Chairman of the Joint Chiefs of Staff) may, in the
31 role of the Chairman of the Joint Chiefs of Staff as principal military ad-
32 viser to the Homeland Security Council and subject to the direction of the
33 President, attend and participate in meetings of the Council.

34 **§ 11903. Functions and activities**

35 To effectively coordinate the policies and functions of the United States
36 Government relating to homeland security, the Homeland Security Council
37 shall—

1 (1) assess the objectives, commitments, and risks of the United
2 States in the interest of homeland security and make resulting rec-
3 ommendations to the President;

4 (2) oversee and review homeland security policies of the Federal Gov-
5 ernment and make resulting recommendations to the President; and

6 (3) perform other functions that the President may direct.

7 **§ 11904. Staff**

8 (a) HEADED BY EXECUTIVE SECRETARY.—The Homeland Security
9 Council has a staff, the head of which is a civilian Executive Secretary ap-
10 pointed by the President.

11 (b) PAY OF EXECUTIVE SECRETARY.—The President shall fix the pay of
12 the Executive Secretary at a rate not to exceed the rate of pay payable to
13 the Executive Secretary of the National Security Council.

14 **§ 11905. Joint meetings with National Security Council**

15 The President may convene joint meetings of the Homeland Security
16 Council and the National Security Council with participation by members
17 of either Council or as the President may otherwise direct.

18 **Chapter 121—Emergency Communications**

Sec.

12101. Definition; rule of construction.

12102. Responsibilities of Director for Emergency Communications.

12103. National Emergency Communications Plan.

12104. Assessments and reports.

12105. Coordination of Department emergency communications grant programs.

12106. Regional Emergency Communications Coordination.

12107. Emergency Communications Preparedness Center.

12108. Urban and other high risk area communications capabilities.

12109. Interoperable Emergency Communications Grant Program.

19 **§ 12101. Definition; rule of construction**

20 (a) DEFINITION.—In this chapter, the terms “interoperable communica-
21 tions” and “interoperable emergency communications” have the meaning
22 given the term “interoperable communications” under section 10712(a) of
23 this title.

24 (b) RULE OF CONSTRUCTION.— Nothing in this chapter or in sections
25 10713 or 10714 of this title shall be construed to transfer to the Office of
26 Emergency Communications any function, personnel, asset, component, au-
27 thority, grant program, or liability of the Federal Emergency Management
28 Agency as constituted on June 1, 2006.

29 **§ 12102. Responsibilities of Director for Emergency Commu-
30 nications**

31 (a) IN GENERAL.—The Director for Emergency Communications shall—

32 (1) assist the Secretary in developing and implementing the program
33 described in section 10712(b)(1) of this title, except as provided in sec-
34 tion 10713 of this title;

1 (2) administer the Department's responsibilities and authorities re-
2 relating to the SAFECOM Program, excluding elements related to re-
3 search, development, testing, and evaluation and standards;

4 (3) administer the Department's responsibilities and authorities re-
5 relating to the Integrated Wireless Network program;

6 (4) conduct extensive, nationwide outreach to support and promote
7 the ability of emergency response providers and relevant government
8 officials to continue to communicate in the event of natural disasters,
9 acts of terrorism, and other man-made disasters;

10 (5) conduct extensive, nationwide outreach and foster the develop-
11 ment of interoperable emergency communications capabilities by State,
12 regional, local, and tribal governments and public safety agencies, and
13 by regional consortia thereof;

14 (6) provide technical assistance to State, regional, local, and tribal
15 government officials with respect to use of interoperable emergency
16 communications capabilities;

17 (7) coordinate with the Regional Administrators regarding the activi-
18 ties of Regional Emergency Communications Coordination Working
19 Groups under section 12106 of this title;

20 (8) promote the development of standard operating procedures and
21 best practices with respect to use of interoperable emergency commu-
22 nications capabilities for incident response, and facilitate the sharing
23 of information on best practices for achieving, maintaining, and en-
24 hancing interoperable emergency communications capabilities for re-
25 sponse;

26 (9) coordinate, in cooperation with the National Communications
27 System, the establishment of a national response capability with initial
28 and ongoing planning, implementation, and training for the deployment
29 of communications equipment for relevant State, local, and tribal gov-
30 ernments and emergency response providers in the event of a cata-
31 strophic loss of local and regional emergency communications services;

32 (10) assist the President, the National Security Council, the Home-
33 land Security Council, and the Director of the Office of Management
34 and Budget in ensuring the continued operation of the telecommuni-
35 cations functions and responsibilities of the Federal Government, ex-
36 cluding spectrum management;

37 (11) establish, in coordination with the Director of the Office for
38 Interoperability and Compatibility, requirements for interoperable
39 emergency communications capabilities, which shall be nonproprietary
40 where standards for the capabilities exist, for all public safety radio
41 and data communications systems and equipment purchased using

1 homeland security assistance administered by the Department, exclud-
2 ing any alert and warning device, technology, or system;

3 (12) review, in consultation with the Assistant Secretary for Grants
4 and Training, all interoperable emergency communications plans of
5 Federal, State, local, and tribal governments, including Statewide and
6 tactical interoperability plans, developed pursuant to homeland security
7 assistance administered by the Department, but excluding spectrum al-
8 location and management related to the plans;

9 (13) develop and update periodically, as appropriate, a National
10 Emergency Communications Plan under section 12103 of this title;

11 (14) perform other duties of the Department necessary to support
12 and promote the ability of emergency response providers and relevant
13 government officials to continue to communicate in the event of natural
14 disasters, acts of terrorism, and other man-made disasters; and

15 (15) perform other duties of the Department necessary to achieve
16 the goal of, and maintain and enhance, interoperable emergency com-
17 munications capabilities.

18 (b) PERFORMANCE OF PREVIOUSLY TRANSFERRED FUNCTIONS.—The
19 Secretary shall administer through the Director for Emergency Communica-
20 tions the following programs and responsibilities:

21 (1) The SAFECOM Program, excluding elements related to re-
22 search, development, testing, and evaluation and standards.

23 (2) The responsibilities of the Chief Information Officer related to
24 the implementation of the Integrated Wireless Network.

25 (3) The Interoperable Communications Technical Assistance Pro-
26 gram.

27 (c) COORDINATION.—The Director for Emergency Communications shall
28 coordinate—

29 (1) as appropriate, with the Director of the Office for Interoper-
30 ability and Compatibility with respect to the responsibilities described
31 in section 10713 of this title; and

32 (2) with the Administrator of the Federal Emergency Management
33 Agency with respect to the responsibilities described in this chapter.

34 **§ 12103. National Emergency Communications Plan**

35 (a) IN GENERAL.—The Secretary, acting through the Director for Emer-
36 gency Communications, and in cooperation with the National Communica-
37 tions System Office of the Department (as appropriate), shall, in coopera-
38 tion with State, local, and tribal governments, Federal departments and
39 agencies, emergency response providers, and the private sector, develop, and
40 periodically update, a National Emergency Communications Plan to provide
41 recommendations regarding how the United States should—

1 (1) support and promote the ability of emergency response providers
2 and relevant government officials to continue to communicate in the
3 event of natural disasters, acts of terrorism, and other man-made dis-
4 asters; and

5 (2) ensure, accelerate, and attain interoperable emergency commu-
6 nications nationwide.

7 (b) COORDINATION.—The Emergency Communications Preparedness
8 Center under section 12107 of this title shall coordinate the development
9 of the Federal aspects of the National Emergency Communications Plan.

10 (c) CONTENTS.—The National Emergency Communications Plan shall—

11 (1) include recommendations developed in consultation with the Fed-
12 eral Communications Commission and the National Institute of Stand-
13 ards and Technology for a process for expediting national voluntary
14 consensus standards for emergency communications equipment for the
15 purchase and use by public safety agencies of interoperable emergency
16 communications equipment and technologies;

17 (2) identify the appropriate capabilities necessary for emergency re-
18 sponse providers and relevant government officials to continue to com-
19 municate in the event of natural disasters, acts of terrorism, and other
20 man-made disasters;

21 (3) identify the appropriate interoperable emergency communications
22 capabilities necessary for Federal, State, local, and tribal governments
23 in the event of natural disasters, acts of terrorism, and other man-
24 made disasters;

25 (4) recommend both short-term and long-term solutions for ensuring
26 that emergency response providers and relevant government officials
27 can continue to communicate in the event of natural disasters, acts of
28 terrorism, and other man-made disasters;

29 (5) recommend both short-term and long-term solutions for deploy-
30 ing interoperable emergency communications systems for Federal,
31 State, local, and tribal governments throughout the Nation, including
32 through the provision of existing and emerging technologies;

33 (6) identify how Federal departments and agencies that respond to
34 natural disasters, acts of terrorism, and other man-made disasters can
35 work effectively with State, local, and tribal governments, in all States,
36 and with other entities;

37 (7) identify obstacles to deploying interoperable emergency commu-
38 nications capabilities nationwide and recommend short-term and long-
39 term measures to overcome those obstacles, including recommendations
40 for multijurisdictional coordination among Federal, State, local, and
41 tribal governments;

1 (8) recommend goals and timeframes for the deployment of emer-
2 gency, command-level communications systems based on new and exist-
3 ing equipment across the United States and develop a timetable for the
4 deployment of interoperable emergency communications systems nation-
5 wide;

6 (9) recommend appropriate measures that emergency response pro-
7 viders should employ to ensure the continued operation of relevant gov-
8 ernmental communications infrastructure in the event of natural disas-
9 ters, acts of terrorism, or other man-made disasters; and

10 (10) set a date, including interim benchmarks, as appropriate, by
11 which State, local, and tribal governments, Federal departments and
12 agencies, and emergency response providers expect to achieve a baseline
13 level of national interoperable communications, as that term is defined
14 under section 10712(a) of this title.

15 **§ 12104. Assessments and reports**

16 (a) BASELINE ASSESSMENT.—The Secretary, acting through the Director
17 for Emergency Communications, shall conduct an assessment of Federal,
18 State, local, and tribal governments every 5 years, that—

19 (1) defines the range of capabilities needed by emergency response
20 providers and relevant government officials to continue to communicate
21 in the event of natural disasters, acts of terrorism, and other man-
22 made disasters;

23 (2) defines the range of interoperable emergency communications ca-
24 pabilities needed for specific events;

25 (3) assesses the currently available capabilities to meet the commu-
26 nications needs;

27 (4) identifies the gap between current capabilities and defined re-
28 quirements; and

29 (5) includes a national interoperable emergency communications in-
30 ventory to be completed by the Secretary, the Secretary of Commerce,
31 and the Chairman of the Federal Communications Commission that—

32 (A) identifies for each Federal department and agency—

33 (i) the channels and frequencies used;

34 (ii) the nomenclature used to refer to each channel or fre-
35 quency used; and

36 (iii) the types of communications systems and equipment
37 used; and

38 (B) identifies the interoperable emergency communications sys-
39 tems in use by public safety agencies in the United States.

1 (b) CLASSIFIED ANNEX.—The baseline assessment under this section
2 may include a classified annex, including information provided under sub-
3 section (a)(5)(A).

4 (c) SAVINGS CLAUSE.—In conducting the baseline assessment under this
5 section, the Secretary may incorporate findings from assessments conducted
6 before, or ongoing on, October 4, 2006.

7 (d) PROGRESS REPORTS.—The Secretary, acting through the Director for
8 Emergency Communications, shall submit to Congress every 2 years a re-
9 port on the progress of the Department in achieving the goals of, and carry-
10 rying out its responsibilities under, this chapter, including—

11 (1) a description of the findings of the most recent baseline assess-
12 ment conducted under subsection (a);

13 (2) a determination of the degree to which interoperable emergency
14 communications capabilities have been attained to date and the gaps
15 that remain for interoperability to be achieved;

16 (3) an evaluation of the ability to continue to communicate and to
17 provide and maintain interoperable emergency communications by
18 emergency managers, emergency response providers, and relevant gov-
19 ernment officials in the event of—

20 (A) natural disasters, acts of terrorism, or other man-made dis-
21 asters, including Incidents of National Significance declared by the
22 Secretary under the National Response Plan; and

23 (B) a catastrophic loss of local and regional communications
24 services;

25 (4) a list of best practices relating to the ability to continue to com-
26 municate and to provide and maintain interoperable emergency commu-
27 nications in the event of natural disasters, acts of terrorism, or other
28 man-made disasters; and

29 (5) an evaluation of the feasibility and desirability of the Department
30 developing, on its own or in conjunction with the Department of De-
31 fense, a mobile communications capability, modeled on the Army Signal
32 Corps, that could be deployed to support emergency communications at
33 the site of natural disasters, acts of terrorism, or other man-made dis-
34 asters.

35 **§ 12105. Coordination of Department emergency commu-**
36 **nications grant programs**

37 (a) COORDINATION OF GRANTS AND STANDARDS PROGRAMS.—The Sec-
38 retary, acting through the Director for Emergency Communications, shall
39 ensure that grant guidelines for the use of homeland security assistance ad-
40 ministered by the Department relating to interoperable emergency commu-
41 nications are coordinated and consistent with the goals and recommenda-

1 tions in the National Emergency Communications Plan under section 12103
2 of this title.

3 (b) DENIAL OF ELIGIBILITY FOR GRANTS.—

4 (1) IN GENERAL.—The Secretary, acting through the Assistant Sec-
5 retary for Grants and Planning, and in consultation with the Director
6 for Emergency Communications, may prohibit any State, local, or trib-
7 al government from using homeland security assistance administered by
8 the Department to achieve, maintain, or enhance emergency commu-
9 nications capabilities, if—

10 (A) the government has not complied with the requirement to
11 submit a Statewide Interoperable Communications Plan as re-
12 quired by section 10712(e) of this title;

13 (B) the government has proposed to upgrade or purchase new
14 equipment or systems that do not meet or exceed any applicable
15 national voluntary consensus standards and has not provided a
16 reasonable explanation of why the equipment or systems will serve
17 the needs of the applicant better than equipment or systems that
18 meet or exceed the standards; and

19 (C) as of the date that is 3 years after the date of the comple-
20 tion of the initial National Emergency Communications Plan
21 under section 12103 of this title, national voluntary consensus
22 standards for interoperable emergency communications capabilities
23 have not been developed and promulgated.

24 (2) STANDARDS.—The Secretary, in coordination with the Federal
25 Communications Commission, the National Institute of Standards and
26 Technology, and other Federal departments and agencies responsible
27 for standards, shall support the development, promulgation, and updat-
28 ing as necessary of national voluntary consensus standards for inter-
29 operable emergency communications.

30 **§ 12106. Regional Emergency Communications Coordination**

31 (a) IN GENERAL.—There is in each Regional Office a Regional Emer-
32 gency Communications Coordination Working Group (in this section re-
33 ferred to as an “RECC Working Group”). Each RECC Working Group
34 shall report to the relevant Regional Administrator and coordinate its activi-
35 ties with the relevant Regional Advisory Council.

36 (b) MEMBERSHIP.—Each RECC Working Group consists of the following:

37 (1) Organizations representing the interests of the following:

38 (A) State officials.

39 (B) Local government officials, including sheriffs.

40 (C) State police departments.

41 (D) Local police departments.

- 1 (E) Local fire departments.
2 (F) Public safety answering points (9-1-1 services).
3 (G) State emergency managers, homeland security directors, or
4 representatives of State Administrative Agencies.
5 (H) Local emergency managers or homeland security directors.
6 (I) Other emergency response providers as appropriate.
7 (2) Representatives from the Department, the Federal Communica-
8 tions Commission, and other Federal departments and agencies with
9 responsibility for coordinating interoperable emergency communications
10 with, or providing emergency support services to, State, local, and trib-
11 al governments.
- 12 (c) COORDINATION.—Each RECC Working Group shall coordinate its ac-
13 tivities with the following:
- 14 (1) Communications equipment manufacturers and vendors (includ-
15 ing broadband data service providers).
16 (2) Local exchange carriers.
17 (3) Local broadcast media.
18 (4) Wireless carriers.
19 (5) Satellite communications services.
20 (6) Cable operators.
21 (7) Hospitals.
22 (8) Public utility services.
23 (9) Emergency evacuation transit services.
24 (10) Ambulance services.
25 (11) HAM and amateur radio operators.
26 (12) Representatives from other private-sector entities and non-
27 governmental organizations as the Regional Administrator determines
28 appropriate.
- 29 (d) DUTIES.—The duties of each RECC Working Group include—
- 30 (1) assessing the survivability, sustainability, and interoperability of
31 local emergency communications systems to meet the goals of the Na-
32 tional Emergency Communications Plan;
- 33 (2) reporting annually to the relevant Regional Administrator, the
34 Director for Emergency Communications, the Chairman of the Federal
35 Communications Commission, and the Assistant Secretary for Commu-
36 nications and Information of the Department of Commerce on the sta-
37 tus of its region in building robust and sustainable interoperable voice
38 and data emergency communications networks and, not later than 60
39 days after the completion of the initial National Emergency Commu-
40 nications Plan under section 12103 of this title, on the progress of the
41 region in meeting the goals of the plan;

1 (3) ensuring a process for the coordination of effective multijuris-
2 dictional, multi-agency emergency communications networks for use
3 during natural disasters, acts of terrorism, and other man-made disas-
4 ters through the expanded use of emergency management and public
5 safety communications mutual aid agreements; and

6 (4) coordinating the establishment of Federal, State, local, and tribal
7 support services and networks designed to address the immediate and
8 critical human needs in responding to natural disasters, acts of ter-
9 rorism, and other man-made disasters.

10 **§ 12107. Emergency Communications Preparedness Center**

11 (a) ESTABLISHMENT.—There is the Emergency Communications Pre-
12 paredness Center.

13 (b) OPERATION.—The Secretary, the Chairman of the Federal Commu-
14 nications Commission, the Secretary of Defense, the Secretary of Commerce,
15 the Attorney General, and the heads of other Federal departments and
16 agencies or their designees shall jointly operate the Emergency Communica-
17 tions Preparedness Center in accordance with the Memorandum of Under-
18 standing entitled, “Emergency Communications Preparedness Center
19 (ECPC) Charter”.

20 (c) FUNCTIONS.—The Emergency Communications Preparedness Center
21 shall—

22 (1) serve as the focal point for interagency efforts and as a clearing-
23 house with respect to all relevant intergovernmental information to sup-
24 port and promote (including specifically by working to avoid duplica-
25 tion, hindrances, and counteractive efforts among the participating
26 Federal departments and agencies)—

27 (A) the ability of emergency response providers and relevant
28 government officials to continue to communicate in the event of
29 natural disasters, acts of terrorism, and other man-made disasters;
30 and

31 (B) interoperable emergency communications;

32 (2) prepare and submit to Congress annually a strategic assessment
33 regarding the coordination efforts of Federal departments and agencies
34 to advance—

35 (A) the ability of emergency response providers and relevant
36 government officials to continue to communicate in the event of
37 natural disasters, acts of terrorism, and other man-made disasters;
38 and

39 (B) interoperable emergency communications;

1 (3) consider, in preparing the strategic assessment under paragraph
2 (2), the goals stated in the National Emergency Communications Plan
3 under section 12103 of this title; and

4 (4) perform other functions provided in the ECPC Charter described
5 in subsection (b).

6 **§ 12108. Urban and other high risk area communications ca-**
7 **pabilities**

8 (a) IN GENERAL.—The Secretary, in consultation with the Chairman of
9 the Federal Communications Commission and the Secretary of Defense, and
10 with appropriate State, local, and tribal government officials, shall provide
11 technical guidance, training, and other assistance, as appropriate, to sup-
12 port the rapid establishment of consistent, secure, and effective interoper-
13 able emergency communications capabilities in the event of an emergency
14 in urban and other areas determined by the Secretary to be at consistently
15 high levels of risk from natural disasters, acts of terrorism, and other man-
16 made disasters.

17 (b) MINIMUM CAPABILITIES.—The interoperable emergency communica-
18 tions capabilities established under subsection (a) shall ensure the ability of
19 all levels of government, emergency response providers, the private sector,
20 and other organizations with emergency response capabilities—

21 (1) to communicate with each other in the event of an emergency;

22 (2) to have appropriate and timely access to the information sharing
23 environment described in section 11708 of this title; and

24 (3) to be consistent with any applicable State or Urban Area home-
25 land strategy or plan.

26 **§ 12109. Interoperable Emergency Communications Grant**
27 **Program**

28 (a) ESTABLISHMENT.—The Secretary shall establish the Interoperable
29 Emergency Communications Grant Program to make grants to States to
30 carry out initiatives to improve local, tribal, statewide, regional, national
31 and, where appropriate, international interoperable emergency communica-
32 tions, including communications in collective response to natural disasters,
33 acts of terrorism, and other man-made disasters.

34 (b) POLICY.—The Director for Emergency Communications shall ensure
35 that a grant awarded to a State under this section is consistent with the
36 policies established pursuant to the responsibilities and authorities of the
37 Office of Emergency Communications under this chapter, including ensuring
38 that activities funded by the grant—

39 (1) comply with the statewide plan for that State required by section
40 10712(e) of this title; and

1 (2) comply with the National Emergency Communications Plan
2 under section 12103 of this title, when completed.

3 (c) ADMINISTRATION.—

4 (1) IN GENERAL.—The Administrator of the Federal Emergency
5 Management Agency shall administer the Interoperable Emergency
6 Communications Grant Program pursuant to the responsibilities and
7 authorities of the Administrator under chapter 111 of this title.

8 (2) GUIDANCE.—In administering the grant program, the Adminis-
9 trator shall ensure that the use of grants is consistent with guidance
10 established by the Director of Emergency Communications under sec-
11 tion 10712(b)(1)(H) of this title.

12 (d) USE OF FUNDS.—A State that receives a grant under this section
13 shall use the grant to implement that State’s Statewide Interoperable Com-
14 munications Plan required under section 10712(e) of this title and approved
15 under subsection (e) of this section, and to assist with activities determined
16 by the Secretary to be integral to interoperable emergency communications.

17 (e) APPROVAL OF PLANS.—

18 (1) APPROVAL AS CONDITION OF GRANT.—Before a State may re-
19 ceive a grant under this section, the Director of Emergency Commu-
20 nications shall approve the State’s Statewide Interoperable Communica-
21 tions Plan required under section 10712(e) of this title.

22 (2) PLAN REQUIREMENTS.—In approving a plan under this sub-
23 section, the Director of Emergency Communications shall ensure that
24 the plan—

25 (A) is designed to improve interoperability at the city, county,
26 regional, State, and interstate level;

27 (B) considers any applicable local or regional plan; and

28 (C) complies, to the maximum extent practicable, with the Na-
29 tional Emergency Communications Plan under section 12103 of
30 this title.

31 (3) APPROVAL OF REVISIONS.—The Director of Emergency Commu-
32 nications may approve revisions to a State’s plan if the Director deter-
33 mines that doing so is likely to further interoperability.

34 (f) LIMITATIONS ON USES OF FUNDS.—

35 (1) IN GENERAL.—The recipient of a grant under this section may
36 not use the grant—

37 (A) to supplant State or local funds;

38 (B) for any State or local government cost-sharing contribution;

39 or

40 (C) for recreational or social purposes.

1 (2) PENALTIES.—In addition to other remedies currently available,
2 the Secretary may take necessary actions to ensure that recipients of
3 grant funds are using the funds for the purpose for which they were
4 intended.

5 (g) LIMITATIONS ON AWARD OF GRANTS.—

6 (1) NATIONAL EMERGENCY COMMUNICATIONS PLAN REQUIRED.—
7 The Secretary may not award a grant under this section before the
8 date on which the Secretary completes and submits to Congress the
9 National Emergency Communications Plan required under section
10 12103 of this title.

11 (2) VOLUNTARY CONSENSUS STANDARDS.—The Secretary may not
12 award a grant to a State under this section for the purchase of equip-
13 ment that does not meet applicable voluntary consensus standards, un-
14 less the State demonstrates that there are compelling reasons for the
15 purchase.

16 (h) AWARD OF GRANTS.—In approving applications and awarding grants
17 under this section, the Secretary shall consider—

18 (1) the risk posed to each State by natural disasters, acts of ter-
19 rorism, or other man-made disasters, including—

20 (A) the likely need of a jurisdiction within the State to respond
21 to the risk in nearby jurisdictions;

22 (B) the degree of threat, vulnerability, and consequences related
23 to critical infrastructure (from all critical infrastructure sectors)
24 or key resources identified by the Administrator or the State
25 homeland security and emergency management plans, including
26 threats to, vulnerabilities of, and consequences from damage to
27 critical infrastructure and key resources in nearby jurisdictions;

28 (C) the size of the population and density of the population of
29 the State, including appropriate consideration of military, tourist,
30 and commuter populations;

31 (D) whether the State is on or near an international border;

32 (E) whether the State encompasses an economically significant
33 border crossing; and

34 (F) whether the State has a coastline bordering an ocean, a
35 major waterway used for interstate commerce, or international
36 waters; and

37 (2) the anticipated effectiveness of the State's proposed use of grant
38 funds to improve interoperability.

39 (i) OPPORTUNITY TO AMEND APPLICATIONS.—In considering applications
40 for grants under this section, the Administrator shall provide applicants

1 with a reasonable opportunity to correct defects in the application, if any,
2 before making final awards.

3 (j) MINIMUM GRANT AMOUNTS.—

4 (1) STATES.—In awarding grants under this section, the Secretary
5 shall ensure that for each fiscal year, except as provided in paragraph
6 (2), no State receives a grant in an amount that is less than 0.35 per-
7 cent of the total amount appropriated for grants under this section for
8 that fiscal year.

9 (2) TERRITORIES.—In awarding grants under this section, the Sec-
10 retary shall ensure that for each fiscal year, American Samoa, the
11 Northern Mariana Islands, Guam, and the Virgin Islands each receive
12 grants in amounts that are not less than 0.08 percent of the total
13 amount appropriated for grants under this section for that fiscal year.

14 (k) CERTIFICATION.—Each State that receives a grant under this section
15 shall certify that the grant is used for the purpose for which the funds were
16 intended and in compliance with the State's approved Statewide Interoper-
17 able Communications Plan.

18 (l) STATE RESPONSIBILITIES.—

19 (1) AVAILABILITY OF FUNDS TO LOCAL AND TRIBAL GOVERN-
20 MENTS.—Not later than 45 days after receiving grant funds, a State
21 that receives a grant under this section shall obligate or otherwise
22 make available to local and tribal governments—

23 (A) not less than 80 percent of the grant funds;

24 (B) with the consent of local and tribal governments, eligible ex-
25 penditures having a value of not less than 80 percent of the
26 amount of the grant; or

27 (C) grant funds combined with other eligible expenditures hav-
28 ing a total value of not less than 80 percent of the amount of the
29 grant.

30 (2) ALLOCATION OF FUNDS.—A State that receives a grant under
31 this section shall allocate grant funds to tribal governments in the
32 State to assist tribal communities in improving interoperable commu-
33 nications, in a manner consistent with the Statewide Interoperable
34 Communications Plan. A State may not impose unreasonable or unduly
35 burdensome requirements on a tribal government as a condition of pro-
36 viding grant funds or resources to the tribal government.

37 (3) PENALTIES.—If a State violates the requirements of this sub-
38 section, in addition to other remedies available to the Secretary, the
39 Secretary may terminate or reduce the amount of the grant awarded
40 to that State or transfer grant funds previously awarded to the State
41 directly to the appropriate local or tribal government.

1 (m) REPORTS.—

2 (1) ANNUAL REPORTS BY STATE GRANT RECIPIENTS.—A State that
3 receives a grant under this section shall annually submit to the Direc-
4 tor of Emergency Communications a report on the progress of the
5 State in implementing that State’s Statewide Interoperable Commu-
6 nications Plan required under section 10712(e) of this title and achiev-
7 ing interoperability at the city, county, regional, State, and interstate
8 levels. The Director shall make the reports publicly available, including
9 by making them available on the Internet website of the Office of
10 Emergency Communications, subject to any redactions that the Direc-
11 tor determines are necessary to protect classified or other sensitive in-
12 formation.

13 (2) ANNUAL REPORTS TO CONGRESS.—At least once each year, the
14 Director of Emergency Communications shall submit to Congress a re-
15 port on the use of grants awarded under this section and any progress
16 in implementing Statewide Interoperable Communications Plans and
17 improving interoperability at the city, county, regional, State, and
18 interstate level, as a result of the award of the grants.

19 (n) RULE OF CONSTRUCTION.—Nothing in this section shall be construed
20 or interpreted to preclude a State from using a grant awarded under this
21 section for interim or long-term Internet Protocol-based interoperable solu-
22 tions.

23 (o) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be
24 appropriated for grants under this section such sums as may be necessary.

25 **Chapter 123—Domestic Nuclear Detection**
26 **Office**

Sec.

12301. Mission.

12302. Technology research and development investment strategy for nuclear and radiological
detection.

12303. Testing authority.

12304. Personnel.

12305. Relationship to other Department entities and Federal agencies.

12306. Contracting and grant making authorities.

12307. Joint annual interagency review of global nuclear detection architecture.

27 **§ 12301. Mission**

28 (a) DEFINITIONS.—In this section:

29 (1) ALASKA NATIVE-SERVING INSTITUTION.—The term “Alaska Na-
30 tive-serving institution” has the meaning given the term in section 317
31 of the Higher Education Act of 1965 (20 U.S.C. 1059d).

32 (2) ASIAN AMERICAN AND NATIVE AMERICAN PACIFIC ISLANDER-
33 SERVING INSTITUTION.—The term “Asian American and Native Amer-
34 ican Pacific Islander-serving institution” has the meaning given the

1 term in section 320 of the Higher Education Act of 1965 (20 U.S.C.
2 1059g).

3 (3) HISPANIC-SERVING INSTITUTION.—The term “Hispanic-serving
4 institution” has the meaning given the term in section 502 of the
5 Higher Education Act of 1965 (20 U.S.C. 1101a).

6 (4) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term
7 “historically Black college or university” has the meaning given the
8 term “part B institution” in section 322(2) of the Higher Education
9 Act of 1965 (20 U.S.C. 1061(2)).

10 (5) NATIVE HAWAIIAN-SERVING INSTITUTION.—The term “Native
11 Hawaiian-serving institution” has the meaning given the term in sec-
12 tion 317 of the Higher Education Act of 1965 (20 U.S.C. 1059d).

13 (6) TRIBAL COLLEGE OR UNIVERSITY.—The term “Tribal College or
14 University” has the meaning given the term in section 316(b) of the
15 Higher Education Act of 1965 (20 U.S.C. 1059c(b)).

16 (b) MISSION.—The Domestic Nuclear Detection Office is responsible for
17 coordinating Federal efforts to detect and protect against the unauthorized
18 importation, possession, storage, transportation, development, or use of a
19 nuclear explosive device, fissile material, or radiological material in the
20 United States, and to protect against attack using such devices or materials
21 against the people, territory, or interests of the United States and, to this
22 end, shall—

23 (1) serve as the primary entity of the United States Government to
24 further develop, acquire, and support the deployment of an enhanced
25 domestic system to detect and report on attempts to import, possess,
26 store, transport, develop, or use an unauthorized nuclear explosive de-
27 vice, fissile material, or radiological material in the United States, and
28 improve that system over time;

29 (2) enhance and coordinate the nuclear detection efforts of Federal,
30 State, local, and tribal governments and the private sector to ensure
31 a managed, coordinated response;

32 (3) establish, with the approval of the Secretary and in coordination
33 with the Attorney General, the Secretary of Defense, and the Secretary
34 of Energy, additional protocols and procedures for use within the
35 United States to ensure that the detection of unauthorized nuclear ex-
36 plosive devices, fissile material, or radiological material is promptly re-
37 ported to the Attorney General, the Secretary, the Secretary of De-
38 fense, the Secretary of Energy, and other appropriate officials or their
39 respective designees for appropriate action by law enforcement, mili-
40 tary, emergency response, or other authorities;

1 (4) develop, with the approval of the Secretary and in coordination
2 with the Attorney General, the Secretary of State, the Secretary of De-
3 fense, and the Secretary of Energy, an enhanced global nuclear detec-
4 tion architecture with implementation under which—

5 (A) the Domestic Nuclear Detection Office will be responsible
6 for the implementation of the domestic portion of the global archi-
7 tecture;

8 (B) the Secretary of Defense will retain responsibility for imple-
9 mentation of Department of Defense requirements within and out-
10 side the United States; and

11 (C) the Secretary of State, the Secretary of Defense, and the
12 Secretary of Energy will maintain their respective responsibilities
13 for policy guidance and implementation of the portion of the global
14 architecture outside the United States, which will be implemented
15 consistent with applicable law and relevant international arrange-
16 ments;

17 (5) ensure that the expertise necessary to accurately interpret detec-
18 tion data is made available in a timely manner for all technology de-
19 ployed by the Domestic Nuclear Detection Office to implement the
20 global nuclear detection architecture;

21 (6) conduct, support, coordinate, and encourage an aggressive, exp-
22 dited, evolutionary, and transformational program of research and de-
23 velopment to generate and improve technologies to detect and prevent
24 the illicit entry, transport, assembly, or potential use within the United
25 States of a nuclear explosive device or fissile or radiological material,
26 and coordinate with the Under Secretary for Science and Technology
27 on basic and advanced or transformational research and development
28 efforts relevant to the mission of both organizations;

29 (7) carry out a program to test and evaluate technology for detecting
30 a nuclear explosive device and fissile or radiological material, in coordi-
31 nation with the Secretary of Defense and the Secretary of Energy, as
32 appropriate, and establish performance metrics for evaluating the effec-
33 tiveness of individual detectors and detection systems in detecting such
34 devices or material—

35 (A) under realistic operational and environmental conditions;
36 and

37 (B) against realistic adversary tactics and countermeasures;

38 (8) support and enhance the effective sharing and use of appropriate
39 information generated by the intelligence community, law enforcement
40 agencies, counterterrorism community, other government agencies, and

1 foreign governments, as well as provide appropriate information to the
2 entities;

3 (9) further enhance and maintain continuous awareness by analyzing
4 information from all Domestic Nuclear Detection Office mission-related
5 detection systems;

6 (10) lead the development and implementation of the national stra-
7 tegic five-year plan for improving the nuclear forensic and attribution
8 capabilities of the United States required under section 1036 of the
9 National Defense Authorization Act for Fiscal Year 2010 (Public Law
10 111–84, 123 Stat. 2450);

11 (11) establish in the Domestic Nuclear Detection Office the National
12 Technical Nuclear Forensics Center to provide centralized stewardship,
13 planning, assessment, gap analysis, exercises, improvement, and inte-
14 gration for all Federal nuclear forensics and attribution activities—

15 (A) to ensure an enduring national technical nuclear forensics
16 capability to strengthen the collective response of the United
17 States to nuclear terrorism or other nuclear attacks; and

18 (B) to coordinate and implement the national strategic five-year
19 plan referred to in paragraph (10);

20 (12) establish a National Nuclear Forensics Expertise Development
21 Program, which—

22 (A) is devoted to developing and maintaining a vibrant and en-
23 during academic pathway from undergraduate to post-doctorate
24 study in nuclear and geochemical science specialties directly rel-
25 evant to technical nuclear forensics, including radiochemistry, geo-
26 chemistry, nuclear physics, nuclear engineering, materials science,
27 and analytical chemistry;

28 (B) shall—

29 (i) make available for undergraduate study, student schol-
30 arships, with a duration of up to 4 years per student, that
31 shall include, if possible, at least one summer internship at
32 a national laboratory or appropriate Federal agency in the
33 field of technical nuclear forensics during the course of the
34 student’s undergraduate career;

35 (ii) make available for doctoral study, student fellowships,
36 with a duration of up to 5 years per student, which shall—

37 (I) include, if possible, at least two summer intern-
38 ships at a national laboratory or appropriate Federal
39 agency in the field of technical nuclear forensics during
40 the course of the student’s graduate career; and

1 (II) require each recipient to commit to serve for 2
2 years in a post-doctoral position in a technical nuclear
3 forensics-related specialty at a national laboratory or ap-
4 propriate Federal agency after graduation;

5 (iii) make available to faculty, awards, with a duration of
6 3 to 5 years each, to ensure faculty and their graduate stu-
7 dents have a sustained funding stream; and

8 (iv) place a particular emphasis on reinvigorating technical
9 nuclear forensics programs while encouraging the participa-
10 tion of undergraduate students, graduate students, and uni-
11 versity faculty from historically Black colleges and univer-
12 sities, Hispanic-serving institutions, Tribal Colleges and Uni-
13 versities, Asian American and Native American Pacific Is-
14 lander-serving institutions, Alaska Native-serving institutions,
15 and Native Hawaiian-serving institutions; and

16 (C) shall—

17 (i) provide for the selection of individuals to receive schol-
18 arships or fellowships under this section through a competi-
19 tive process primarily on the basis of academic merit and the
20 nuclear forensics and attribution needs of the United States
21 Government;

22 (ii) provide for the setting aside of up to 10 percent of the
23 scholarships or fellowships awarded under this section for in-
24 dividuals who are Federal employees to enhance the education
25 of the employees in areas of critical nuclear forensics and at-
26 tribution needs of the United States Government, for doctoral
27 education under the scholarship on a full-time or part-time
28 basis;

29 (iii) provide that the Secretary may enter into a contrac-
30 tual agreement with an institution of higher education under
31 which the amounts provided for a scholarship under this sec-
32 tion for tuition, fees, and other authorized expenses are paid
33 directly to the institution with respect to which the scholar-
34 ship is awarded;

35 (iv) require scholarship recipients to maintain satisfactory
36 academic progress; and

37 (v) require that—

38 (I) a scholarship recipient who fails to maintain a high
39 level of academic standing, as defined by the Secretary,
40 who is dismissed for disciplinary reasons from the edu-
41 cational institution the recipient is attending, or who vol-

1 untarily terminates academic training before graduation
2 from the educational program for which the scholarship
3 was awarded is liable to the United States for repayment
4 within 1 year after the date of default of all scholarship
5 funds paid to the recipient and to the institution of high-
6 er education on the behalf of the recipient, provided that
7 the repayment period may be extended by the Secretary
8 if the Secretary determines it necessary, as established
9 by regulation; and

10 (II) a scholarship recipient who, for any reason except
11 death or disability, fails to begin or complete the post-
12 doctoral service requirements in a technical nuclear
13 forensics-related specialty at a national laboratory or ap-
14 propriate Federal agency after completion of academic
15 training is liable to the United States for an amount
16 equal to—

17 (aa) the total amount of the scholarship received
18 by the recipient under this section; and

19 (bb) the interest on the amounts which would be
20 payable if at the time the scholarship was received
21 the scholarship was a loan bearing interest at the
22 maximum legally prevailing rate;

23 (13) provide an annual report to Congress on the activities carried
24 out under paragraphs (10), (11), and (12); and

25 (14) perform other duties assigned by the Secretary.

26 **§ 12302. Technology research and development investment**
27 **strategy for nuclear and radiological detection**

28 (a) IN GENERAL.—The Secretary, the Secretary of Energy, the Secretary
29 of Defense, and the Director of National Intelligence shall submit to Con-
30 gress a research and development investment strategy for nuclear and radio-
31 logical detection.

32 (b) CONTENTS.—The strategy under subsection (a) shall include—

33 (1) a long term technology roadmap for nuclear and radiological de-
34 tection applicable to the mission needs of the Department, the Depart-
35 ment of Energy, the Department of Defense, and the Office of the Di-
36 rector of National Intelligence;

37 (2) budget requirements necessary to meet the roadmap; and

38 (3) documentation of how the Department, the Department of En-
39 ergy, the Department of Defense, and the Office of the Director of Na-
40 tional Intelligence will execute this strategy.

1 (c) ANNUAL REPORT.—The Director for Domestic Nuclear Detection and
2 the Under Secretary for Science and Technology jointly and annually shall
3 notify Congress that the strategy and technology road map for nuclear and
4 radiological detection developed under subsections (a) and (b) is consistent
5 with the national policy and strategic plan for identifying priorities, goals,
6 objectives, and policies for coordinating the Federal Government’s civilian
7 efforts to identify and develop countermeasures to terrorist threats from
8 weapons of mass destruction that are required under section 10701(2) of
9 this title.

10 **§ 12303. Testing authority**

11 (a) IN GENERAL.—The Secretary, acting through the Director for Do-
12 mestic Nuclear Detection, shall coordinate with the responsible Federal
13 agency or other entity to facilitate the use by the Domestic Nuclear Detec-
14 tion Office, by its contractors, or by other persons or entities, of existing
15 Government laboratories, centers, ranges, or other testing facilities for the
16 testing of materials, equipment, models, computer software, and other items
17 as may be related to the missions identified in section 12301 of this title.
18 Use of Government facilities shall be carried out in accordance with all ap-
19 plicable laws, regulations, and contractual provisions, including those gov-
20 erning security, safety, and environmental protection, including, when appli-
21 cable, the provisions of section 10708 of this title. The Domestic Nuclear
22 Detection Office may direct that private-sector entities utilizing Government
23 facilities under this section pay an appropriate fee to the agency that owns
24 or operates those facilities to defray additional costs to the Government re-
25 sulting from private-sector use.

26 (b) CONFIDENTIALITY OF TEST RESULTS.—The results of tests per-
27 formed with services made available shall be confidential and shall not be
28 disclosed outside the Federal Government without the consent of the per-
29 sons for whom the tests are performed.

30 (c) FEES.—Fees for services made available under this section shall not
31 exceed the amount necessary to recoup the direct and indirect costs in-
32 volved, such as direct costs of utilities, contractor support, and salaries of
33 personnel that are incurred by the United States to provide for the testing.

34 (d) USE OF FEES.—Fees received for services made available under this
35 section may be credited to the appropriation from which funds were ex-
36 pended to provide the services.

37 **§ 12304. Personnel**

38 (a) HIRING.—In hiring personnel for the Domestic Nuclear Detection Of-
39 fice, the Secretary has the hiring and management authorities provided in
40 section 1101 of the Strom Thurmond National Defense Authorization Act
41 for Fiscal Year 1999 (Public Law 105–261, 5 U.S.C. 3104 note). The term

1 of appointments for employees under subsection (c)(1) of that section may
2 not exceed 5 years before granting any extension under subsection (c)(2)
3 of that section.

4 (b) **DETAIL.**—The Secretary may request that the Secretary of Defense,
5 the Secretary of Energy, the Secretary of State, the Attorney General, the
6 Nuclear Regulatory Commission, and the directors of other Federal agen-
7 cies, including elements of the Intelligence Community, provide for the reim-
8 bursable detail of personnel with relevant expertise to the Domestic Nuclear
9 Detection Office.

10 **§ 12305. Relationship to other Department entities and Fed-**
11 **eral agencies**

12 The authority of the Secretary exercised by the Director for Domestic
13 Nuclear Detection under this chapter shall not affect the authorities or re-
14 sponsibilities of any officer of the Department or of any officer of any other
15 department or agency of the United States with respect to the command,
16 control, or direction of the functions, personnel, funds, assets, and liabilities
17 of any entity in the Department or of any Federal department or agency.

18 **§ 12306. Contracting and grant making authorities**

19 The Secretary, acting through the Director for Domestic Nuclear Detec-
20 tion, in carrying out the responsibilities under paragraphs (6) and (7) of
21 subsection (b) of section 12301 of this title shall—

22 (1) operate extramural and intramural programs and distribute
23 funds through grants, cooperative agreements, and other transactions
24 and contracts;

25 (2) ensure that activities under paragraphs (6) and (7) of subsection
26 (b) of section 12301 of this title include investigations of radiation de-
27 tection equipment in configurations suitable for deployment at seaports,
28 which may include underwater or water surface detection equipment
29 and detection equipment that can be mounted on cranes and straddle
30 cars used to move shipping containers; and

31 (3) have the authority to establish or contract with one or more fed-
32 erally funded research and development centers to provide independent
33 analysis of homeland security issues and carry out other responsibilities
34 under this chapter.

35 **§ 12307. Joint annual interagency review of global nuclear**
36 **detection architecture**

37 (a) **DEFINITION OF GLOBAL NUCLEAR DETECTION ARCHITECTURE.**—In
38 this section, the term “global nuclear detection architecture” means the
39 global nuclear detection architecture developed under section 12301 of this
40 title.

41 (b) **ANNUAL REVIEW.**—

1 (1) IN GENERAL.—The Secretary, the Attorney General, the Sec-
2 retary of State, the Secretary of Defense, the Secretary of Energy, and
3 the Director of National Intelligence shall jointly ensure interagency co-
4 ordination on the development and implementation of the global nu-
5 clear detection architecture by ensuring that, not less frequently than
6 once each year—

7 (A) each relevant agency, office, or entity—

8 (i) assesses its involvement, support, and participation in
9 the development, revision, and implementation of the global
10 nuclear detection architecture; and

11 (ii) examines and evaluates components of the global nu-
12 clear detection architecture (including associated strategies
13 and acquisition plans) relating to the operations of that agen-
14 cy, office, or entity, to determine whether the components in-
15 corporate and address current threat assessments, scenarios,
16 or intelligence analyses developed by the Director of National
17 Intelligence or other agencies regarding threats relating to
18 nuclear or radiological weapons of mass destruction;

19 (B) each agency, office, or entity deploying or operating any nu-
20 clear or radiological detection technology under the global nuclear
21 detection architecture—

22 (i) evaluates the deployment and operation by that agency,
23 office, or entity of nuclear or radiological detection tech-
24 nologies under the global nuclear detection architecture;

25 (ii) identifies performance deficiencies and operational or
26 technical deficiencies in nuclear or radiological detection tech-
27 nologies deployed under the global nuclear detection architec-
28 ture; and

29 (iii) assesses the capacity of that agency, office, or entity
30 to implement the responsibilities of that agency, office, or en-
31 tity under the global nuclear detection architecture; and

32 (C) the Director of the Domestic Nuclear Detection Office and
33 each of the relevant departments that are partners in the National
34 Technical Forensics Center—

35 (i) include, as part of the assessments, evaluations, and re-
36 views required under this paragraph, each office's or depart-
37 ment's activities and investments in support of nuclear
38 forensics and attribution activities and specific goals and ob-
39 jectives accomplished during the previous year pursuant to
40 the national strategic five-year plan for improving the nuclear
41 forensic and attribution capabilities of the United States re-

1 required under section 1036 of the National Defense Authoriza-
2 tion Act for Fiscal Year 2010 (Public Law 111–84, 123 Stat.
3 2450);

4 (ii) attach, as an appendix to the Joint Interagency Annual
5 Review, the most current version of the strategy and plan;
6 and

7 (iii) include a description of new or amended bilateral and
8 multilateral agreements and efforts in support of nuclear
9 forensics and attribution activities accomplished during the
10 previous year.

11 (2) TECHNOLOGY.—Not less frequently than once each year, the
12 Secretary shall examine and evaluate the development, assessment, and
13 acquisition of radiation detection technologies deployed or implemented
14 in support of the domestic portion of the global nuclear detection archi-
15 tecture.

16 (e) ANNUAL REPORT ON JOINT INTERAGENCY REVIEW.—

17 (1) IN GENERAL.—Not later than March 31 of each year, the Sec-
18 retary, the Attorney General, the Secretary of State, the Secretary of
19 Defense, the Secretary of Energy, and the Director of National Intel-
20 ligence, shall jointly submit a report regarding the implementation of
21 this section and the results of the reviews required under subsection

22 (a) to—

23 (A) the President;

24 (B) the Committee on Appropriations, the Committee on Armed
25 Services, the Select Committee on Intelligence, and the Committee
26 on Homeland Security and Governmental Affairs of the Senate;
27 and

28 (C) the Committee on Appropriations, the Committee on Armed
29 Services, the Permanent Select Committee on Intelligence, the
30 Committee on Homeland Security, and the Committee on Science
31 and Technology of the House of Representatives.

32 (2) FORM.—The annual report submitted under paragraph (1) shall
33 be submitted in unclassified form to the maximum extent practicable,
34 but may include a classified annex.

35 **Chapter 125—Homeland Security Grants**

Sec.

- 12501. Definitions.
- 12502. Homeland security grant programs.
- 12503. Urban Area Security Initiative.
- 12504. State Homeland Security Grant Program.
- 12505. Grants to directly eligible tribes.
- 12506. Terrorism prevention.
- 12507. Prioritization.
- 12508. Use of funds.
- 12509. Administration and coordination.

12510. Accountability.

12511. Identification of reporting redundancies and development of performance metrics.

1 **§ 12501. Definitions**

2 In this chapter:

3 (1) ADMINISTRATOR.—The term “Administrator” means the Admin-
4 istrator of the Federal Emergency Management Agency.

5 (2) 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 (3) CRITICAL INFRASTRUCTURE SECTORS.—The term “critical infra-
12 structure sectors” means the following sectors, in both urban and rural
13 areas:

14 (A) Agriculture and food.

15 (B) Banking and finance.

16 (C) Chemical industries.

17 (D) Commercial facilities.

18 (E) Commercial nuclear reactors, materials, and waste.

19 (F) Dams.

20 (G) The defense industrial base.

21 (H) Emergency services.

22 (I) Energy.

23 (J) Government facilities.

24 (K) Information technology.

25 (L) National monuments and icons.

26 (M) Postal and shipping.

27 (N) Public health and health care.

28 (O) Telecommunications.

29 (P) Transportation systems.

30 (Q) Water.

31 (4) DIRECTLY ELIGIBLE TRIBE.—The term “directly eligible tribe”
32 means—

33 (A) an Indian tribe—

34 (i) that is located in the continental United States;

35 (ii) that operates a law enforcement or emergency response
36 agency with the capacity to respond to calls for law enforce-
37 ment or emergency services;

38 (iii) that—

1 (I) is located on or near an international border or a
2 coastline bordering an ocean (including the Gulf of Mex-
3 ico) or international waters;

4 (II) is located within 10 miles of a system or asset in-
5 cluded on the prioritized critical infrastructure list estab-
6 lished under section 10516(a)(2) of this title or has such
7 a system or asset within its territory;

8 (III) is located within or contiguous to one of the 50
9 most populous metropolitan statistical areas in the
10 United States; or

11 (IV) has jurisdiction over not less than 1,000 square
12 miles of Indian country, as that term is defined in sec-
13 tion 1151 of title 18; and

14 (iv) that certifies to the Secretary that a State has not pro-
15 vided funds under section 12503 or 12504 of this title to the
16 Indian tribe or consortium of Indian tribes for the purpose
17 for which direct funding is sought; and

18 (B) a consortium of Indian tribes, if each tribe satisfies the re-
19 quirements of subparagraph (A).

20 (5) ELIGIBLE METROPOLITAN AREA.—The term “eligible metropoli-
21 tan area” means any of the 100 most populous metropolitan statistical
22 areas in the United States.

23 (6) HIGH-RISK URBAN AREA.—The term “high-risk urban area”
24 means a high-risk urban area designated under section 12503(b)(3)(A)
25 of this title.

26 (7) INDIAN TRIBE.—The term “Indian tribe” has the meaning given
27 the term in section 4(e) of the Indian Self-Determination and Edu-
28 cation Assistance Act (25 U.S.C. 450b(e)).

29 (8) METROPOLITAN STATISTICAL AREA.—The term “metropolitan
30 statistical area” means a metropolitan statistical area, as defined by
31 the Office of Management and Budget.

32 (9) NATIONAL SPECIAL SECURITY EVENT.—The term “National Spe-
33 cial Security Event” means a designated event that, by virtue of its po-
34 litical, economic, social, or religious significance, may be the target of
35 terrorism or other criminal activity.

36 (10) POPULATION.—The term “population” means population ac-
37 cording to the most recent United States census population estimates
38 available at the start of the relevant fiscal year.

39 (11) POPULATION DENSITY.—The term “population density” means
40 population divided by land area in square miles.

1 (12) QUALIFIED INTELLIGENCE ANALYST.—The term “qualified in-
2 telligence analyst” means an intelligence analyst (as that term is de-
3 fined in section 10512(a) of this title), including law enforcement per-
4 sonnel—

5 (A) who has successfully completed training to ensure baseline
6 proficiency in intelligence analysis and production, as determined
7 by the Secretary, which may include training using a curriculum
8 developed under section 10510 of this title; or

9 (B) whose experience ensures baseline proficiency in intelligence
10 analysis and production equivalent to the training required under
11 subparagraph (A), as determined by the Secretary.

12 (13) TARGET CAPABILITIES.—The term “target capabilities” means
13 the target capabilities for Federal, State, local, and tribal government
14 preparedness for which guidelines are required to be established under
15 section 20506 of this title.

16 (14) TRIBAL GOVERNMENT.—The term “tribal government” means
17 the government of an Indian tribe.

18 **§ 12502. Homeland security grant programs**

19 (a) GRANTS AUTHORIZED.—The Secretary, acting through the Adminis-
20 trator, may award grants under sections 12503 and 12504 of this title to
21 State, local, and tribal governments.

22 (b) PROGRAMS NOT AFFECTED.—This chapter shall not be construed to
23 affect any of the following Federal programs:

24 (1) Firefighter and other assistance programs authorized under the
25 Federal Fire Prevention and Control Act of 1974 (15 U.S.C. 2201 et
26 seq.).

27 (2) Grants authorized under the Robert T. Stafford Disaster Relief
28 and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

29 (3) Emergency Management Performance Grants under the amend-
30 ments made by title II of the Implementing Recommendations of the
31 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 294).

32 (4) Grants to protect critical infrastructure, including port security
33 grants authorized under section 70107 of title 46, and grants author-
34 ized under titles XIV and XV of the Implementing Recommendations
35 of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat.
36 400, 422) and the amendments made by those titles.

37 (5) The Metropolitan Medical Response System authorized under
38 section 20304 of this title.

39 (6) The Interoperable Emergency Communications Grant Program
40 authorized under section 12109 of this title.

1 (7) Grant programs other than those administered by the Depart-
2 ment.

3 (c) RELATIONSHIP TO OTHER LAWS.—

4 (1) IN GENERAL.—The grant programs authorized under sections
5 12503 and 12504 of this title supersede all grant programs authorized
6 under section 1014 of the USA PATRIOT Act (42 U.S.C. 3714).

7 (2) ALLOCATION.—The allocation of grants authorized under sec-
8 tions 12503 and 12504 of this title is governed by the terms of this
9 chapter and not by any other provision of law.

10 **§ 12503. Urban Area Security Initiative**

11 (a) ESTABLISHMENT.—There is in the Department the Urban Area Secu-
12 rity Initiative to provide grants to assist high-risk urban areas in pre-
13 venting, preparing for, protecting against, and responding to acts of ter-
14 rorism.

15 (b) ASSESSMENT AND DESIGNATION OF HIGH-RISK URBAN AREAS.—

16 (1) IN GENERAL.—The Secretary shall designate high-risk urban
17 areas to receive grants under this section based on procedures under
18 this subsection.

19 (2) INITIAL ASSESSMENT.—

20 (A) IN GENERAL.—For each fiscal year, the Secretary shall con-
21 duct an initial assessment of the relative threat, vulnerability, and
22 consequences from acts of terrorism faced by each eligible metro-
23 politan area, including consideration of—

24 (i) the factors set forth in subparagraphs (A) through (H)
25 and (K) of section 12507(a)(1) of this title; and

26 (ii) information and materials submitted under subpara-
27 graph (B).

28 (B) SUBMISSION OF INFORMATION BY ELIGIBLE METROPOLITAN
29 AREAS.—Prior to conducting each initial assessment under sub-
30 paragraph (A), the Secretary shall provide each eligible metropoli-
31 tan area with, and shall notify each eligible metropolitan area of,
32 the opportunity to—

33 (i) submit information that the eligible metropolitan area
34 believes to be relevant to the determination of the threat, vul-
35 nerability, and consequences it faces from acts of terrorism;
36 and

37 (ii) review the risk assessment conducted by the Depart-
38 ment of that eligible metropolitan area, including the bases
39 for the assessment by the Department of the threat, vulner-
40 ability, and consequences from acts of terrorism faced by that

1 eligible metropolitan area, and remedy erroneous or incom-
2 plete information.

3 (3) DESIGNATION OF HIGH-RISK URBAN AREAS.—

4 (A) IN GENERAL.—

5 (i) DESIGNATION.—For each fiscal year, after conducting
6 the initial assessment under paragraph (2), and based on that
7 assessment, the Secretary shall designate high-risk urban
8 areas that may submit applications for grants under this sec-
9 tion.

10 (ii) EXCEPTIONS.—Notwithstanding paragraph (2), the
11 Secretary may—

12 (I) in any case where an eligible metropolitan area
13 consists of more than one metropolitan division (as that
14 term is defined by the Office of Management and Budget)
15 designate more than one high-risk urban area within
16 a single eligible metropolitan area; and

17 (II) designate an area that is not an eligible metropoli-
18 tan area as a high-risk urban area based on the assess-
19 ment by the Secretary of the relative threat, vulner-
20 ability, and consequences from acts of terrorism faced by
21 the area.

22 (iii) SECRETARY NOT REQUIRED TO DESIGNATE ALL ELIGI-
23 BLE AREAS AS HIGH-RISK URBAN AREAS.—Nothing in this
24 subsection may be construed to require the Secretary to—

25 (I) designate all eligible metropolitan areas that sub-
26 mit information to the Secretary under paragraph
27 (2)(B)(i) as high-risk urban areas; or

28 (II) designate all areas within an eligible metropolitan
29 area as part of the high-risk urban area.

30 (B) JURISDICTIONS INCLUDED IN HIGH-RISK URBAN AREAS.—

31 (i) BY SECRETARY.—In designating high-risk urban areas
32 under subparagraph (A), the Secretary shall determine which
33 jurisdictions, at a minimum, shall be included in each high-
34 risk urban area.

35 (ii) BY HIGH-RISK URBAN AREA.—A high-risk urban area
36 designated by the Secretary may, in consultation with the
37 State or States in which the high-risk urban area is located,
38 add additional jurisdictions to the high-risk urban area.

39 (c) APPLICATION.—

40 (1) IN GENERAL.—An area designated as a high-risk urban area
41 under subsection (b) may apply for a grant under this section.

1 (2) MINIMUM CONTENTS OF APPLICATION.—In an application for a
2 grant under this section, a high-risk urban area shall submit—

3 (A) a plan describing the proposed division of responsibilities
4 and distribution of funding among the local and tribal govern-
5 ments in the high-risk urban area;

6 (B) the name of an individual to serve as a high-risk urban area
7 liaison with the Department and among the various jurisdictions
8 in the high-risk urban area; and

9 (C) information in support of the application the Secretary may
10 reasonably require.

11 (3) ANNUAL APPLICATIONS.—Applicants for grants under this sec-
12 tion shall apply or reapply on an annual basis.

13 (4) STATE REVIEW AND TRANSMISSION.—

14 (A) IN GENERAL.—To ensure consistency with State homeland
15 security plans, a high-risk urban area applying for a grant under
16 this section shall submit its application to each State within which
17 any part of that high-risk urban area is located for review before
18 submission of the application to the Department.

19 (B) DEADLINE.—Not later than 30 days after receiving an ap-
20 plication from a high-risk urban area under subparagraph (A), a
21 State shall transmit the application to the Department.

22 (C) OPPORTUNITY FOR STATE COMMENT.—If the Governor of
23 a State determines that an application of a high-risk urban area
24 is inconsistent with the State homeland security plan of that
25 State, or otherwise does not support the application, the Governor
26 shall—

27 (i) notify the Secretary, in writing, of that fact; and

28 (ii) provide an explanation of the reason for not supporting
29 the application at the time of transmission of the application.

30 (5) OPPORTUNITY TO AMEND.—In considering applications for
31 grants under this section, the Secretary shall provide applicants with
32 a reasonable opportunity to correct defects in the application, if any,
33 before making final awards.

34 (d) DISTRIBUTION OF AWARDS.—

35 (1) IN GENERAL.—If the Secretary approves the application of a
36 high-risk urban area for a grant under this section, the Secretary shall
37 distribute the grant funds to the State or States in which that high-
38 risk urban area is located.

39 (2) STATE DISTRIBUTION OF FUNDS.—

40 (A) IN GENERAL.—Not later than 45 days after the date that
41 a State receives grant funds under paragraph (1), that State shall

1 provide the high-risk urban area awarded that grant not less than
 2 80 percent of the grant funds. Any funds retained by a State shall
 3 be expended on items, services, or activities that benefit the high-
 4 risk urban area.

5 (B) FUNDS RETAINED.—A State shall provide each relevant
 6 high-risk urban area with an accounting of the items, services, or
 7 activities on which any funds retained by the State under subpara-
 8 graph (A) were expended.

9 (3) INTERSTATE URBAN AREAS.—If parts of a high-risk urban area
 10 awarded a grant under this section are located in 2 or more States,
 11 the Secretary shall distribute to each State—

12 (A) a portion of the grant funds in accordance with the pro-
 13 posed distribution set forth in the application; or

14 (B) if no agreement on distribution has been reached, a portion
 15 of the grant funds determined by the Secretary to be appropriate.

16 (4) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS
 17 TO HIGH-RISK URBAN AREAS.—A State that receives grant funds under
 18 paragraph (1) shall certify to the Secretary that the State has made
 19 available to the applicable high-risk urban area the required funds
 20 under paragraph (2).

21 (e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be
 22 appropriated for grants under this section such sums as may be necessary.

23 **§ 12504. State Homeland Security Grant Program**

24 (a) ESTABLISHMENT.—There is in the Department a State Homeland Se-
 25 curity Grant Program to assist State, local, and tribal governments in pre-
 26 venting, preparing for, protecting against, and responding to acts of ter-
 27 rorism.

28 (b) APPLICATION.—

29 (1) IN GENERAL.—Each State may apply for a grant under this sec-
 30 tion, and shall submit information in support of the application that
 31 the Secretary may reasonably require.

32 (2) MINIMUM CONTENTS OF APPLICATION.—The Secretary shall re-
 33 quire that each State include in its application, at a minimum—

34 (A) the purpose for which the State seeks grant funds and the
 35 reasons why the State needs the grant to meet the target capabili-
 36 ties of that State;

37 (B) a description of how the State plans to allocate the grant
 38 funds to local governments and Indian tribes; and

39 (C) a budget showing how the State intends to expend the grant
 40 funds.

1 (3) ANNUAL APPLICATIONS.—Applicants for grants under this sec-
2 tion shall apply or reapply on an annual basis.

3 (c) DISTRIBUTION TO LOCAL AND TRIBAL GOVERNMENTS.—

4 (1) IN GENERAL.—Not later than 45 days after receiving grant
5 funds, any State receiving a grant under this section shall make avail-
6 able to local and tribal governments, consistent with the applicable
7 State homeland security plan—

8 (A) not less than 80 percent of the grant funds;

9 (B) with the consent of local and tribal governments, items,
10 services, or activities having a value of not less than 80 percent
11 of the amount of the grant; or

12 (C) with the consent of local and tribal governments, grant
13 funds combined with other items, services, or activities having a
14 total value of not less than 80 percent of the amount of the grant.

15 (2) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS
16 TO LOCAL GOVERNMENTS.—A State shall certify to the Secretary that
17 the State has made the distribution to local and tribal governments re-
18 quired under paragraph (1).

19 (3) EXTENSION OF PERIOD.—The Governor of a State may request
20 in writing that the Secretary extend the period under paragraph (1)
21 for an additional period of time. The Secretary may approve a request
22 if the Secretary determines that the resulting delay in providing grant
23 funding to the local and tribal governments is necessary to promote ef-
24 fective investments to prevent, prepare for, protect against, or respond
25 to acts of terrorism.

26 (4) EXCEPTION.—Paragraph (1) does not apply to the District of
27 Columbia, Puerto Rico, American Samoa, the Northern Mariana Is-
28 lands, Guam, or the Virgin Islands.

29 (5) DIRECT FUNDING.—If a State fails to make the distribution to
30 local or tribal governments required under paragraph (1) in a timely
31 fashion, a local or tribal government entitled to receive the distribution
32 may petition the Secretary to request that grant funds be provided di-
33 rectly to the local or tribal government.

34 (d) MULTISTATE APPLICATIONS.—

35 (1) IN GENERAL.—Instead of, or in addition to, any application for
36 a grant under subsection (b), 2 or more States may submit an applica-
37 tion for a grant under this section in support of multistate efforts to
38 prevent, prepare for, protect against, and respond to acts of terrorism.

39 (2) ADMINISTRATION OF GRANT.—If a group of States applies for
40 a grant under this section, the States shall submit to the Secretary at
41 the time of application a plan describing—

1 (A) the division of responsibilities for administering the grant;
2 and

3 (B) the distribution of funding among the States that are par-
4 ties to the application.

5 (e) MINIMUM ALLOCATION.—

6 (1) IN GENERAL.—In allocating funds under this section, the Sec-
7 retary shall ensure that—

8 (A) except as provided in subparagraph (B), each State receives
9 for each fiscal year, from the funds appropriated for the State
10 Homeland Security Grant Program established under this section,
11 not less than 0.35 percent of the total funds appropriated for
12 grants under this section and section 12503 of this title; and

13 (B) for each fiscal year, American Samoa, the Northern Mar-
14 iana Islands, Guam, and the Virgin Islands each receive, from the
15 funds appropriated for the State Homeland Security Grant Pro-
16 gram established under this section, not less than an amount
17 equal to 0.08 percent of the total funds appropriated for grants
18 under this section and section 12503 of this title.

19 (2) EFFECT OF MULTISTATE AWARD ON STATE MINIMUM.—Any por-
20 tion of a multistate award provided to a State under subsection (d)
21 shall be considered in calculating the minimum State allocation under
22 this subsection.

23 (f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be
24 appropriated for grants under this section such sums as may be necessary.

25 **§ 12505. Grants to directly eligible tribes**

26 (a) IN GENERAL.—Notwithstanding section 12504(b) of this title, the
27 Secretary, acting through the Administrator, may award grants to directly
28 eligible tribes under section 12504.

29 (b) TRIBAL APPLICATIONS.—A directly eligible tribe may apply for a
30 grant under section 12504 of this title by submitting an application to the
31 Secretary that includes, as appropriate, the information required for an ap-
32 plication by a State under section 12504(b).

33 (c) CONSISTENCY WITH STATE PLANS.—

34 (1) IN GENERAL.—To ensure consistency with any applicable State
35 homeland security plan, a directly eligible tribe applying for a grant
36 under section 12504 of this title shall provide a copy of its application
37 to each State within which any part of the tribe is located for review
38 before the tribe submits the application to the Department.

39 (2) OPPORTUNITY FOR COMMENT.—If the Governor of a State deter-
40 mines that the application of a directly eligible tribe is inconsistent
41 with the State homeland security plan of that State, or otherwise does

1 not support the application, not later than 30 days after the date of
2 receipt of that application the Governor shall—

3 (A) notify the Secretary, in writing, of that fact; and

4 (B) provide an explanation of the reason for not supporting the
5 application.

6 (d) FINAL AUTHORITY.—The Secretary shall have final authority to ap-
7 prove any application of a directly eligible tribe. The Secretary shall notify
8 each State within the boundaries of which any part of a directly eligible
9 tribe is located of the approval of an application by the tribe.

10 (e) PRIORITIZATION.—The Secretary shall allocate funds to directly eligi-
11 ble tribes in accordance with the factors applicable to allocating funds
12 among States under section 12507 of this title.

13 (f) DISTRIBUTION OF AWARDS TO DIRECTLY ELIGIBLE TRIBES.—If the
14 Secretary awards funds to a directly eligible tribe under this section, the
15 Secretary shall distribute the grant funds directly to the tribe and not
16 through any State.

17 (g) MINIMUM ALLOCATION.—

18 (1) IN GENERAL.—In allocating funds under this section, the Sec-
19 retary shall ensure that, for each fiscal year, directly eligible tribes col-
20 lectively receive, from the funds appropriated for the State Homeland
21 Security Grant Program established under section 12504 of this title,
22 not less than an amount equal to 0.1 percent of the total funds appro-
23 priated for grants under sections 12503 and 12504 of this title.

24 (2) EXCEPTION.—This subsection shall not apply in any fiscal year
25 in which the Secretary—

26 (A) receives fewer than 5 applications under this section; or

27 (B) does not approve at least 2 applications under this section.

28 (h) TRIBAL LIAISON.—A directly eligible tribe applying for a grant under
29 section 12504 of this title shall designate an individual to serve as a tribal
30 liaison with the Department and other Federal, State, local, and regional
31 government officials concerning preventing, preparing for, protecting
32 against, and responding to acts of terrorism.

33 (i) ELIGIBILITY FOR OTHER FUNDS.—A directly eligible tribe that re-
34 ceives a grant under section 12504 of this title may receive funds for other
35 purposes under a grant from the State or States within the boundaries of
36 which any part of the tribe is located and from any high-risk urban area
37 of which it is a part, consistent with the homeland security plan of the State
38 or high-risk urban area.

39 (j) STATE OBLIGATIONS.—

40 (1) IN GENERAL.—States are responsible for allocating grant funds
41 received under section 12504 of this title to tribal governments in order

1 to help those tribal communities achieve target capabilities not achieved
2 through grants to directly eligible tribes.

3 (2) DISTRIBUTION OF GRANT FUNDS.—With respect to a grant to
4 a State under section 12504, an Indian tribe shall be eligible for fund-
5 ing directly from that State, and shall not be required to seek funding
6 from any local government.

7 (3) IMPOSITION OF REQUIREMENTS.—A State may not impose un-
8 reasonable or unduly burdensome requirements on an Indian tribe as
9 a condition of providing the Indian tribe with grant funds or resources
10 under section 12504 of this title.

11 (k) RULE OF CONSTRUCTION.—Nothing in this section shall be construed
12 to affect the authority of an Indian tribe that receives funds under this
13 chapter.

14 **§ 12506. Terrorism prevention**

15 (a) LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM.—

16 (1) IN GENERAL.—The Secretary, acting through the Administrator,
17 shall ensure that not less than 25 percent of the total combined funds
18 appropriated for grants under sections 12503 and 12504 of this title
19 is used for law enforcement terrorism prevention activities.

20 (2) LAW ENFORCEMENT TERRORISM PREVENTION ACTIVITIES.—Law
21 enforcement terrorism prevention activities include—

22 (A) information sharing and analysis;

23 (B) target hardening;

24 (C) threat recognition;

25 (D) terrorist interdiction;

26 (E) training exercises to enhance preparedness for and response
27 to mass casualty and active shooter incidents and security events
28 at public locations, including airports and mass transit systems;

29 (F) overtime expenses consistent with a State homeland security
30 plan, including for the provision of enhanced law enforcement op-
31 erations in support of Federal agencies, including for increased
32 border security and border crossing enforcement;

33 (G) establishing, enhancing, and staffing with appropriately
34 qualified personnel State, local, and regional fusion centers that
35 comply with the guidelines established under section 10512(j) of
36 this title;

37 (H) paying salaries and benefits for personnel, including individ-
38 uals employed by the grant recipient on the date of the relevant
39 grant application, to serve as qualified intelligence analysts;

1 (I) any other activity permitted under the Fiscal Year 2007
2 Program Guidance of the Department for the Law Enforcement
3 Terrorism Prevention Program; and

4 (J) any other terrorism prevention activity authorized by the
5 Secretary.

6 (3) PARTICIPATION OF UNDERREPRESENTED COMMUNITIES IN FU-
7 SION CENTERS.—The Secretary shall ensure that grant funds described
8 in paragraph (1) are used to support the participation in fusion cen-
9 ters, as appropriate, of law enforcement and other emergency response
10 providers from rural and other underrepresented communities at risk
11 from acts of terrorism.

12 (b) OFFICE FOR STATE AND LOCAL LAW ENFORCEMENT.—

13 (1) ESTABLISHMENT.—There is in the Policy Directorate of the De-
14 partment the Office for State and Local Law Enforcement.

15 (2) ASSISTANT SECRETARY FOR STATE AND LOCAL LAW ENFORCE-
16 MENT.— The Assistant Secretary for State and Local Law Enforce-
17 ment—

18 (A) is the head of the Office for State and Local Law Enforce-
19 ment; and

20 (B) shall have an appropriate background with experience in
21 law enforcement, intelligence, and other counterterrorism func-
22 tions.

23 (3) ASSIGNMENT OF PERSONNEL.—The Secretary shall assign to the
24 Office for State and Local Law Enforcement permanent staff and, as
25 appropriate and consistent with sections 10311(a), 10312(b)(2), and
26 11106(b)(2) of this title, other appropriate personnel detailed from
27 other components of the Department to carry out the responsibilities
28 under this subsection.

29 (4) RESPONSIBILITIES.—The Assistant Secretary for State and
30 Local Law Enforcement shall—

31 (A) lead the coordination of Department-wide policies relating
32 to the role of State and local law enforcement in preventing, pre-
33 paring for, protecting against, and responding to natural disasters,
34 acts of terrorism, and other man-made disasters within the United
35 States;

36 (B) serve as a liaison between State, local, and tribal law en-
37 forcement agencies and the Department;

38 (C) coordinate with the Office of Intelligence and Analysis to
39 ensure the intelligence and information sharing requirements of
40 State, local, and tribal law enforcement agencies are being ad-
41 dressed;

1 (D) work with the Secretary to ensure that law enforcement and
 2 terrorism-focused grants to State, local, and tribal government
 3 agencies, including grants under sections 12503 and 12504 of this
 4 title, the Commercial Equipment Direct Assistance Program, and
 5 other grants administered by the Department to support fusion
 6 centers and law enforcement-oriented programs, are appropriately
 7 focused on terrorism prevention activities;

8 (E) coordinate with the Directorate of Science and Technology,
 9 the Federal Emergency Management Agency, the Department of
 10 Justice, the National Institute of Justice, law enforcement organi-
 11 zations, and other appropriate entities to support the development,
 12 promulgation, and updating, as necessary, of national voluntary
 13 consensus standards for training and personal protective equip-
 14 ment to be used in a tactical environment by law enforcement offi-
 15 cers; and

16 (F) conduct, jointly with the Secretary, a study to determine the
 17 efficacy and feasibility of establishing specialized law enforcement
 18 deployment teams to assist State, local, and tribal governments in
 19 responding to natural disasters, acts of terrorism, or other man-
 20 made disasters and report on the results of that study to the ap-
 21 propriate committees of Congress.

22 (5) RULE OF CONSTRUCTION.—Nothing in this subsection shall be
 23 construed to diminish, supersede, or replace the responsibilities, au-
 24 thorities, or role of the Secretary.

25 **§ 12507. Prioritization**

26 (a) IN GENERAL.—In allocating funds among States and high-risk urban
 27 areas applying for grants under section 12503 or 12504 of this title, the
 28 Secretary, acting through the Administrator, shall consider, for each State
 29 or high-risk urban area—

30 (1) its relative threat, vulnerability, and consequences from acts of
 31 terrorism, including consideration of—

32 (A) its population, including appropriate consideration of mili-
 33 tary, tourist, and commuter populations;

34 (B) its population density;

35 (C) its history of threats, including whether it has been the tar-
 36 get of a prior act of terrorism;

37 (D) its degree of threat, vulnerability, and consequences related
 38 to critical infrastructure (for all critical infrastructure sectors) or
 39 key resources identified by the Secretary or the State homeland
 40 security plan, including threats, vulnerabilities, and consequences

1 related to critical infrastructure or key resources in nearby juris-
 2 dictions;

3 (E) the most current threat assessments available to the De-
 4 partment;

5 (F) whether the State has, or the high-risk urban area is lo-
 6 cated at or near, an international border;

7 (G) whether it has a coastline bordering an ocean (including the
 8 Gulf of Mexico) or international waters;

9 (H) its likely need to respond to acts of terrorism occurring in
 10 nearby jurisdictions;

11 (I) the extent to which it has unmet target capabilities;

12 (J) in the case of a high-risk urban area, the extent to which
 13 that high-risk urban area includes—

14 (i) those incorporated municipalities, counties, parishes,
 15 and Indian tribes within the relevant eligible metropolitan
 16 area, the inclusion of which will enhance regional efforts to
 17 prevent, prepare for, protect against, and respond to acts of
 18 terrorism; and

19 (ii) other local and tribal governments in the surrounding
 20 area that are likely to be called upon to respond to acts of
 21 terrorism within the high-risk urban area; and

22 (K) such other factors as are specified in writing by the Sec-
 23 retary; and

24 (2) the anticipated effectiveness of the proposed use of the grant by
 25 the State or high-risk urban area in increasing the ability of that State
 26 or high-risk urban area to prevent, prepare for, protect against, and
 27 respond to acts of terrorism, to meet its target capabilities, and to oth-
 28 erwise reduce the overall risk to the high-risk urban area, the State,
 29 or the Nation.

30 (b) TYPES OF THREAT.—In assessing threat under this section, the Sec-
 31 retary shall consider the following types of threat to critical infrastructure
 32 sectors and to populations in all areas of the United States, urban and
 33 rural:

34 (1) Biological.

35 (2) Chemical.

36 (3) Cyber.

37 (4) Explosives.

38 (5) Incendiary.

39 (6) Nuclear.

40 (7) Radiological.

41 (8) Suicide bombers.

1 (9) Other types of threat determined relevant by the Secretary.

2 **§ 12508. Use of funds**

3 (a) PERMITTED USES.—The Secretary, acting through the Administrator,
4 shall permit the recipient of a grant under section 12503 or 12504 of this
5 title to use grant funds to achieve target capabilities related to preventing,
6 preparing for, protecting against, and responding to acts of terrorism, con-
7 sistent with a State homeland security plan and relevant local, tribal, and
8 regional homeland security plans, including by working in conjunction with
9 a National Laboratory (as defined in section 2 of the Energy Policy Act
10 of 2005 (42 U.S.C. 15801)), through—

11 (1) developing and enhancing homeland security, emergency manage-
12 ment, or other relevant plans, assessments, or mutual aid agreements;

13 (2) designing, conducting, and evaluating training and exercises, in-
14 cluding training and exercises conducted under section 11112 and
15 20508 of this title;

16 (3) protecting a system or asset included on the prioritized critical
17 infrastructure list established under section 10516(a)(2) of this title;

18 (4) purchasing, upgrading, storing, or maintaining equipment, in-
19 cluding computer hardware and software;

20 (5) ensuring operability and achieving interoperability of emergency
21 communications;

22 (6) responding to an increase in the threat level under the Homeland
23 Security Advisory System, or to the needs resulting from a National
24 Special Security Event;

25 (7) establishing, enhancing, and staffing with appropriately qualified
26 personnel, State, local, and regional fusion centers that comply with the
27 guidelines established under section 10512(j) of this title;

28 (8) enhancing school preparedness;

29 (9) enhancing the security and preparedness of secure and nonsecure
30 areas of eligible airports and surface transportation systems;

31 (10) supporting public safety answering points;

32 (11) paying salaries and benefits for personnel, including individuals
33 employed by the grant recipient on the date of the relevant grant appli-
34 cation, to serve as qualified intelligence analysts, regardless of whether
35 the analysts are current or new full-time employees or contract employ-
36 ees;

37 (12) paying expenses directly relating to administration of the grant,
38 except that expenses may not exceed 3 percent of the amount of the
39 grant;

40 (13) any activity permitted under the Fiscal Year 2007 Program
41 Guidance of the Department for the State Homeland Security Grant

1 Program, the Urban Area Security Initiative (including activities per-
2 mitted under the full-time counterterrorism staffing pilot), or the Law
3 Enforcement Terrorism Prevention Program; and

4 (14) any other appropriate activity, as determined by the Secretary.

5 (b) LIMITATIONS ON USE OF FUNDS.—

6 (1) IN GENERAL.—Funds provided under section 12503 or 12504 of
7 this title may not be used—

8 (A) to supplant State or local funds, except that nothing in this
9 paragraph shall prohibit the use of grant funds provided to a
10 State or high-risk urban area for otherwise permissible uses under
11 subsection (a) on the basis that a State or high-risk urban area
12 has previously used State or local funds to support the same or
13 similar uses; or

14 (B) for any State or local government cost-sharing contribution.

15 (2) PERSONNEL.—

16 (A) IN GENERAL.—Not more than 50 percent of the amount
17 awarded to a grant recipient under section 12503 or 12504 of this
18 title in any fiscal year may be used to pay for personnel, including
19 overtime and backfill costs, in support of the permitted uses under
20 subsection (a).

21 (B) WAIVER.—At the request of the recipient of a grant under
22 section 12503 or 12504, the Secretary may grant a waiver of the
23 limitation under subparagraph (A).

24 (3) LIMITATIONS ON DISCRETION.—

25 (A) IN GENERAL.—With respect to the use of amounts awarded
26 to a grant recipient under section 12503 or 12504 for personnel
27 costs under paragraph (2) of this subsection, the Secretary may
28 not—

29 (i) impose a limit on the amount of the award that may
30 be used to pay for personnel, or personnel-related, costs that
31 is higher or lower than the percent limit imposed in para-
32 graph (2)(A); or

33 (ii) impose any additional limitation on the portion of the
34 funds of a recipient that may be used for a specific type, pur-
35 pose, or category of personnel, or personnel-related, costs.

36 (B) ANALYSTS.—If amounts awarded to a grant recipient under
37 section 12503 or 12504 of this title are used for paying salary or
38 benefits of a qualified intelligence analyst under subsection
39 (a)(10), the Secretary shall make the amounts available without
40 time limitations placed on the period of time that the analyst can
41 serve under the grant.

1 (4) CONSTRUCTION.—

2 (A) IN GENERAL.—A grant awarded under section 12503 or
3 12504 of this title may not be used to acquire land or to construct
4 buildings or other physical facilities.

5 (B) EXCEPTIONS.—

6 (i) IN GENERAL.—Notwithstanding subparagraph (A),
7 nothing in this paragraph shall prohibit the use of a grant
8 awarded under section 12503 or 12504 of this title to achieve
9 target capabilities related to preventing, preparing for, pro-
10 tecting against, or responding to acts of terrorism, including
11 through the alteration or remodeling of existing buildings for
12 the purpose of making the buildings secure against acts of
13 terrorism.

14 (ii) REQUIREMENTS FOR EXCEPTION.—No grant awarded
15 under section 12503 or 12504 of this title may be used for
16 a purpose described in clause (i) unless—

17 (I) specifically approved by the Secretary;

18 (II) any construction work occurs under terms and
19 conditions consistent with the requirements under section
20 611(j)(9) of the Robert T. Stafford Disaster Relief and
21 Emergency Assistance Act (42 U.S.C. 5196(j)(9)); and

22 (III) the amount allocated for purposes under clause
23 (i) does not exceed the greater of \$1,000,000 or 15 per-
24 cent of the grant award.

25 (5) RECREATION.—Grants awarded under this chapter may not be
26 used for recreational or social purposes.

27 (c) MULTIPLE-PURPOSE FUNDS.—Nothing in this chapter shall be con-
28 strued to prohibit State, local, or tribal governments from using grant funds
29 under section 12503 or 12504 of this title in a manner that enhances pre-
30 paredness for disasters unrelated to acts of terrorism, if the use assists the
31 governments in achieving target capabilities related to preventing, preparing
32 for, protecting against, or responding to acts of terrorism.

33 (d) REIMBURSEMENT OF COSTS.—

34 (1) PAID-ON-CALL OR VOLUNTEER REIMBURSEMENT.—In addition to
35 the activities described in subsection (a), a grant under section 12503
36 or 12504 of this title may be used to provide a reasonable stipend to
37 paid-on-call or volunteer emergency response providers who are not oth-
38 erwise compensated for travel to, or participation in, training or exer-
39 cises related to the purposes of this chapter. Any reimbursement shall
40 not be considered compensation for purposes of rendering an emer-

1 agency response provider an employee under the Fair Labor Standards
2 Act of 1938 (29 U.S.C. 201 et seq.).

3 (2) PERFORMANCE OF FEDERAL DUTY.—An applicant for a grant
4 under section 12503 or 12504 may petition the Secretary to use the
5 funds from its grants under those sections for the reimbursement of
6 the cost of any activity relating to preventing, preparing for, protecting
7 against, or responding to acts of terrorism that is a Federal duty and
8 usually performed by a Federal agency, and that is being performed
9 by a State or local government under agreement with a Federal agency.

10 (e) FLEXIBILITY IN UNSPENT HOMELAND SECURITY GRANT FUNDS.—
11 On request by the recipient of a grant under section 12503 or 12504 of
12 this title, the Secretary may authorize the grant recipient to transfer all or
13 part of the grant funds from uses specified in the grant agreement to other
14 uses authorized under this section, if the Secretary determines that the
15 transfer is in the interests of homeland security.

16 (f) EQUIPMENT STANDARDS.—If an applicant for a grant under section
17 12503 or 12504 of this title proposes to upgrade or purchase, with assist-
18 ance provided under that grant, new equipment or systems that do not meet
19 or exceed any applicable national voluntary consensus standards developed
20 under section 20507 of this title, the applicant shall include in its applica-
21 tion an explanation of why the equipment or systems will serve the needs
22 of the applicant better than equipment or systems that meet or exceed the
23 standards.

24 **§ 12509. Administration and coordination**

25 (a) REGIONAL COORDINATION.—The Administrator shall ensure that—

26 (1) all recipients of grants administered by the Department to pre-
27 vent, prepare for, protect against, or respond to natural disasters, acts
28 of terrorism, or other man-made disasters (excluding assistance pro-
29 vided under section 203 or title IV or V of the Robert T. Stafford Dis-
30 aster Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et
31 seq., 5191 et seq.)) coordinate, as appropriate, their prevention, pre-
32 paredness, and protection efforts with neighboring State, local, and
33 tribal governments; and

34 (2) all high-risk urban areas and other recipients of grants adminis-
35 tered by the Department to prevent, prepare for, protect against, or
36 respond to natural disasters, acts of terrorism, or other man-made dis-
37 asters (excluding assistance provided under section 203 or title IV or
38 V of the Robert T. Stafford Disaster Relief and Emergency Assistance
39 Act (42 U.S.C. 5133, 5170 et seq., 5191 et seq.)) that include or sub-
40 stantially affect parts or all of more than one State coordinate, as ap-
41 propriate, across State boundaries, including, where appropriate,

1 through the use of regional working groups and requirements for re-
2 gional plans.

3 (b) PLANNING COMMITTEES.—

4 (1) IN GENERAL.—Any State or high-risk urban area receiving a
5 grant under section 12503 or 12504 of this title shall establish a State
6 planning committee or urban area working group to assist in prepara-
7 tion and revision of the State, regional, or local homeland security plan
8 or the threat and hazard identification and risk assessment and to as-
9 sist in determining effective funding priorities for grants under sections
10 12503 and 12504.

11 (2) COMPOSITION.—

12 (A) IN GENERAL.—The State planning committees and urban
13 area working groups shall include at least 1 representative from
14 each of the following significant stakeholders:

15 (i) Local or tribal government officials.

16 (ii) Emergency response providers, which shall include rep-
17 resentatives of the fire service, law enforcement, emergency
18 medical services, and emergency managers.

19 (iii) Public health officials and other appropriate medical
20 practitioners.

21 (iv) Individuals representing educational institutions, in-
22 cluding elementary schools, community colleges, and other in-
23 stitutions of higher learning.

24 (v) State and regional interoperable communications coor-
25 dinators, as appropriate.

26 (vi) State and major urban area fusion centers, as appro-
27 priate.

28 (B) GEOGRAPHIC REPRESENTATION.—The members of the
29 State planning committee or urban area working group shall be
30 a representative group of individuals from the counties, cities,
31 towns, and Indian tribes in the State or high-risk urban area, in-
32 cluding, as appropriate, representatives of rural, high-population,
33 and high-threat jurisdictions.

34 (3) EXISTING PLANNING COMMITTEES.—Nothing in this subsection
35 may be construed to require that any State or high-risk urban area cre-
36 ate a State planning committee or urban area working group if that
37 State or high-risk urban area has established and uses a multijuris-
38 dictional planning committee or commission that meets the require-
39 ments of this subsection.

40 (c) INTERAGENCY COORDINATION.—

1 (1) IN GENERAL.—The Secretary (acting through the Adminis-
 2 trator), the Attorney General, the Secretary of Health and Human
 3 Services, and the heads of other agencies providing assistance to State,
 4 local, and tribal governments for preventing, preparing for, protecting
 5 against, and responding to natural disasters, acts of terrorism, and
 6 other man-made disasters, shall jointly—

7 (A) compile a comprehensive list of Federal grant programs for
 8 State, local, and tribal governments for preventing, preparing for,
 9 protecting against, and responding to natural disasters, acts of
 10 terrorism, and other man-made disasters;

11 (B) compile the planning, reporting, application, and other re-
 12 quirements and guidance for the grant programs described in sub-
 13 paragraph (A);

14 (C) develop recommendations, as appropriate, to—

15 (i) eliminate redundant and duplicative requirements for
 16 State, local, and tribal governments, including onerous appli-
 17 cation and ongoing reporting requirements;

18 (ii) ensure accountability of the programs to the intended
 19 purposes of the programs;

20 (iii) coordinate allocation of grant funds to avoid duplica-
 21 tive or inconsistent purchases by the recipients;

22 (iv) make the programs more accessible and user friendly
 23 to applicants; and

24 (v) ensure the programs are coordinated to enhance the
 25 overall preparedness of the Nation;

26 (D) submit the information and recommendations under sub-
 27 paragraphs (A), (B), and (C) to the appropriate committees of
 28 Congress; and

29 (E) provide the appropriate committees of Congress, the Comp-
 30 troller General, and any officer or employee of the Government Ac-
 31 countability Office with full access to any information collected or
 32 reviewed in preparing the submission under subparagraph (D).

33 (2) SCOPE OF TASK.—Nothing in this subsection shall authorize the
 34 elimination, or the alteration of the purposes, as delineated by statute,
 35 regulation, or guidance, of a grant program that existed on August 3,
 36 2007, nor authorize the review or preparation of proposals on the elimi-
 37 nation, or the alteration of the purposes, of such a grant program.

38 **§ 12510. Accountability**

39 (a) AUDITS OF GRANT PROGRAMS.—

40 (1) COMPLIANCE REQUIREMENTS.—

1 (A) AUDIT REQUIREMENT.—Each recipient of a grant adminis-
2 tered by the Department that expends not less than \$500,000 in
3 Federal funds during its fiscal year shall submit to the Secretary,
4 through the Administrator, a copy of the organization-wide finan-
5 cial and compliance audit report required under chapter 75 of title
6 31.

7 (B) ACCESS TO INFORMATION.—The Department and each re-
8 cipient of a grant administered by the Department shall provide
9 the Comptroller General and any officer or employee of the Gov-
10 ernment Accountability Office with full access to information re-
11 garding the activities carried out related to any grant administered
12 by the Department.

13 (C) IMPROPER PAYMENTS.—Consistent with the Improper Pay-
14 ments Information Act of 2002 (Public Law 107–300, 31 U.S.C.
15 3321 note), for each of the grant programs under sections 12503,
16 12504, and 20522 of this title, the Secretary shall specify policies
17 and procedures for—

18 (i) identifying activities funded under a grant program that
19 are susceptible to significant improper payments; and

20 (ii) reporting any improper payments to the Department.

21 (2) AGENCY PROGRAM REVIEW.—

22 (A) IN GENERAL.—The Secretary shall biennially conduct, for
23 each State and high-risk urban area receiving a grant adminis-
24 tered by the Department, a programmatic and financial review of
25 all grants awarded by the Department to prevent, prepare for,
26 protect against, or respond to natural disasters, acts of terrorism,
27 or other man-made disasters, excluding assistance provided under
28 section 203, title IV, or title V of the Robert T. Stafford Disaster
29 Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et
30 seq., 5191 et seq.).

31 (B) CONTENTS.—Each review under subparagraph (A) shall, at
32 a minimum, examine—

33 (i) whether the funds awarded were used in accordance
34 with the law, program guidance, and State homeland security
35 plans or other applicable plans; and

36 (ii) the extent to which funds awarded enhanced the ability
37 of a grantee to prevent, prepare for, protect against, and re-
38 spond to natural disasters, acts of terrorism, and other man-
39 made disasters.

40 (C) AUTHORIZATION OF APPROPRIATIONS.—In addition to any
41 other amounts authorized to be appropriated to the Secretary,

1 there are authorized to be appropriated to the Secretary for re-
2 views under this paragraph such sums as may be necessary.

3 (3) PERFORMANCE ASSESSMENT.—In order to ensure that States
4 and high-risk urban areas are using grants administered by the De-
5 partment appropriately to meet target capabilities and preparedness
6 priorities, the Secretary shall—

7 (A) ensure that each State or high-risk urban area conducts or
8 participates in exercises under section 20508(b) of this title;

9 (B) use performance metrics in accordance with the compre-
10 hensive assessment system under section 20509 of this title and en-
11 sure that each State or high-risk urban area regularly tests its
12 progress against the metrics through the exercises required under
13 subparagraph (A);

14 (C) use the remedial action management program under section
15 20510 of this title; and

16 (D) ensure that each State receiving a grant administered by
17 the Department submits a report to the Secretary on its level of
18 preparedness, as required by section 20512(e) of this title.

19 (4) CONSIDERATION OF ASSESSMENTS.—In conducting program re-
20 views and performance audits under paragraph (2), the Secretary and
21 the Inspector General of the Department shall take into account the
22 performance assessment elements required under paragraph (3).

23 (5) RECOVERY AUDITS.—The Secretary shall conduct a recovery
24 audit under section 2(h) of the Improper Payments Elimination and
25 Recovery Act of 2010 (Public Law 111–204, 31 U.S.C. 3321 note) for
26 any grant administered by the Department with a total value of not
27 less than \$1,000,000, if the Secretary finds that—

28 (A) a financial audit has identified improper payments that can
29 be recouped; and

30 (B) it is cost-effective to conduct a recovery audit to recapture
31 the targeted funds.

32 (6) REMEDIES FOR NONCOMPLIANCE.—

33 (A) IN GENERAL.—If, as a result of a review or audit under this
34 subsection or otherwise, the Secretary finds that a recipient of a
35 grant under this chapter has failed to substantially comply with
36 any provision of law or with any regulations or guidelines of the
37 Department regarding eligible expenditures, the Secretary shall—

38 (i) reduce the amount of payment of grant funds to the re-
39 cipient by an amount equal to the amount of grants funds
40 that were not properly expended by the recipient;

1 (ii) limit the use of grant funds to programs, projects, or
2 activities not affected by the failure to comply;

3 (iii) refer the matter to the Inspector General of the De-
4 partment for further investigation;

5 (iv) terminate any payment of grant funds to be made to
6 the recipient; or

7 (v) take other actions the Secretary determines appro-
8 priate.

9 (B) DURATION OF PENALTY.—The Secretary shall apply an ap-
10 propriate penalty under subparagraph (A) until the Secretary de-
11 termines that the grant recipient is in full compliance with the law
12 and with applicable guidelines or regulations of the Department.

13 (b) REPORTS BY GRANT RECIPIENTS.—

14 (1) QUARTERLY REPORTS ON HOMELAND SECURITY SPENDING.—

15 (A) IN GENERAL.—As a condition of receiving a grant under
16 section 12503 or 12504 of this title, a State, high-risk urban area,
17 or directly eligible tribe shall, not later than 30 days after the end
18 of each Federal fiscal quarter, submit to the Secretary a report
19 on activities performed using grant funds during that fiscal quar-
20 ter.

21 (B) CONTENTS.—Each report submitted under subparagraph
22 (A) shall at a minimum include, for the applicable State, high-risk
23 urban area, or directly eligible tribe, and each subgrantee there-
24 of—

25 (i) the amount obligated to that recipient under section
26 12503 or 12504 in that quarter;

27 (ii) the amount of funds received and expended under sec-
28 tion 12503 or 12504 by that recipient in that quarter; and

29 (iii) a summary description of expenditures made by that
30 recipient using the funds, and the purposes for which the ex-
31 penditures were made.

32 (C) END-OF-YEAR REPORT.—The report submitted under sub-
33 paragraph (A) by a State, high-risk urban area, or directly eligible
34 tribe relating to the last quarter of any fiscal year shall include—

35 (i) the amount and date of receipt of all funds received
36 under the grant during that fiscal year;

37 (ii) the identity of, and amount provided to, any subgrantee
38 for that grant during that fiscal year;

39 (iii) the amount and the dates of disbursements of funds
40 expended in compliance with section 12509(a)(1) of this title
41 or under mutual aid agreements or other sharing arrange-

1 ments that apply within the State, high-risk urban area, or
2 directly eligible tribe, as applicable, during that fiscal year;
3 and

4 (iv) how the funds were used by each recipient or sub-
5 grantee during that fiscal year.

6 (2) ANNUAL STATE PREPAREDNESS REPORT.—Any State applying
7 for a grant under section 12504 shall submit to the Secretary annually
8 a State preparedness report, as required by section 20512(e) of this
9 title.

10 (3) ANNUAL REPORT ON EXPENDITURES.—

11 (A) DEFINITION OF HOMELAND SECURITY GRANT.—In this
12 paragraph, the term “homeland security grant” means any grant
13 made or administered by the Department, including—

- 14 (i) the State Homeland Security Grant Program;
15 (ii) the Urban Area Security Initiative Grant Program;
16 (iii) the Law Enforcement Terrorism Prevention Program;
17 (iv) the Citizen Corps; and
18 (v) the Metropolitan Medical Response System.

19 (B) LIST OF EXPENDITURES.—Not later than 12 months after
20 the date of receipt of the grant, and every 12 months thereafter
21 until all funds provided under the grant are expended, each State
22 or local government that receives a homeland security grant shall
23 submit a report to the Secretary that contains a list of all expendi-
24 tures made by the State or local government using funds from the
25 grant.

26 (c) REPORTS BY THE ADMINISTRATOR.—

27 (1) FEDERAL PREPAREDNESS REPORT.—The Administrator shall
28 submit to the appropriate committees of Congress annually the Federal
29 Preparedness Report required under section 20512(a) of this title.

30 (2) RISK ASSESSMENT.—

31 (A) IN GENERAL.—For each fiscal year, the Administrator shall
32 provide to the appropriate committees of Congress a detailed and
33 comprehensive explanation of the methodologies used to calculate
34 risk and compute the allocation of funds for grants administered
35 by the Department, including—

- 36 (i) all variables included in the risk assessment and the
37 weights assigned to each variable;
38 (ii) an explanation of how each variable, as weighted, cor-
39 relates to risk, and the basis for concluding there is a correla-
40 tion; and

(iii) any change in the methodologies from the previous fiscal year, including changes in variables considered, the weighting of those variables, and computational methods.

(B) CLASSIFIED ANNEX.—The information required under subparagraph (A) shall be provided in unclassified form to the greatest extent possible, and may include a classified annex if necessary.

(C) DEADLINE.—For each fiscal year, the information required under subparagraph (A) shall be provided on the earlier of—

(i) October 31; or

(ii) 30 days before the issuance of any program guidance for grants administered by the Department.

(3) TRIBAL FUNDING REPORT.—At the end of each fiscal year, the Administrator shall submit to the appropriate committees of Congress a report setting forth the amount of funding provided during that fiscal year to Indian tribes under any grant program administered by the Department, whether provided directly or through a subgrant from a State or high-risk urban area.

§ 12511. Identification of reporting redundancies and development of performance metrics

(a) DEFINITION OF COVERED GRANTS.—In this section, the term “covered grants” means grants awarded under section 12503 of this title, grants awarded under section 12504 of this title, and any other grants specified by the Administrator.

(b) PLAN TO ELIMINATE REDUNDANT AND UNNECESSARY REPORTING REQUIREMENTS AND TO ASSESS EFFECTIVENESS OF PROGRAMS.—The Administrator shall develop—

(1) a plan, including a specific timetable, for eliminating any redundant and unnecessary reporting requirements imposed by the Administrator on State, local and tribal governments in connection with the awarding of grants; and

(2) a plan, including a specific timetable, for promptly developing a set of quantifiable performance measures and metrics to assess the effectiveness of the programs under which covered grants are awarded.

(c) BIENNIAL REPORTS.—Not later than January 10, 2018, and every 2 years thereafter, the Secretary shall submit to the appropriate committees of Congress a grants management report that includes—

(1) the status of efforts to eliminate redundant and unnecessary reporting requirements imposed on grant recipients, including—

(A) progress made in implementing the plan required under subsection (b)(1);

1 (B) a reassessment of the reporting requirements to identify
2 and eliminate redundant and unnecessary requirements;

3 (2) the status of efforts to develop quantifiable performance meas-
4 ures and metrics to assess the effectiveness of the programs under
5 which the covered grants are awarded, including—

6 (A) progress made in implementing the plan required under
7 subsection (b)(2); and

8 (B) progress made in developing and implementing additional
9 performance metrics and measures for grants, including as part of
10 the comprehensive assessment system required under section
11 20509 of this title; and

12 (3) a performance assessment of each program under which the cov-
13 ered grants are awarded, including—

14 (A) a description of the objectives and goals of the program;

15 (B) an assessment of the extent to which the objectives and
16 goals described in subparagraph (A) have been met, based on the
17 quantifiable performance measures and metrics required under
18 this section and sections 12510(a)(3) and 20509 of this title;

19 (C) recommendations for any program modifications to improve
20 the effectiveness of the program, to address changed or emerging
21 conditions; and

22 (D) an assessment of the experience of recipients of covered
23 grants, including the availability of clear and accurate information,
24 the timeliness of reviews and awards, and the provision of tech-
25 nical assistance, and recommendations for improving that experi-
26 ence.

27 (d) GRANTS PROGRAM MEASUREMENT STUDY.—

28 (1) IN GENERAL.—The National Academy of Public Administration
29 shall assist the Administrator in implementing—

30 (A) quantifiable performance measures and metrics to assess
31 the effectiveness of grants administered by the Department, as re-
32 quired under this section and section 20509 of this title; and

33 (B) the plan required under subsection (b)(2).

34 (2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to
35 be appropriated to the Secretary such sums as may be necessary to
36 carry out this subsection.

37 **Chapter 127—Anti-Trafficking Training for** 38 **Department Personnel**

Sec.

12701. Definition of human trafficking.

12702. Training to identify human trafficking.

12703. Report.

12704. Assistance to non-Federal entities.

1 **§ 12701. Definition of human trafficking**

2 In this chapter, the term “human trafficking” means an art or practice
3 described in paragraph (9) or (10) of section 103 of the Trafficking Victims
4 Protection Act of 2000 (22 U.S.C. 7102(9), (10)).

5 **§ 12702. Training to identify human trafficking**

6 (a) IN GENERAL.—The Secretary shall implement a program to—

7 (1) train and periodically retrain relevant Transportation Security
8 Administration, U. S. Customs and Border Protection, and other De-
9 partment personnel that the Secretary considers appropriate, with re-
10 spect to how to effectively deter, detect, and disrupt human trafficking,
11 and, where appropriate, interdict a suspected perpetrator of human
12 trafficking, during the course of their primary roles and responsibil-
13 ities; and

14 (2) ensure that the personnel referred to in paragraph (1) regularly
15 receive current information on matters relating to the detection of
16 human trafficking, including information that becomes available outside
17 of the Department’s initial or periodic retraining schedule, to the ex-
18 tent relevant to their official duties and consistent with applicable in-
19 formation and privacy laws.

20 (b) TRAINING.—The training referred to in subsection (a) may be con-
21 ducted through in-class or virtual learning capabilities, and shall include—

22 (1) methods for identifying suspected victims of human trafficking
23 and, where appropriate, perpetrators of human trafficking;

24 (2) for appropriate personnel, methods to approach a suspected vic-
25 tim of human trafficking, where appropriate, in a manner that is sen-
26 sitive to the suspected victim and is not likely to alert a suspected per-
27 petrator of human trafficking;

28 (3) training that is most appropriate for a particular location or en-
29 vironment in which the personnel receiving such training perform their
30 official duties;

31 (4) other topics determined by the Secretary to be appropriate; and

32 (5) a post-training evaluation for personnel receiving the training.

33 (c) TRAINING CURRICULUM REVIEW.—The Secretary shall annually reas-
34 sess the training program established under subsection (a) to ensure it is
35 consistent with current techniques, patterns, and trends associated with
36 human trafficking.

37 **§ 12703. Report**

38 Not later than May 29 of each year, the Secretary shall report to Con-
39 gress with respect to the overall effectiveness of the program required by
40 this chapter, the number of cases reported by Department personnel in

1 which human trafficking was suspected, and, of those cases, the number of
2 cases that were confirmed cases of human trafficking.

3 **§ 12704. Assistance to non-Federal entities**

4 The Secretary may provide training curricula to any State, local, or tribal
5 government, or private organization, to assist the government or organiza-
6 tion in establishing a program of training to identify human trafficking, on
7 request from the government or organization.

8 **Subtitle II—National Emergency**
9 **Management**
10 **Chapter 201—General**

Sec.
20101. Definitions.

11 **§ 20101. Definitions**

12 In this subtitle:

13 (1) ADMINISTRATOR.—The term “Administrator” means the Admin-
14 istrator of the Agency.

15 (2) AGENCY.—The term “Agency” means the Federal Emergency
16 Management Agency.

17 (3) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appro-
18 priate committees of Congress” means—

19 (A) the Committee on Homeland Security and Governmental
20 Affairs of the Senate; and

21 (B) those committees of the House of Representatives that the
22 Speaker of the House of Representatives determines appropriate.

23 (4) CATASTROPHIC INCIDENT.—The term “catastrophic incident”
24 means any natural disaster, act of terrorism, or other man-made dis-
25 aster that results in extraordinary levels of casualties or damage or dis-
26 ruption severely affecting the population (including mass evacuations),
27 infrastructure, environment, economy, national morale, or government
28 functions in an area.

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

31 (6) EMERGENCY; MAJOR DISASTER.—The terms “emergency” and
32 “major disaster” have the meanings given the terms in section 102 of
33 the Robert T. Stafford Disaster Relief and Emergency Assistance Act
34 (42 U.S.C. 5122).

35 (7) EMERGENCY MANAGEMENT.—The term “emergency manage-
36 ment” means the governmental function that coordinates and inte-
37 grates all activities necessary to build, sustain, and improve the capa-
38 bility to prepare for, protect against, respond to, recover from, or miti-
39 gate against threatened or actual natural disasters, acts of terrorism,
40 or other man-made disasters.

1 (8) EMERGENCY RESPONSE PROVIDERS.—The term “emergency re-
2 sponse providers” has the meaning given the term in section 10101 of
3 this title.

4 (9) 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 (10) INDIVIDUAL WITH A DISABILITY.—The term “individual with a
9 disability” has the meaning given the term in section 3 of the Ameri-
10 cans with Disabilities Act of 1990 (42 U.S.C. 12102).

11 (11) LOCAL GOVERNMENT.—The term “local government” has the
12 meaning given the term in section 10101 of this title.

13 (12) NATIONAL INCIDENT MANAGEMENT SYSTEM.—The term “Na-
14 tional Incident Management System” means a system to enable effec-
15 tive, efficient, and collaborative incident management.

16 (13) NATIONAL RESPONSE PLAN.—The term “National Response
17 Plan” means the National Response Plan or any successor plan pre-
18 pared under section 11103(a)(6) of this title.

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

21 (15) STATE.—The term “State” has the meaning given the term in
22 section 10101 of this title.

23 (16) SURGE CAPACITY.—The term “surge capacity” means the abil-
24 ity to rapidly and substantially increase the provision of search and res-
25 cue capabilities, food, water, medicine, shelter and housing, medical
26 care, evacuation capacity, staffing (including disaster assistance em-
27 ployees), and other resources necessary to save lives and protect prop-
28 erty during a catastrophic incident.

29 (17) TRIBAL GOVERNMENT.—The term “tribal government” means
30 the government of an Indian tribe or authorized tribal organization, or,
31 in Alaska, a Native village or Alaska Regional Native Corporation.

32 **Chapter 203—Emergency Management** 33 **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.

34 **§ 20301. Surge Capacity Force**

35 (a) ESTABLISHMENT.—

1 (1) IN GENERAL.—The Administrator shall prepare and submit to
2 the appropriate committees of Congress a plan to establish and imple-
3 ment a Surge Capacity Force for deployment of individuals to respond
4 to natural disasters, acts of terrorism, and other man-made disasters,
5 including catastrophic incidents.

6 (2) AUTHORITY.—

7 (A) IN GENERAL.—Except as provided in subparagraph (B), the
8 plan shall provide for individuals in the Surge Capacity Force to
9 be trained and deployed under the authorities set forth in the Rob-
10 ert T. Stafford Disaster Relief and Emergency Assistance Act (42
11 U.S.C. 5121 et seq.).

12 (B) EXCEPTION.—If the Administrator determines that the ex-
13 isting authorities are inadequate for the training and deployment
14 of individuals in the Surge Capacity Force, the Administrator shall
15 report to Congress as to the additional statutory authorities that
16 the Administrator determines necessary.

17 (b) EMPLOYEES DESIGNATED TO SERVE.—The plan shall include proce-
18 dures under which the Secretary shall designate employees of the Depart-
19 ment who are not employees of the Agency and shall, in conjunction with
20 the heads of other Executive agencies, designate employees of those other
21 Executive agencies, as appropriate, to serve on the Surge Capacity Force.

22 (c) CAPABILITIES.—The plan shall ensure that the Surge Capacity
23 Force—

24 (1) includes a sufficient number of individuals credentialed under
25 section 11110 of this title that are capable of deploying rapidly and ef-
26 ficiently after activation to prepare for, respond to, and recover from
27 natural disasters, acts of terrorism, and other man-made disasters, in-
28 cluding catastrophic incidents; and

29 (2) includes a sufficient number of full-time, highly trained individ-
30 uals credentialed under section 11110 to lead and manage the Surge
31 Capacity Force.

32 (d) TRAINING.—The plan shall ensure that the Administrator provides
33 appropriate and continuous training to members of the Surge Capacity
34 Force to ensure the personnel are adequately trained on the Agency's pro-
35 grams and policies for natural disasters, acts of terrorism, and other man-
36 made disasters.

37 (e) NO IMPACT ON AGENCY PERSONNEL CEILING.—Surge Capacity
38 Force members shall not be counted against any personnel ceiling applicable
39 to the Agency.

40 (f) EXPENSES.—The Administrator may provide members of the Surge
41 Capacity Force with travel expenses, including per diem in lieu of subsist-

1 ence, at rates authorized for employees of agencies under subchapter I of
2 chapter 57 of title 5, for the purpose of participating in any training that
3 relates to service as a member of the Surge Capacity Force.

4 (g) IMMEDIATE IMPLEMENTATION OF SURGE CAPACITY FORCE INVOLV-
5 ING FEDERAL EMPLOYEES.—The Administrator shall develop and imple-
6 ment—

7 (1) the procedures under subsection (b); and

8 (2) other elements of the plan needed to establish the portion of the
9 Surge Capacity Force consisting of individuals designated under those
10 procedures.

11 **§ 20302. Evacuation preparedness technical assistance**

12 The Administrator, in coordination with the heads of other appropriate
13 Federal agencies, shall provide evacuation preparedness technical assistance
14 to State, local, and tribal governments, including the preparation of hurri-
15 cane evacuation studies and technical assistance in developing evacuation
16 plans, assessing storm surge estimates, evacuation zones, evacuation clear-
17 ance times, transportation capacity, and shelter capacity.

18 **§ 20303. Urban Search and Rescue Response System**

19 There is in the Agency the Urban Search and Rescue Response System.

20 **§ 20304. Metropolitan Medical Response System Program**

21 (a) IN GENERAL.—There is in the Agency the Metropolitan Medical Re-
22 sponse System Program.

23 (b) PURPOSES.—The Metropolitan Medical Response System Program
24 shall include each purpose of the Program as it existed on June 1, 2006.

25 **§ 20305. Logistics**

26 The Administrator shall develop an efficient, transparent, and flexible lo-
27 gistics system for procurement and delivery of goods and services necessary
28 for an effective and timely response to natural disasters, acts of terrorism,
29 and other man-made disasters and for real-time visibility of items at each
30 point throughout the logistics system.

31 **§ 20306. Pre-positioned equipment program**

32 (a) IN GENERAL.—The Administrator shall establish a pre-positioned
33 equipment program to pre-position standardized emergency equipment in at
34 least 11 locations to sustain and replenish critical assets used by State,
35 local, and tribal governments in response to (or rendered inoperable by the
36 effects of) natural disasters, acts of terrorism, and other man-made disas-
37 ters.

38 (b) NOTICE.—Not later than 60 days before the date of closure, the Ad-
39 ministrator shall notify State, local, and tribal officials in an area in which
40 a location for the pre-positioned equipment program will be closed.

1 **§ 20307. Basic life supporting first aid and education**

2 The Administrator shall enter into agreements with organizations to pro-
3 vide funds to emergency response providers to provide education and train-
4 ing in life supporting first aid to children.

5 **§ 20308. Improvements to information technology systems**

6 The Administrator, in coordination with the Chief Information Officer of
7 the Department, shall take appropriate measures to update and improve the
8 information technology systems of the Agency, including measures to—

9 (1) ensure that the multiple information technology systems of the
10 Agency (including the National Emergency Management Information
11 System, the Logistics Information Management System III, and the
12 Automated Deployment Database) are, to the extent practicable, fully
13 compatible and can share and access information, as appropriate, from
14 each other;

15 (2) ensure technology enhancements reach the headquarters and re-
16 gional offices of the Agency in a timely fashion, to allow seamless inte-
17 gration;

18 (3) develop and maintain a testing environment that ensures that all
19 system components are properly and thoroughly tested before their re-
20 lease;

21 (4) ensure that the information technology systems of the Agency
22 have the capacity to track disaster response personnel, mission assign-
23 ment task orders, commodities, and supplies used in response to a nat-
24 ural disaster, act of terrorism, or other man-made disaster;

25 (5) make appropriate improvements to the National Emergency
26 Management Information System to address shortcomings in the sys-
27 tem on October 4, 2006; and

28 (6) provide training, manuals, and guidance on information tech-
29 nology systems to personnel, including disaster response personnel, to
30 help ensure employees can properly use information technology sys-
31 tems.

32 **§ 20309. Disclosure of certain information to law enforce-**
33 **ment agencies**

34 If circumstances require an evacuation, sheltering, or mass relocation, the
35 Administrator may disclose information in any individual assistance data-
36 base of the Agency under section 552a(b) of title 5 to any law enforcement
37 agency of the Federal Government or a State, local, or tribal government
38 in order to identify illegal conduct or address public safety or security
39 issues, including compliance with sex offender notification laws.

1
2

Chapter 205—Comprehensive 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 governments, 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.

3
4

Subchapter I—National Preparedness System

§ 20501. Definitions

In this chapter:

- (1) CAPABILITY.—The term “capability” means the ability to provide the means to accomplish one or more tasks under specific conditions and to meet specific performance standards. A capability may be achieved with any combination of properly planned, organized, equipped, trained, and exercised personnel that achieves the intended outcome.
- (2) CREDENTIALLED; CREDENTIALING.—The terms “credentialed” and “credentialing” have the meanings given the terms in section 11101 of this title.
- (3) HAZARD.—The term “hazard” has the meaning given the term under section 602(a) of the Robert T. Stafford Disaster Relief and Assistance Act (42 U.S.C. 5195a(a)).
- (4) MISSION ASSIGNMENT.—The term “mission assignment” means a work order issued to a Federal agency by the Agency, directing completion by that agency of a specified task and setting forth funding, other managerial controls, and guidance.

22

1 (5) NATIONAL PREPAREDNESS GOAL.—The term “national prepared-
2 ness goal” means the national preparedness goal established under sec-
3 tion 20503 of this title.

4 (6) NATIONAL PREPAREDNESS SYSTEM.—The term “national pre-
5 paredness system” means the national preparedness system established
6 under section 20504 of this title.

7 (7) NATIONAL TRAINING PROGRAM.—The term “national training
8 program” means the national training program established under sec-
9 tion 20508(a) of this title.

10 (8) OPERATIONAL READINESS.—The term “operational readiness”
11 means the capability of an organization, an asset, a system, or equip-
12 ment to perform the missions or functions for which it is organized or
13 designed.

14 (9) PERFORMANCE MEASURE.—The term “performance measure”
15 means a quantitative or qualitative characteristic used to gauge the re-
16 sults of an outcome compared to its intended purpose.

17 (10) PERFORMANCE METRIC.—The term “performance metric”
18 means a particular value or characteristic used to measure the outcome
19 that is generally expressed in terms of a baseline and a target.

20 (11) PREVENTION.—The term “prevention” means any activity un-
21 dertaken to avoid, prevent, or stop a threatened or actual act of ter-
22 rorism.

23 (12) RESOURCES.—The term “resources” has the meaning given the
24 term in section 11101 of this title.

25 (13) TYPE.—The term “type” means a classification of resources
26 that refers to the capability of a resource.

27 (14) TYPED; TYPING.—The terms “typed” and “typing” have the
28 meanings given the terms in section 11101 of this title.

29 **§ 20502. Development of national preparedness goal and na-**
30 **tional preparedness system**

31 To prepare the Nation for all hazards, including natural disasters, acts
32 of terrorism, and other man-made disasters, the President, consistent with
33 the declaration of policy under section 601 of the Robert T. Stafford Dis-
34 aster Relief and Emergency Assistance Act (42 U.S.C. 5195) and chapter
35 111 of this title, shall develop a national preparedness goal and a national
36 preparedness system.

37 **§ 20503. National preparedness goal**

38 (a) ESTABLISHMENT.—The President, acting through the Administrator,
39 shall complete, revise, and update, as necessary, a national preparedness
40 goal that defines the target level of preparedness to ensure the Nation’s

1 ability to prevent, respond to, recover from, and mitigate against natural
2 disasters, acts of terrorism, and other man-made disasters.

3 (b) CONSISTENT WITH NATIONAL INCIDENT MANAGEMENT SYSTEM AND
4 NATIONAL RESPONSE PLAN.—The national preparedness goal, to the great-
5 est extent practicable, shall be consistent with the National Incident Man-
6 agement System and the National Response Plan.

7 **§ 20504. National preparedness system**

8 (a) ESTABLISHMENT.—The President, acting through the Administrator,
9 shall develop a national preparedness system to enable the Nation to meet
10 the national preparedness goal.

11 (b) COMPONENTS.—The national preparedness system shall include the
12 following components:

- 13 (1) Target capabilities and preparedness priorities.
- 14 (2) Equipment and training standards.
- 15 (3) Training and exercises.
- 16 (4) Comprehensive assessment system.
- 17 (5) Remedial action management program.
- 18 (6) Federal response capability inventory.
- 19 (7) Reporting requirements.
- 20 (8) Federal preparedness.

21 (c) NATIONAL PLANNING SCENARIOS.—The national preparedness system
22 may include national planning scenarios.

23 **§ 20505. National planning scenarios**

24 (a) IN GENERAL.—The Administrator, in coordination with the heads of
25 appropriate Federal agencies and the National Advisory Council, may de-
26 velop planning scenarios to reflect the relative risk requirements presented
27 by all hazards, including natural disasters, acts of terrorism, and other
28 man-made disasters, to provide the foundation for the flexible and adaptive
29 development of target capabilities and the identification of target capability
30 levels to meet the national preparedness goal.

31 (b) DEVELOPMENT.—In developing, revising, and replacing national plan-
32 ning scenarios, the Administrator shall ensure that the scenarios—

- 33 (1) reflect the relative risk of all hazards and illustrate the potential
34 scope, magnitude, and complexity of a broad range of representative
35 hazards; and
- 36 (2) provide the minimum number of representative scenarios nec-
37 essary to identify and define the tasks and target capabilities required
38 to respond to all hazards.

39 **§ 20506. Target capabilities and preparedness priorities**

40 (a) ESTABLISHMENT OF GUIDELINES ON TARGET CAPABILITIES.—The
41 Administrator, in coordination with the heads of appropriate Federal agen-

1 cies, the National Council on Disability, and the National Advisory Council,
2 shall complete, revise, and update, as necessary, guidelines to define risk-
3 based target capabilities for Federal, State, local, and tribal government
4 preparedness that will enable the Nation to prevent, respond to, recover
5 from, and mitigate against all hazards, including natural disasters, acts of
6 terrorism, and other man-made disasters.

7 (b) DISTRIBUTION OF GUIDELINES.—The Administrator shall ensure that
8 the guidelines are provided promptly to the appropriate committees of Con-
9 gress and the States.

10 (c) OBJECTIVES.—The Administrator shall ensure that the guidelines are
11 specific, flexible, and measurable.

12 (d) TERRORISM RISK ASSESSMENT.—With respect to analyzing and as-
13 sessing the risk of acts of terrorism, the Administrator shall consider—

14 (1) the variables of threat, vulnerability, and consequences related to
15 population (including transient commuting and tourist populations),
16 areas of high population density, critical infrastructure, coastline, and
17 international borders; and

18 (2) the most current risk assessment available from the Chief Intel-
19 ligence Officer of the Department of the threats of terrorism against
20 the United States.

21 (e) PREPAREDNESS PRIORITIES.—In establishing the guidelines under
22 subsection (a), the Administrator shall establish preparedness priorities that
23 appropriately balance the risk of all hazards, including natural disasters,
24 acts of terrorism, and other man-made disasters, with the resources re-
25 quired to prevent, respond to, recover from, and mitigate against the haz-
26 ards.

27 (f) MUTUAL AID AGREEMENTS.—The Administrator may provide support
28 for the development of mutual aid agreements in States.

29 **§ 20507. Equipment and training standards**

30 (a) EQUIPMENT STANDARDS.—

31 (1) IN GENERAL.—The Administrator, in coordination with the
32 heads of appropriate Federal agencies and the National Advisory Coun-
33 cil, shall support the development, promulgation, and updating, as nec-
34 essary, of national voluntary consensus standards for the performance,
35 use, and validation of equipment used by Federal, State, local, and
36 tribal governments and nongovernmental emergency response providers.

37 (2) REQUIREMENTS.—The national voluntary consensus standards
38 shall—

39 (A) be designed to achieve equipment and other capabilities con-
40 sistent with the national preparedness goal, including the safety
41 and health of emergency response providers;

1 (B) to the maximum extent practicable, be consistent with exist-
2 ing national voluntary consensus standards;

3 (C) take into account, as appropriate, threats that may not have
4 been contemplated when the existing standards were developed;
5 and

6 (D) focus on maximizing operability, interoperability, inter-
7 changeability, durability, flexibility, efficiency, efficacy, portability,
8 sustainability, and safety.

9 (b) TRAINING STANDARDS.—The Administrator shall—

10 (1) support the development, promulgation, and regular updating, as
11 necessary, of national voluntary consensus standards for training; and

12 (2) ensure that the training provided under the national training
13 program is consistent with the standards.

14 (c) CONSULTATION WITH STANDARDS ORGANIZATIONS.—In carrying out
15 this section, the Administrator shall consult with representatives of relevant
16 public- and private-sector national voluntary consensus standards develop-
17 ment organizations.

18 **§ 20508. Training and exercises**

19 (a) NATIONAL TRAINING PROGRAM.—

20 (1) IN GENERAL.—The Administrator, in coordination with the
21 heads of appropriate Federal agencies, the National Council on Dis-
22 ability, and the National Advisory Council, shall carry out a national
23 training program to implement the national preparedness goal, Na-
24 tional Incident Management System, National Response Plan, and
25 other related plans and strategies.

26 (2) TRAINING PARTNERS.—In developing and implementing the na-
27 tional training program, the Administrator shall—

28 (A) work with government training facilities, academic institu-
29 tions, private organizations, and other entities that provide special-
30 ized, state-of-the-art training for emergency managers or emer-
31 gency response providers; and

32 (B) utilize, as appropriate, training courses provided by commu-
33 nity colleges, State and local public safety academies, State and
34 private universities, and other facilities.

35 (b) NATIONAL EXERCISE PROGRAM.—

36 (1) IN GENERAL.—The Administrator, in coordination with the
37 heads of appropriate Federal agencies, the National Council on Dis-
38 ability, and the National Advisory Council, shall carry out a national
39 exercise program to test and evaluate the national preparedness goal,
40 National Incident Management System, National Response Plan, and
41 other related plans and strategies.

1 (2) REQUIREMENTS.—The national exercise program—

2 (A) shall be—

3 (i) as realistic as practicable, based on current risk assess-
4 ments, including credible threats, vulnerabilities, and con-
5 sequences, and designed to stress the national preparedness
6 system;

7 (ii) designed, as practicable, to simulate the partial or com-
8 plete incapacitation of a State, local, or tribal government;

9 (iii) carried out, as appropriate, with a minimum degree of
10 notice to involved parties regarding the timing and details of
11 the exercises, consistent with safety considerations;

12 (iv) designed to provide for the systematic evaluation of
13 readiness and enhance operational understanding of the inci-
14 dent command system and relevant mutual aid agreements;

15 (v) designed to address the unique requirements of popu-
16 lations with special needs, including the elderly; and

17 (vi) designed to promptly develop after-action reports and
18 plans for quickly incorporating lessons learned into future op-
19 erations; and

20 (B) shall include a selection of model exercises that State, local,
21 and tribal governments can readily adapt for use and provide as-
22 sistance to State, local, and tribal governments with the design,
23 implementation, and evaluation of exercises (whether a model exer-
24 cise program or an exercise designed locally) that—

25 (i) conform to the requirements under subparagraph (A);

26 (ii) are consistent with any applicable State, local, or tribal
27 strategy or plan; and

28 (iii) provide for systematic evaluation of readiness.

29 (3) NATIONAL LEVEL EXERCISES.—Periodically but not less than bi-
30 ennially, the Administrator shall perform national exercises to test and
31 evaluate the following:

32 (A) The capability of Federal, State, local, and tribal govern-
33 ments to detect, disrupt, and prevent threatened or actual cata-
34 strophic acts of terrorism, especially those involving weapons of
35 mass destruction.

36 (B) The readiness of Federal, State, local, and tribal govern-
37 ments to respond and recover in a coordinated and unified manner
38 to catastrophic incidents.

39 **§ 20509. Comprehensive assessment system**

40 (a) ESTABLISHMENT.—The Administrator, in coordination with the Na-
41 tional Council on Disability and the National Advisory Council, shall estab-

1 lish a comprehensive system to assess, on an ongoing basis, the Nation's
 2 prevention capabilities and overall preparedness, including operational readi-
 3 ness.

4 (b) PERFORMANCE METRICS AND MEASURES.—The Administrator shall
 5 ensure that each component of the national preparedness system, National
 6 Incident Management System, National Response Plan, and other related
 7 plans and strategies, and the reports required under section 20512 of this
 8 title is developed, revised, and updated with clear and quantifiable perform-
 9 ance metrics, measures, and outcomes.

10 (c) CONTENTS.—The assessment system established under subsection (a)
 11 shall assess—

12 (1) compliance with the national preparedness system, National Inci-
 13 dent Management System, National Response Plan, and other related
 14 plans and strategies;

15 (2) capability levels at the time of assessment against target capa-
 16 bility levels defined pursuant to the guidelines established under section
 17 20506(a) of this title;

18 (3) resource needs to meet the desired target capability levels defined
 19 pursuant to the guidelines established under section 20506(a); and

20 (4) performance of training, exercises, and operations.

21 **§ 20510. Remedial action management program**

22 The Administrator, in coordination with the National Council on Dis-
 23 ability and the National Advisory Council, shall establish a remedial action
 24 management program to—

25 (1) analyze training, exercises, and real-world events to identify and
 26 disseminate lessons learned and best practices;

27 (2) generate and disseminate, as appropriate, after-action reports to
 28 participants in exercises and real-world events; and

29 (3) conduct remedial action tracking and long-term trend analysis.

30 **§ 20511. Federal response capability inventory**

31 (a) IN GENERAL.—Under section 611(h)(1)(C) of the Robert T. Stafford
 32 Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196(h)(1)(C)),
 33 the Administrator shall accelerate the completion of the inventory of Federal
 34 response capabilities.

35 (b) CONTENTS.—For each Federal agency with responsibilities under the
 36 National Response Plan, the inventory shall include—

37 (1) for each capability—

38 (A) the performance parameters of the capability;

39 (B) the timeframe within which the capability can be brought
 40 to bear on an incident; and

1 (C) the readiness of the capability to respond to all hazards, in-
 2 cluding natural disasters, acts of terrorism, and other man-made
 3 disasters;

4 (2) a list of personnel credentialed under section 11110 of this title;

5 (3) a list of resources typed under section 11110; and

6 (4) emergency communications assets maintained by the Federal
 7 Government and, if appropriate, State, local, and tribal governments
 8 and the private sector.

9 (c) DEPARTMENT OF DEFENSE.—The Administrator, in coordination
 10 with the Secretary of Defense, shall develop a list of organizations and func-
 11 tions within the Department of Defense that may be used, pursuant to the
 12 authority provided under the National Response Plan and sections 402,
 13 403, and 502 of the Robert T. Stafford Disaster Relief and Emergency As-
 14 sistance Act (42 U.S.C. 5170a, 5170b, 5192), to provide support to civil
 15 authorities during natural disasters, acts of terrorism, and other man-made
 16 disasters.

17 (d) DATABASE.—The Administrator shall establish an inventory database
 18 to allow—

19 (1) real-time exchange of information regarding—

20 (A) capabilities;

21 (B) readiness;

22 (C) the compatibility of equipment;

23 (D) credentialed personnel; and

24 (E) typed resources;

25 (2) easy identification and rapid deployment of capabilities,
 26 credentialed personnel, and typed resources during an incident; and

27 (3) the sharing of the inventory described in subsection (a) with
 28 other Federal agencies, as appropriate.

29 **§ 20512. Reporting requirements**

30 (a) FEDERAL PREPAREDNESS REPORT.—

31 (1) IN GENERAL.—The Administrator, in coordination with the
 32 heads of appropriate Federal agencies, shall submit annually to the ap-
 33 propriate committees of Congress a report on the Nation's level of pre-
 34 paredness for all hazards, including natural disasters, acts of terrorism,
 35 and other man-made disasters.

36 (2) CONTENTS.—Each report shall include—

37 (A) an assessment of how Federal assistance supports the na-
 38 tional preparedness system;

39 (B) the results of the comprehensive assessment carried out
 40 under section 20509 of this title;

1 (C) a review of the inventory described in section 20511 of this
 2 title, including the number and type of credentialed personnel in
 3 each category of personnel trained and ready to respond to a nat-
 4 ural disaster, act of terrorism, or other man-made disaster;

5 (D) an assessment of resource needs to meet preparedness pri-
 6 orities established under section 20506(e) of this title, including—

7 (i) an estimate of the amount of Federal, State, local, and
 8 tribal expenditures required to attain the preparedness prior-
 9 ities; and

10 (ii) the extent to which the use of Federal assistance dur-
 11 ing the preceding fiscal year achieved the preparedness prior-
 12 ities;

13 (E) an evaluation of the extent to which grants administered by
 14 the Department, including grants under chapter 125 of this title—

15 (i) have contributed to the progress of State, local, and
 16 tribal governments in achieving target capabilities; and

17 (ii) have led to the reduction of risk from natural disasters,
 18 acts of terrorism, or other man-made disasters nationally and
 19 in State, local, and tribal jurisdictions; and

20 (F) a discussion of whether the list of credentialed personnel of
 21 the Agency described in section 20511(b)(2) of this title—

22 (i) complies with the strategic human capital plan devel-
 23 oped under section 10102 of title 5; and

24 (ii) is sufficient to respond to a natural disaster, act of ter-
 25 rorism, or other man-made disaster, including a catastrophic
 26 incident.

27 (b) CATASTROPHIC RESOURCE ESTIMATE.—

28 (1) IN GENERAL.—The Administrator shall develop and submit an-
 29 nually to the appropriate committees of Congress an estimate of the
 30 resources of the Agency and other Federal agencies needed for, and de-
 31 voted specifically to, developing the capabilities of Federal, State, local,
 32 and tribal governments necessary to respond to a catastrophic incident.

33 (2) CONTENTS.—Each estimate shall include the resources necessary
 34 for and devoted to—

35 (A) planning;

36 (B) training and exercises;

37 (C) Regional Office enhancements;

38 (D) staffing, including for surge capacity during a catastrophic
 39 incident;

40 (E) additional logistics capabilities;

1 (F) other responsibilities under the catastrophic incident annex
 2 and the catastrophic incident supplement of the National Response
 3 Plan;

4 (G) State, local, and tribal government catastrophic incident
 5 preparedness; and

6 (H) increases in the fixed costs or expenses of the Agency, in-
 7 cluding rent or property acquisition costs or expenses, taxes, con-
 8 tributions to the working capital fund of the Department, and se-
 9 curity costs for the year after the year in which the estimate is
 10 submitted.

11 (c) STATE PREPAREDNESS REPORT.—

12 (1) IN GENERAL.—A State receiving Federal preparedness assistance
 13 administered by the Department annually shall submit a report to the
 14 Administrator on the State’s level of preparedness.

15 (2) CONTENTS.—Each report shall include—

16 (A) an assessment of State compliance with the national pre-
 17 paredness system, National Incident Management System, Na-
 18 tional Response Plan, and other related plans and strategies;

19 (B) an assessment of current capability levels and a description
 20 of target capability levels; and

21 (C) a discussion of the extent to which target capabilities identi-
 22 fied in the applicable State homeland security plan and other ap-
 23 plicable plans remain unmet and an assessment of resources need-
 24 ed to meet the preparedness priorities established under section
 25 20506(e) of this title, including—

26 (i) an estimate of the amount of expenditures required to
 27 attain the preparedness priorities; and

28 (ii) the extent to which the use of Federal assistance dur-
 29 ing the preceding fiscal year achieved the preparedness prior-
 30 ities.

31 **§ 20513. Federal preparedness**

32 (a) AGENCY RESPONSIBILITY.—In support of the national preparedness
 33 system, the President shall ensure that each Federal agency with respon-
 34 sibilities under the National Response Plan—

35 (1) has the operational capability to meet the national preparedness
 36 goal, including—

37 (A) the personnel to make and communicate decisions;

38 (B) organizational structures that are assigned, trained, and ex-
 39 ercised for the missions of the agency;

40 (C) sufficient physical resources; and

1 (D) the command, control, and communication channels to
2 make, monitor, and communicate decisions;

3 (2) complies with the National Incident Management System, includ-
4 ing credentialing of personnel and typing of resources likely needed to
5 respond to a natural disaster, act of terrorism, or other man-made dis-
6 aster under section 11110 of this title;

7 (3) develops, trains, and exercises rosters of response personnel to
8 be deployed when the agency is called on to support a Federal re-
9 sponse;

10 (4) develops deliberate operational plans and the corresponding capa-
11 bilities, including crisis planning, to respond effectively to natural dis-
12 asters, acts of terrorism, and other man-made disasters in support of
13 the National Response Plan to ensure a coordinated Federal response;
14 and

15 (5) regularly updates, verifies the accuracy of, and provides to the
16 Administrator the information in the inventory required under section
17 20511 of this title.

18 (b) OPERATIONAL PLANS.—An operations plan developed under sub-
19 section (a)(4) shall meet the following requirements:

20 (1) The operations plan shall be coordinated under a unified system
21 with a common terminology, approach, and framework.

22 (2) The operations plan shall be developed, in coordination with
23 State, local, and tribal government officials, to address both regional
24 and national risks.

25 (3) The operations plan shall contain, as appropriate, the following
26 elements:

27 (A) Concepts of operations.

28 (B) Critical tasks and responsibilities.

29 (C) Detailed resource and personnel requirements, together with
30 sourcing requirements.

31 (D) Specific provisions for the rapid integration of the resources
32 and personnel of the agency into the overall response.

33 (4) The operations plan shall address, as appropriate, the following
34 matters:

35 (A) Support of State, local, and tribal governments in con-
36 ducting mass evacuations, including—

37 (i) transportation and relocation;

38 (ii) short- and long-term sheltering and accommodation;

39 (iii) provisions for populations with special needs, keeping
40 families together, and expeditious location of missing chil-
41 dren; and

1 (iv) policies and provisions for pets.

2 (B) The preparedness and deployment of public health and med-
3 ical resources, including resources to address the needs of evacuees
4 and populations with special needs.

5 (C) The coordination of interagency search and rescue oper-
6 ations, including land, water, and airborne search and rescue oper-
7 ations.

8 (D) The roles and responsibilities of the Senior Federal Law
9 Enforcement Official with respect to other law enforcement enti-
10 ties.

11 (E) The protection of critical infrastructure.

12 (F) The coordination of maritime salvage efforts among relevant
13 agencies.

14 (G) The coordination of Department of Defense and National
15 Guard support of civilian authorities.

16 (H) To the extent practicable, the utilization of Department of
17 Defense, National Air and Space Administration, National Oceanic
18 and Atmospheric Administration, and commercial aircraft and sat-
19 ellite remotely sensed imagery.

20 (I) The coordination and integration of support from the private
21 sector and nongovernmental organizations.

22 (J) The safe disposal of debris, including hazardous materials,
23 and, when practicable, the recycling of debris.

24 (K) The identification of the required surge capacity.

25 (L) Specific provisions for the recovery of affected geographic
26 areas.

27 (c) MISSION ASSIGNMENTS.—To expedite the provision of assistance
28 under the National Response Plan, the President shall ensure that the Ad-
29 ministrator, in coordination with Federal agencies with responsibilities
30 under the National Response Plan, develops pre-scripted mission assign-
31 ments, including logistics, communications, mass care, health services, and
32 public safety.

33 (d) CERTIFICATION.—The President shall certify to the Committee on
34 Homeland Security and Governmental Affairs of the Senate and the Com-
35 mittee on Homeland Security and the Committee on Transportation and In-
36 frastructure of the House of Representatives on an annual basis that each
37 Federal agency with responsibilities under the National Response Plan com-
38 plies with subsections (a) and (b).

39 (e) CONSTRUCTION.—Nothing in this section shall be construed to limit
40 the authority of the Secretary of Defense with regard to—

- 1 (1) the command, control, training, planning, equipment, exercises,
 2 or employment of Department of Defense forces; or
 3 (2) the allocation of Department of Defense resources.

4 **§ 20514. Use of existing resources**

5 In establishing the national preparedness goal and national preparedness
 6 system, the Administrator shall use existing preparedness documents, plan-
 7 ning tools, and guidelines to the extent practicable and consistent with this
 8 subtitle.

9 **Subchapter II—Additional Preparedness**

10 **§ 20521. Emergency Management Assistance Compact grants**

11 (a) IN GENERAL.—The Administrator may make grants to administer the
 12 Emergency Management Assistance Compact consented to by the Joint Res-
 13 olution entitled “Joint Resolution granting the consent of Congress to the
 14 Emergency Management Assistance Compact” (Public Law 104–321, 110
 15 Stat. 3877).

16 (b) USES.—A grant under this section shall be used—

- 17 (1) to carry out recommendations identified in the Emergency Man-
 18 agement Assistance Compact after-action reports for the 2004 and
 19 2005 hurricane season;
 20 (2) to administer compact operations on behalf of all member States
 21 and territories;
 22 (3) to continue coordination with the Agency and appropriate Fed-
 23 eral agencies;
 24 (4) to continue coordination with State, local, and tribal government
 25 entities and their respective national organizations; and
 26 (5) to assist State and local governments, emergency response pro-
 27 viders, and organizations representing the providers with credentialing
 28 emergency response providers and the typing of emergency response re-
 29 sources.

30 (c) COORDINATION.—The Administrator shall consult with the Adminis-
 31 trator of the Emergency Management Assistance Compact to ensure effec-
 32 tive coordination of efforts in responding to requests for assistance.

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—

20 (A) the population of each State; bears to

21 (B) the population of all States.

22 **§ 20523. Training for emergency response providers from**
23 **Federal Government, foreign governments, or pri-**
24 **ivate entities**

25 (a) IN GENERAL.—The Center for Domestic Preparedness may provide
26 training to emergency response providers from the Federal Government, for-
27 eign governments, or private entities if the Center for Domestic Prepared-
28 ness is reimbursed for the cost of the training. Any reimbursement under
29 this subsection shall be credited to the account from which the expenditure
30 being reimbursed was made and is available, without fiscal year limitation,
31 for the purposes for which amounts in the account may be expended.

32 (b) TRAINING NOT TO INTERFERE WITH PRIMARY MISSION.—The head
33 of the Center for Domestic Preparedness shall ensure that any training pro-
34 vided under subsection (a) does not interfere with the primary mission of
35 the Center for Domestic Preparedness to train State and local emergency
36 response providers.

37 (c) TRAINING FEDERAL EMERGENCY MANAGEMENT AGENCY EMPLOY-
38 EES.—Subject to subsection (b), subsection (a) does not prohibit the Center
39 for Domestic Preparedness from providing training to employees of the
40 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 report of excess real property owned by the United States
2 to a disposal agency, if the estimated value is more than \$50,000.

3 (2) SUMMARY OF GENERAL PLAN REQUIRED FOR CERTAIN TRANS-
4 ACTIONS.—If a transaction covered by clause (A) or (B) of paragraph
5 (1) is part of a project, the report must include a summarization of
6 the general plan for that project, including an estimate of the total cost
7 of the lands to be acquired or leases to be made.

8 (c) ANNUAL REPORTS TO ARMED SERVICES COMMITTEES.—The Director
9 of the Office of Civil and Defense Mobilization shall report annually to the
10 Committees on Armed Services of the Senate and the House of Representa-
11 tives on transactions described in subsection (a) that involve an estimated
12 value of more than \$5,000 but not more than \$50,000.

13 (d) STATEMENT OF COMPLIANCE IS CONCLUSIVE.—A statement in an in-
14 strument of conveyance, including a lease, that the requirements of this sec-
15 tion have been met, or that the conveyance is not subject to this section,
16 is conclusive.

17 **Subchapter III—Miscellaneous Authorities**
18 **§ 20531. National Disaster Recovery Strategy**

19 (a) IN GENERAL.—The Administrator, in coordination with the Secretary
20 of Housing and Urban Development, the Administrator of the Environ-
21 mental Protection Agency, the Secretary of Agriculture, the Secretary of
22 Commerce, the Secretary of the Treasury, the Secretary of Transportation,
23 the Administrator of the Small Business Administration, the Assistant Sec-
24 retary for Indian Affairs of the Department of the Interior, and the heads
25 of other appropriate Federal agencies, State, local, and tribal government
26 officials (including through the National Advisory Council), and representa-
27 tives of appropriate nongovernmental organizations, shall develop, coordi-
28 nate, and maintain a National Disaster Recovery Strategy to serve as a
29 guide to recovery efforts after major disasters and emergencies.

30 (b) CONTENTS.—The National Disaster Recovery Strategy shall—

31 (1) outline the most efficient and cost-effective Federal programs
32 that will meet the recovery needs of States, local and tribal govern-
33 ments, and individuals and households affected by a major disaster;

34 (2) clearly define the role, programs, authorities, and responsibilities
35 of each Federal agency that may be of assistance in providing assist-
36 ance in the recovery from a major disaster;

37 (3) promote the use of the most appropriate and cost-effective build-
38 ing materials (based on the hazards present in an area) in an area af-
39 fected by a major disaster, with the goal of encouraging the construc-
40 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 (e) 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 essary 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) of this section, the National Advisory Council, the National
26 Council on Disability, and other entities at the Administrator's discretion,
27 shall develop, coordinate, and maintain a National Disaster Housing Strat-
28 egy.

29 (b) CONTENTS.—The National Disaster Housing Strategy shall—

30 (1) outline the most efficient and cost-effective Federal programs
31 that will best meet the short-term and long-term housing needs of indi-
32 viduals and households affected by a major disaster;

33 (2) clearly define the role, programs, authorities, and responsibilities
34 of each entity in providing housing assistance in the event of a major
35 disaster, including—

36 (A) the Agency;

37 (B) the Department of Housing and Urban Development;

38 (C) the Department of Agriculture;

39 (D) the Department of Veterans Affairs;

40 (E) the Department of Health and Human Services;

41 (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 11113 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 Secretary shall establish procedures to make all relevant information
41 available to the Child Locator Center in a timely manner to facilitate

1 the expeditious identification and reunification of children with their
2 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 that is the parent or guardian of
15 a 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. Limitations on tiering of subcontractors.

20703. Oversight and accountability of Federal disaster expenditures.

20704. Limitation on length of certain noncompetitive contracts.

20705. Fraud, waste, and abuse controls.
 20706. Registry of disaster response contractors.
 20707. 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 **§ 20702. Limitations on tiering of subcontractors**

34 (a) APPLICATION.—This section applies to any cost-reimbursement type
 35 contract or task or delivery order in an amount greater than the simplified
 36 acquisition threshold (as defined by section 134 of title 41) entered into by
 37 the Department to facilitate response to or recovery from a natural disaster
 38 or act of terrorism or other man-made disaster.

1 (b) REGULATIONS.—The Administrator shall promulgate regulations ap-
2 plicable to contracts described in subsection (a) to minimize the excessive
3 use by contractors of subcontractors or tiers of subcontractors to perform
4 the principal work of the contract.

5 (c) SPECIFIC REQUIREMENT.—At a minimum, the regulations promul-
6 gated under subsection (b) shall preclude a contractor from using sub-
7 contracts for more than 65 percent of the cost of the contract or the cost
8 of any individual task or delivery order (not including overhead and profit),
9 unless the Secretary determines that this requirement is not feasible or
10 practicable.

11 **§ 20703. Oversight and accountability of Federal disaster ex-**
12 **penditures**

13 (a) DEFINITION OF OVERSIGHT FUNDS.—In this section, the term “over-
14 sight funds” means funds referred to in subsection (b) that are designated
15 for use in performing oversight activities.

16 (b) AUTHORITY OF ADMINISTRATOR TO DESIGNATE FUNDS FOR OVER-
17 SIGHT ACTIVITIES.—The Administrator may designate up to 1 percent of
18 the total amount provided to a Federal agency for a mission assignment as
19 oversight funds to be used by the recipient agency for performing oversight
20 of activities carried out under the Agency reimbursable mission assignment
21 process. The funds are available until expended.

22 (c) USE OF FUNDS.—

23 (1) TYPES OF OVERSIGHT ACTIVITIES.—Oversight funds may be
24 used for the following types of oversight activities related to Agency
25 mission assignments:

26 (A) Monitoring, tracking, and auditing expenditures of funds.

27 (B) Ensuring that sufficient management and internal control
28 mechanisms are available so that Agency funds are spent appro-
29 priately and in accordance with all applicable laws and regulations.

30 (C) Reviewing selected contracts and other activities.

31 (D) Investigating allegations of fraud involving Agency funds.

32 (E) Conducting and participating in fraud prevention activities
33 with other Federal, State, and local government personnel and
34 contractors.

35 (2) PLANS AND REPORTS.—Oversight funds may be used to issue the
36 plans required under subsection (f) and the reports required under sub-
37 section (g).

38 (d) RESTRICTION ON USE OF FUNDS.—Oversight funds may not be used
39 to finance existing agency oversight responsibilities related to direct agency
40 appropriations used for disaster response, relief, and recovery activities.

41 (e) METHODS OF OVERSIGHT ACTIVITIES.—

1 (1) IN GENERAL.—Oversight activities may be carried out by an
2 agency under this section either directly or by contract. The activities
3 may include evaluations and financial and performance audits.

4 (2) COORDINATION OF OVERSIGHT ACTIVITIES.—To the extent prac-
5 ticable, evaluations and audits under this section shall be performed by
6 the inspector general of the agency.

7 (f) DEVELOPMENT OF OVERSIGHT PLANS.—

8 (1) IN GENERAL.—If an agency receives oversight funds for a fiscal
9 year, the head of the agency shall prepare a plan describing the over-
10 sight activities for disaster response, relief, and recovery anticipated to
11 be undertaken during the subsequent fiscal year.

12 (2) SELECTION OF OVERSIGHT ACTIVITIES.—In preparing the plan,
13 the head of the agency shall select oversight activities based upon a
14 risk assessment of those areas that present the greatest risk of fraud,
15 waste, and abuse.

16 (3) SCHEDULE.—The plan shall include a schedule for conducting
17 oversight activities, including anticipated dates of completion.

18 (g) FEDERAL DISASTER ASSISTANCE ACCOUNTABILITY REPORTS.—An
19 agency receiving oversight funds under this section shall submit annually to
20 the Administrator and the appropriate committees of Congress a consoli-
21 dated report regarding the use of the funds, including information summa-
22 rizing oversight activities and the results achieved.

23 **§ 20704. Limitation on length of certain noncompetitive con-**
24 **tracts**

25 (a) COVERED CONTRACTS.—This section applies to any contract in an
26 amount greater than the simplified acquisition threshold (as defined by sec-
27 tion 134 of title 41) entered into by the Department to facilitate response
28 to or recovery from a natural disaster, act of terrorism, or other man-made
29 disaster.

30 (b) REGULATIONS.—The Secretary shall promulgate regulations applica-
31 ble to contracts described in subsection (a) to restrict the contract period
32 of a contract entered into using procedures other than competitive proce-
33 dures pursuant to the exception provided in section 3304(a)(2) of title 41
34 to the minimum contract period necessary—

35 (1) to meet the urgent and compelling requirements of the work to
36 be performed under the contract; and

37 (2) to enter into another contract for the required goods or services
38 through the use of competitive procedures.

39 (c) SPECIFIC CONTRACT PERIOD.—The regulations promulgated under
40 subsection (b) shall require the contract period to not exceed 150 days, un-
41 less the Secretary determines that exceptional circumstances apply.

1 **§ 20705. Fraud, waste, and abuse controls**

2 (a) IN GENERAL.—The Administrator shall ensure that—

3 (1) all programs in the Agency administering Federal disaster relief
4 assistance develop and maintain proper internal management controls
5 to prevent and detect fraud, waste, and abuse;

6 (2) application databases are used by the Agency to collect informa-
7 tion on eligible recipients record disbursements;

8 (3) tracking to prevent and detect fraud, waste, and abuse is de-
9 signed to highlight and identify ineligible applications; and

10 (4) the databases used to collect information from applications for
11 assistance are integrated with disbursements and payment records.

12 (b) AUDITS AND REVIEWS REQUIRED.—The Administrator shall ensure
13 that any database or similar application processing system for Federal dis-
14 aster relief assistance programs administered by the Agency undergoes a re-
15 view by the Inspector General of the Department to determine the existence
16 and implementation of internal controls required under this section and sec-
17 tion 408(i) of the Robert T. Stafford Disaster Relief and Emergency Assist-
18 ance Act (42 U.S.C. 5174(i)).

19 **§ 20706. Registry of disaster response contractors**

20 (a) DEFINITIONS.—In this section, the terms “small business concern”,
21 “small business concern owned and controlled by service-disabled veterans”,
22 “small business concern owned and controlled by socially and economically
23 disadvantaged individuals”, and “small business concern owned and con-
24 trolled by women” have the meanings given the terms under the Small Busi-
25 ness Act (15 U.S.C. 631 et seq.).

26 (b) REGISTRY.—

27 (1) IN GENERAL.—The Administrator shall establish and maintain
28 a registry of contractors who are willing to perform debris removal, dis-
29 tribution of supplies, reconstruction, and other disaster or emergency
30 relief activities.

31 (2) CONTENTS.—The registry shall include, for each business con-
32 cern—

33 (A) the name of the business concern;

34 (B) the location of the business concern;

35 (C) the area served by the business concern;

36 (D) the type of good or service provided by the business con-
37 cern;

38 (E) the bonding level of the business concern; and

39 (F) whether the business concern is—

40 (i) a small business concern;

1 (ii) a small business concern owned and controlled by so-
2 cially and economically disadvantaged individuals;

3 (iii) a small business concern owned and controlled by
4 women; or

5 (iv) a small business concern owned and controlled by serv-
6 ice-disabled veterans.

7 (3) SOURCE OF INFORMATION.—

8 (A) SUBMISSION.—Information maintained in the registry shall
9 be submitted on a voluntary basis and be kept current by the sub-
10 mitting business concerns.

11 (B) ATTESTATION.—Each business concern submitting informa-
12 tion to the registry shall submit—

13 (i) an attestation that the information is true; and

14 (ii) documentation supporting the attestation.

15 (C) VERIFICATION.—The Administrator shall verify that the
16 documentation submitted by each business concern supports the
17 information submitted by that business concern.

18 (4) AVAILABILITY.—The registry shall be made generally available
19 on the Internet site of the Agency.

20 (5) CONSULTATION OF REGISTRY AS PART OF ACQUISITION PLAN-
21 NING.—A Federal agency shall consult the registry as part of the ac-
22 quisition planning for contracting for debris removal, distribution of
23 supplies in a disaster, reconstruction, and other disaster or emergency
24 relief activities.

25 **§ 20707. Fraud prevention training program**

26 The Administrator shall develop and implement a program to provide
27 training on the prevention of waste, fraud, and abuse of Federal disaster
28 relief assistance relating to the response to or recovery from natural disas-
29 ters and acts of terrorism or other man-made disasters and ways to identify
30 potential waste, fraud, and abuse.

31 **Subtitle III— Port Security and**
32 **Accountability**
33 **Chapter 301—General**

Sec.

30101. Definitions.

34 **§ 30101. Definitions**

35 In this subtitle:

36 (1) APPROPRIATE CONGRESSIONAL COMMITTEES.—Except as other-
37 wise provided, the term “appropriate congressional committees”
38 means—

39 (A) the Committee on Appropriations of the Senate;

1 (B) the Committee on Commerce, Science, and Transportation
2 of the Senate;

3 (C) the Committee on Finance of the Senate;

4 (D) the Committee on Homeland Security and Governmental
5 Affairs of the Senate;

6 (E) the Committee on Appropriations of the House of Rep-
7 resentatives;

8 (F) the Committee on Homeland Security of the House of Rep-
9 resentatives;

10 (G) the Committee on Transportation and Infrastructure of the
11 House of Representatives;

12 (H) the Committee on Ways and Means of the House of Rep-
13 resentatives; and

14 (I) other congressional committees, as appropriate.

15 (2) COMMERCIAL OPERATIONS ADVISORY COMMITTEE.—The term
16 “Commercial Operations Advisory Committee” means the Advisory
17 Committee established under section 9503(c) of the Omnibus Budget
18 Reconciliation Act of 1987 (Public Law 100–203, 19 U.S.C. 2071
19 note) or any successor committee.

20 (3) COMMERCIAL SEAPORT PERSONNEL.—The term “commercial
21 seaport personnel” includes any person engaged in an activity relating
22 to the loading or unloading of cargo or passengers, the movement or
23 tracking of cargo, the maintenance and repair of intermodal equipment,
24 the operation of cargo-related equipment (whether or not integral to
25 the vessel), and the handling of mooring lines on the dock when a ves-
26 sel is made fast or let go in the United States.

27 (4) COMMISSIONER.—The term “Commissioner” means the Commis-
28 sioner responsible for U.S. Customs and Border Protection.

29 (5) CONTAINER.—The term “container” has the meaning given the
30 term in the International Convention for Safe Containers, with an-
31 nexes, done at Geneva, December 2, 1972 (29 UST 3707).

32 (6) CONTAINER SECURITY DEVICE.—The term “container security
33 device” means a device, or system—

34 (A) designed, at a minimum—

35 (i) to identify positively a container;

36 (ii) to detect and record unauthorized intrusion into a con-
37 tainer; and

38 (iii) to secure a container against tampering throughout
39 the supply chain; and

40 (B) that has a low false alarm rate, as determined by the Sec-
41 retary.

1 (7) DEPARTMENT.—The term “Department” means the Department
2 of Homeland Security.

3 (8) EXAMINATION.—The term “examination” means an inspection of
4 cargo to detect the presence of mis-declared, restricted, or prohibited
5 items that utilizes nonintrusive imaging and detection technology.

6 (9) INSPECTION.—The term “inspection” means the comprehensive
7 process used by U.S. Customs and Border Protection—

8 (A) to assess goods entering the United States to appraise them
9 for duty purposes, to detect the presence of restricted or prohib-
10 ited items, and to ensure compliance with all applicable laws; and

11 (B) that may include screening, conducting an examination, or
12 conducting a search.

13 (10) INTERNATIONAL SUPPLY CHAIN.—The term “international sup-
14 ply chain” means the end-to-end process for shipping goods to or from
15 the United States beginning at the point of origin (including manufac-
16 turer, supplier, or vendor) through a point of distribution to the des-
17 tination.

18 (11) RADIATION DETECTION EQUIPMENT.—The term “radiation de-
19 tection equipment” means any technology that is capable of detecting
20 or identifying nuclear and radiological material or nuclear and radio-
21 logical explosive devices.

22 (12) SCAN.—The term “scan” means utilizing nonintrusive imaging
23 equipment, radiation detection equipment, or both, to capture data, in-
24 cluding images of a container.

25 (13) SCREENING.—The term “screening” means a visual or auto-
26 mated review of information about goods, including manifest or entry
27 documentation accompanying a shipment being imported into the
28 United States, to determine the presence of mis-declared, restricted, or
29 prohibited items and assess the level of threat posed by the affected
30 cargo.

31 (14) SEARCH.—The term “search” means an intrusive examination
32 in which a container is opened and its contents are devanned and vis-
33 ually inspected for the presence of mis-declared, restricted, or prohib-
34 ited items.

35 (15) SECRETARY.—The term “Secretary” means the Secretary of
36 Homeland Security.

37 (16) TRANSPORTATION DISRUPTION.—The term “transportation dis-
38 ruption” means any significant delay, interruption, or stoppage in the
39 flow of trade caused by a natural disaster, heightened threat level, act
40 of terrorism, or transportation security incident.

1 (17) TRANSPORTATION SECURITY INCIDENT.—The term “transportation security incident” has the meaning given the term in section
 2 70101(6) of title 46.

4 **Chapter 303—Security of United States** 5 **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. Inspection of car ferries entering from abroad.

30306. Random searches of containers.

30307. Threat assessment screening of port truck drivers.

30308. Center of Excellence for Maritime Domain Awareness.

6 **§ 30301. Port Security Exercise Program**

7 (a) IN GENERAL.—The Secretary, acting through the Administrator of
 8 the Federal Emergency Management Agency and in coordination with the
 9 Commandant of the Coast Guard, shall establish a Port Security Exercise
 10 Program (in this section referred to as the “Exercise Program”) to test and
 11 evaluate the capabilities of Federal, State, local, and foreign governments,
 12 commercial seaport personnel and management, governmental and non-
 13 governmental emergency response providers, the private sector, or any other
 14 organization or entity, as the Secretary determines to be appropriate, to
 15 prevent, prepare for, mitigate against, respond to, and recover from acts of
 16 terrorism, natural disasters, and other emergencies at facilities required to
 17 submit a plan under section 70103(c) of title 46.

18 (b) REQUIREMENTS.—The Secretary shall ensure that the Exercise Pro-
 19 gram—

20 (1) conducts, on a periodic basis, port security exercises at the facili-
 21 ties that are—

22 (A) sealed and tailored to the needs of each facility;

23 (B) live, in the case of the most at-risk facilities;

24 (C) as realistic as practicable and based on current risk assess-
 25 ments, including credible threats, vulnerabilities, and con-
 26 sequences;

27 (D) consistent with the National Incident Management System,
 28 the National Response Plan, the National Infrastructure Protec-
 29 tion Plan, the National Preparedness Guidance, the National Pre-
 30 paredness Goal, the National Maritime Transportation Security
 31 Plan, and other national initiatives;

32 (E) evaluated against clear and consistent performance meas-
 33 ures;

34 (F) assessed to learn best practices, which shall be shared with
 35 appropriate Federal, State, and local officials, commercial seaport

1 personnel and management, governmental and nongovernmental
2 emergency response providers, and the private sector; and

3 (G) followed by remedial action in response to lessons learned;
4 and

5 (2) assists State and local governments and facilities in designing,
6 implementing, and evaluating exercises that—

7 (A) conform to the requirements of paragraph (1); and

8 (B) are consistent with any applicable Area Maritime Transporta-
9 tion Security Plan and State or Urban Area Homeland Security
10 Plan.

11 (c) IMPROVEMENT PLAN.—The Secretary shall establish a port security
12 exercise improvement plan process to—

13 (1) identify and analyze each port security exercise for lessons
14 learned and best practices;

15 (2) disseminate lessons learned and best practices to participants in
16 the Exercise Program;

17 (3) monitor the implementation of lessons learned and best practices
18 by participants in the Exercise Program; and

19 (4) conduct remedial action tracking and long-term trend analysis.

20 **§ 30302. Facility exercise requirements**

21 The Secretary of the Department in which the Coast Guard is operating
22 shall require each high-risk facility to conduct live or full-scale exercises de-
23 scribed in section 105.220(e) of title 33, Code of Federal Regulations, not
24 less frequently than once every 2 years, in accordance with the facility secu-
25 rity plan required under section 70103(e) of title 46.

26 **§ 30303. Domestic radiation detection and imaging**

27 (a) SCANNING CONTAINERS.—Subject to section 318 of the Tariff Act of
28 1930 (19 U.S.C. 1318), all containers entering the United States through
29 the 22 ports through which the greatest volume of containers enter the
30 United States by vessel shall be scanned for radiation. To the extent prac-
31 ticable, the Secretary shall deploy next-generation radiation detection tech-
32 nology.

33 (b) STRATEGY.—The Secretary shall develop and implement a strategy
34 for the deployment of radiation detection capabilities that includes—

35 (1) a risk-based prioritization of ports of entry at which radiation
36 detection equipment will be deployed;

37 (2) a proposed timeline of when radiation detection equipment will
38 be deployed at each port of entry identified under paragraph (1);

39 (3) the type of equipment to be used at each port of entry identified
40 under paragraph (1), including the joint deployment and utilization of
41 radiation detection equipment and nonintrusive imaging equipment;

1 (4) standard operating procedures for examining containers with the
2 equipment, including sensor alarming, networking, and communications
3 and response protocols;

4 (5) operator training plans;

5 (6) an evaluation of the environmental health and safety impacts of
6 nonintrusive imaging technology and a radiation risk reduction plan, in
7 consultation with the Nuclear Regulatory Commission, the Occupa-
8 tional Safety and Health Administration, and the National Institute for
9 Occupational Safety and Health, that seeks to minimize radiation expo-
10 sure of workers and the public to levels as low as reasonably achievable;

11 (7) the policy of the Department for using nonintrusive imaging
12 equipment in tandem with radiation detection equipment; and

13 (8) a classified annex that—

14 (A) details plans for covert testing; and

15 (B) outlines the risk-based prioritization of ports of entry iden-
16 tified under paragraph (1).

17 (c) EXPANSION TO OTHER UNITED STATES PORTS OF ENTRY.—

18 (1) IN GENERAL.—The Secretary shall expand the strategy devel-
19 oped under subsection (b), in a manner consistent with the require-
20 ments of subsection (b), to provide for the deployment of radiation de-
21 tection capabilities at all other United States ports of entry not covered
22 by the strategy developed under subsection (b).

23 (2) RISK ASSESSMENT.—In expanding the strategy under paragraph
24 (1), the Secretary shall identify and assess the risks to those other
25 ports of entry in order to determine what equipment and practices will
26 best mitigate the risks.

27 (d) STANDARDS.—The Secretary, acting through the Director for Domes-
28 tic Nuclear Detection and in collaboration with the National Institute of
29 Standards and Technology, shall publish technical capability standards and
30 recommended standard operating procedures for the use of nonintrusive im-
31 aging and radiation detection equipment in the United States. The stand-
32 ards and procedures—

33 (1) should take into account relevant standards and procedures uti-
34 lized by other Federal departments or agencies as well as those devel-
35 oped by international bodies; and

36 (2) shall not be designed so as to endorse specific companies or cre-
37 ate sovereignty conflicts with participating countries.

38 (e) INTERMODAL RAIL RADIATION DETECTION TEST CENTER.—

39 (1) ESTABLISHMENT.—In accordance with subsection (b), and to
40 comply with this section, the Secretary shall establish an Intermodal

1 Rail Radiation Detection Test Center (in this subsection referred to as
2 the “Test Center”).

3 (2) PROJECTS.—The Secretary shall conduct multiple, concurrent
4 projects at the Test Center to rapidly identify and test concepts specific
5 to the challenges posed by on-dock rail.

6 (3) LOCATION.—The Test Center shall be located in a public port
7 facility at which a majority of the containerized cargo is directly laden
8 from (or unladen to) on-dock, intermodal rail.

9 **§ 30304. Integration of detection equipment and tech-**
10 **nologies**

11 The Secretary is responsible for ensuring that domestic chemical, biologi-
12 cal, radiological, and nuclear detection equipment and technologies are inte-
13 grated, as appropriate, with other border security systems and detection
14 technologies.

15 **§ 30305. Inspection of car ferries entering from abroad**

16 The Secretary, acting through the Commissioner, in coordination with the
17 Secretary of State, and in cooperation with ferry operators and appropriate
18 foreign government officials, shall seek to develop a plan for the inspection
19 of passengers and vehicles before the passengers board, or the vehicles are
20 loaded onto, a ferry bound for a United States facility required to submit
21 a plan under section 70103(c) of title 46.

22 **§ 30306. Random searches of containers**

23 The Secretary, acting through the Commissioner, shall develop and imple-
24 ment a plan, utilizing best practices for empirical scientific research design
25 and random sampling, to conduct random searches of containers in addition
26 to any targeted or pre-shipment inspection of the containers required by law
27 or regulation or conducted under any other program conducted by the Sec-
28 retary. Nothing in this section shall be construed to mean that implementa-
29 tion of the random sampling plan precludes additional searches of con-
30 tainers not inspected pursuant to the plan.

31 **§ 30307. Threat assessment screening of port truck drivers**

32 The Secretary shall implement a threat assessment screening, including
33 name-based checks against terrorist watch lists and immigration status
34 checks, for all port truck drivers with access to secure areas of a port who
35 have a commercial driver’s license but do not have a current and valid haz-
36 ardous materials endorsement issued under part 1572 of title 49, Code of
37 Federal Regulations, that is the same as the threat assessment screening
38 required for facility employees and longshoremen by the Commandant of the
39 Coast Guard under Coast Guard Notice USCG-2006-24189 (71 Fed. Reg.
40 25066).

1 **§ 30308. 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 Provisions

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.

Subchapter II—Customs–Trade Partnership Against Terrorism

- 30511. Establishment.
- 30512. Eligible entities.
- 30513. Minimum requirements.
- 30514. Tier 1 participants.
- 30515. Tier 2 participants.
- 30516. Tier 3 participants.
- 30517. Consequences for lack of compliance.
- 30518. Revalidation.
- 30519. Noncontainerized cargo.
- 30520. Program management.

Subchapter III—Miscellaneous Provisions

- 30531. Screening and scanning of cargo containers.
- 30532. International cooperation and coordination.
- 30533. Information sharing relating to supply chain security cooperation.

Subchapter I—General Provisions

§ 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, as appropriate, 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

(12) expand on and relate to existing strategies and plans, including the National Response Plan, the National Maritime Transportation Se-

1 security Plan, the National Strategy for Maritime Security, and the 8
2 supporting plans of the Strategy, as required by Homeland Security
3 Presidential Directive–13.

4 (e) CONSULTATION.—In developing protocols under subsection (b)(10),
5 the Secretary shall consult with Federal, State, local, and private-sector
6 stakeholders, including the National Maritime Security Advisory Committee
7 and the Commercial Operations Advisory Committee.

8 (d) COMMUNICATION.—To the extent practicable, the strategic plan devel-
9 oped under subsection (a) shall provide for coordination with, and lines of
10 communication among, appropriate Federal, State, local, and private-sector
11 stakeholders on law enforcement actions, intermodal rerouting plans, and
12 other strategic infrastructure issues resulting from a transportation security
13 incident or transportation disruption.

14 (e) UTILIZATION OF ADVISORY COMMITTEES.—As part of the consulta-
15 tions described in subsection (a), the Secretary shall, to the extent prac-
16 ticable, utilize the Homeland Security Advisory Committee, the National
17 Maritime Security Advisory Committee, and the Commercial Operations Ad-
18 visory Committee to review, as necessary, the strategic plan and any subse-
19 quent updates to the strategic plan.

20 (f) INTERNATIONAL STANDARDS AND PRACTICES.—In furtherance of the
21 strategic plan required under subsection (a), the Secretary is encouraged to
22 consider proposed or established standards and practices of foreign govern-
23 ments and international organizations, including the International Maritime
24 Organization, the World Customs Organization, the International Labor Or-
25 ganization, and the International Organization for Standardization, as ap-
26 propriate, to establish standards and best practices for the security of con-
27 tainers moving through the international supply chain.

28 **§ 30502. Post-incident resumption of trade**

29 (a) IN GENERAL.—The Secretary shall develop and update, as necessary,
30 protocols for the resumption of trade under section 30501(b)(10) of this
31 title in the event of a transportation disruption or a transportation security
32 incident. The protocols shall include—

33 (1) the identification of the appropriate initial incident commander,
34 if the Commandant of the Coast Guard is not the appropriate indi-
35 vidual, and lead departments, agencies, or offices to execute the proto-
36 cols;

37 (2) a plan to redeploy resources and personnel, as necessary, to rees-
38 tablish the flow of trade;

39 (3) a plan to provide training for the periodic instruction of per-
40 sonnel of U.S. Customs and Border Protection, the Coast Guard, and

1 the Transportation Security Administration in trade resumption func-
2 tions and responsibilities; and

3 (4) appropriate factors for establishing prioritization of vessels and
4 cargo determined by the President to be critical for response and recov-
5 ery, including factors relating to public health, national security, and
6 economic need.

7 (b) VESSELS.—In determining the prioritization of vessels accessing fa-
8 cilities (as defined under section 70101 of title 46), the Commandant of the
9 Coast Guard may, to the extent practicable and consistent with the proto-
10 cols and plans required under this section to ensure the safe and secure
11 transit of vessels to ports in the United States after a transportation secu-
12 rity incident, give priority to a vessel—

13 (1) that has an approved security plan under section 70103(e) of
14 title 46, or a valid international ship security certificate, as provided
15 under part 104 of title 33, Code of Federal Regulations;

16 (2) that is manned by individuals who are described in section
17 70105(b)(2)(B) of title 46; and

18 (3) that is operated by validated participants in the Customs–Trade
19 Partnership Against Terrorism (in this chapter referred to as “C-
20 TPAT”) program.

21 (c) CARGO.—In determining the prioritization of the resumption of the
22 flow of cargo and consistent with the protocols established under this sec-
23 tion, the Commissioner may give preference to cargo—

24 (1) entering a port of entry directly from a foreign seaport des-
25 ignated under the Container Security Initiative;

26 (2) from the supply chain of a validated C–TPAT participant and
27 other private-sector entities, as appropriate; or

28 (3) that has undergone—

29 (A) a nuclear or radiological detection scan;

30 (B) an x-ray, density, or other imaging scan; and

31 (C) a system to positively identify the container at the last port
32 of departure prior to arrival in the United States, which data has
33 been evaluated and analyzed by personnel of U.S. Customs and
34 Border Protection.

35 (d) COORDINATION.—The Secretary shall ensure that there is appropriate
36 coordination among the Commandant of the Coast Guard, the Commis-
37 sioner, and other Federal officials following a maritime disruption or mari-
38 time transportation security incident in order to provide for the resumption
39 of trade.

40 (e) COMMUNICATION.—Consistent with section 30501 of this title, the
41 Commandant of the Coast Guard, the Commissioner, and other appropriate

1 Federal officials shall promptly communicate any revised procedures or in-
2 structions intended for the private sector following a maritime disruption or
3 maritime transportation security incident.

4 **§ 30503. Automated targeting system**

5 (a) IN GENERAL.—The Secretary, acting through the Commissioner,
6 shall—

7 (1) identify and seek the submission of data related to the movement
8 of a shipment of cargo through the international supply chain; and

9 (2) analyze the data described in paragraph (1) to identify high-risk
10 cargo for inspection.

11 (b) REQUIREMENT.—The Secretary, acting through the Commissioner,
12 shall require the electronic transmission to the Department of additional
13 data elements for improved high-risk targeting, including appropriate secu-
14 rity elements of entry data, as determined by the Secretary, to be provided
15 as advanced information with respect to cargo destined for importation into
16 the United States prior to loading of the cargo on vessels at foreign sea-
17 ports.

18 (c) CONSIDERATION.—The Secretary, acting through the Commissioner,
19 shall—

20 (1) consider the cost, benefit, and feasibility of—

21 (A) requiring additional non-manifest documentation;

22 (B) reducing the time period allowed by law for revisions to a
23 container cargo manifest;

24 (C) reducing the time period allowed by law for submission of
25 certain elements of entry data, for vessel or cargo; and

26 (D) other actions the Secretary considers beneficial for improv-
27 ing the information relied on for the Automated Targeting System
28 and any successor targeting system in furthering the security and
29 integrity of the international supply chain; and

30 (2) consult with stakeholders, including the Commercial Operations
31 Advisory Committee, and identify to them the need for the information
32 referred to in paragraph (1)(D), and the appropriate timing of its sub-
33 mission.

34 (d) REGULATIONS.—The Secretary shall promulgate regulations to carry
35 out this section. In promulgating regulations, the Secretary shall adhere to
36 the parameters applicable to the development of regulations under section
37 343(a) of the Trade Act of 2002 (Public Law 107–210, 19 U.S.C. 2071
38 note), including provisions relating to consultation, technology, analysis, use
39 of information, confidentiality, and timing requirements.

40 (e) SYSTEM IMPROVEMENTS.—The Secretary, acting through the Com-
41 missioner, shall—

1 (1) conduct, through an independent panel, a review of the effective-
2 ness and capabilities of the Automated Targeting System;

3 (2) consider future iterations of the Automated Targeting System,
4 which would incorporate smart features, such as more complex algo-
5 rithms and real-time intelligence, instead of relying solely on rule sets
6 that are periodically updated;

7 (3) ensure that the Automated Targeting System has the capability
8 to electronically compare manifest and other available data for cargo
9 entered into or bound for the United States to detect any significant
10 anomalies between the data and facilitate the resolution of the anom-
11 alies;

12 (4) ensure that the Automated Targeting System has the capability
13 to electronically identify, compile, and compare select data elements for
14 cargo entered into or bound for the United States following a maritime
15 transportation security incident, in order to efficiently identify cargo
16 for increased inspection or expeditious release; and

17 (5) develop a schedule to address the recommendations of the Comp-
18 troller General, the Inspector General of the Department of the Treas-
19 ury, and the Inspector General of the Department with respect to the
20 operation of the Automated Targeting System.

21 (f) SECURE TRANSMISSION OF CERTAIN INFORMATION.—All information
22 required by the Department from supply chain partners shall be transmitted
23 in a secure fashion, as determined by the Secretary, so as to protect the
24 information from unauthorized access.

25 **§ 30504. Container security standards and procedures**

26 (a) ESTABLISHMENT.—

27 (1) IN GENERAL.—The Secretary shall initiate a rulemaking pro-
28 ceeding to establish minimum standards and procedures for securing
29 containers in transit to the United States.

30 (2) DEADLINE FOR ENFORCEMENT.—

31 (A) ENFORCEMENT OF RULE.—Not later than 2 years after the
32 date on which the standards and procedures are established under
33 paragraph (1), all containers bound for ports of entry in the
34 United States shall meet the standards and procedures.

35 (B) INTERIM REQUIREMENT.—If an interim final rule issued
36 pursuant to the proceeding described in paragraph (1) was not
37 issued by April 1, 2008—

38 (i) all containers in transit to the United States are re-
39 quired to meet the requirements of International Organization
40 for Standardization Publicly Available Specification 17712
41 standard for sealing containers; and

1 (ii) the requirements of this subparagraph cease to be ef-
2 fective on the effective date of the interim final rule issued
3 under this subsection.

4 (b) REVIEW AND ENHANCEMENT.—The Secretary shall regularly review
5 and enhance the standards and procedures established under subsection (a),
6 as appropriate, based on tests of technologies as they become commercially
7 available to detect container intrusion and the highest consequence threats,
8 particularly weapons of mass destruction.

9 (c) INTERNATIONAL CARGO SECURITY STANDARDS.—The Secretary, in
10 consultation with the Secretary of State, the Secretary of Energy, and other
11 Federal Government officials, as appropriate, and with the Commercial Op-
12 erations Advisory Committee, the Homeland Security Advisory Committee,
13 and the National Maritime Security Advisory Committee, is encouraged to
14 promote and establish international standards for the security of containers
15 moving through the international supply chain with foreign governments
16 and international organizations, including the International Maritime Orga-
17 nization, the International Organization for Standardization, the Inter-
18 national Labor Organization, and the World Customs Organization.

19 (d) INTERNATIONAL TRADE AND OTHER OBLIGATIONS.—In carrying out
20 this section, the Secretary shall consult with appropriate Federal depart-
21 ments and agencies and private-sector stakeholders and ensure that actions
22 under this section do not violate international trade obligations or other
23 international obligations of the United States.

24 **§ 30505. Container Security Initiative**

25 (a) ESTABLISHMENT.—The Secretary, acting through the Commissioner,
26 shall establish and implement a program (in this section referred to as the
27 “Container Security Initiative”) to identify and examine or search maritime
28 containers that pose a security risk before loading the containers in a for-
29 eign port for shipment to the United States, either directly or through a
30 foreign port.

31 (b) ASSESSMENT.—The Secretary, acting through the Commissioner, may
32 designate foreign seaports to participate in the Container Security Initiative
33 after the Secretary has assessed the costs, benefits, and other factors associ-
34 ated with the designation, including—

35 (1) the level of risk for the potential compromise of containers by
36 terrorists, or other threats as determined by the Secretary;

37 (2) the volume of cargo being imported to the United States directly
38 from, or being trans-shipped through, the foreign seaport;

39 (3) the results of the Coast Guard assessments conducted under sec-
40 tion 70108 of title 46;

1 (4) the commitment of the government of the country in which the
2 foreign seaport is located to cooperating with the Department in shar-
3 ing critical data and risk management information and to maintain
4 programs to ensure employee integrity; and

5 (5) the potential for validation of security practices at the foreign
6 seaport by the Department.

7 (e) NOTIFICATION.—The Secretary shall notify the appropriate congres-
8 sional committees of the designation of a foreign port under the Container
9 Security Initiative or the revocation of a designation before notifying the
10 public of the designation or revocation.

11 (d) NEGOTIATIONS.—The Secretary, in cooperation with the Secretary of
12 State and in consultation with the United States Trade Representative, may
13 enter into negotiations with the government of each foreign nation in which
14 a seaport is designated under the Container Security Initiative to ensure full
15 compliance with the requirements under the Container Security Initiative.

16 (e) OVERSEAS INSPECTIONS.—

17 (1) REQUIREMENTS AND PROCEDURES.—The Secretary shall—

18 (A) establish minimum technical capability criteria and standard
19 operating procedures for the use of nonintrusive inspection and
20 nuclear and radiological detection systems in conjunction with the
21 Container Security Initiative;

22 (B) require each port designated under the Container Security
23 Initiative to operate nonintrusive inspection and nuclear and radio-
24 logical detection systems in accordance with the technical capa-
25 bility criteria and standard operating procedures established under
26 subparagraph (A);

27 (C) continually monitor the technologies, processes, and tech-
28 niques used to inspect cargo at ports designated under the Con-
29 tainer Security Initiative to ensure adherence to the criteria and
30 the use of the procedures; and

31 (D) consult with the Secretary of Energy in establishing the
32 minimum technical capability criteria and standard operating pro-
33 cedures established under subparagraph (A) pertaining to radi-
34 ation detection technologies to promote consistency in detection
35 systems at foreign ports designated under the Container Security
36 Initiative.

37 (2) CONSTRAINTS.—The criteria and procedures established under
38 paragraph (1)(A)—

39 (A) shall be consistent, as practicable, with relevant standards
40 and procedures utilized by other Federal departments or agencies,

1 or developed by international bodies if the United States consents
2 to the standards and procedures;

3 (B) shall not apply to activities conducted under the Megaports
4 Initiative of the Department of Energy; and

5 (C) shall not be designed to endorse the product or technology
6 of any specific company or to conflict with the sovereignty of a
7 country in which a foreign seaport designated under the Container
8 Security Initiative is located.

9 (f) SAVINGS PROVISION.—The authority of the Secretary under this sec-
10 tion shall not affect any authority or duplicate any efforts or responsibilities
11 of the Federal Government with respect to the deployment of radiation de-
12 tection equipment outside of the United States.

13 (g) COORDINATION.—The Secretary shall—

14 (1) coordinate with the Secretary of Energy, as necessary, to provide
15 radiation detection equipment required to support the Container Secu-
16 rity Initiative through the Department of Energy’s Second Line of De-
17 fense Program and Megaports Initiative; or

18 (2) work with the private sector or host governments, when possible,
19 to obtain radiation detection equipment that meets the Department’s
20 and the Department of Energy’s technical specifications for the equip-
21 ment.

22 (h) STAFFING.—The Secretary shall develop a human capital manage-
23 ment plan to determine adequate staffing levels in the United States and
24 in foreign seaports including, as appropriate, the remote location of per-
25 sonnel in countries in which foreign seaports are designated under the Con-
26 tainer Security Initiative.

27 (i) ANNUAL DISCUSSIONS.—The Secretary, in coordination with the ap-
28 propriate Federal officials, shall hold annual discussions with foreign gov-
29 ernments of countries in which foreign seaports designated under the Con-
30 tainer Security Initiative are located regarding best practices, technical as-
31 sistance, training needs, and technological developments that will assist in
32 ensuring the efficient and secure movement of international cargo.

33 (j) LESSER RISK PORT.—The Secretary, acting through the Commis-
34 sioner, may treat cargo loaded in a foreign seaport designated under the
35 Container Security Initiative as presenting a lesser risk than similar cargo
36 loaded in a foreign seaport that is not designated under the Container Secu-
37 rity Initiative, for the purpose of clearing the cargo into the United States.

38 (k) PROHIBITION.—

39 (1) IN GENERAL.—The Secretary shall issue a “do not load” order,
40 using existing authorities, to prevent the onload of any cargo loaded
41 at a port designated under the Container Security Initiative that has

1 been identified as high risk, including by the Automated Targeting Sys-
 2 tem, unless the cargo is determined to no longer be high risk
 3 through—

4 (A) a scan of the cargo with nonintrusive imaging equipment
 5 and radiation detection equipment;

6 (B) a search of the cargo; or

7 (C) additional information received by the Department.

8 (2) RULE OF CONSTRUCTION.—Nothing in this subsection shall be
 9 construed to interfere with the ability of the Secretary to deny entry
 10 of any cargo into the United States.

11 (l) COORDINATION OF ASSESSMENTS.—

12 (1) IN GENERAL.—The Secretary shall, to the extent practicable,
 13 conduct the assessments required by the following provisions of law
 14 concurrently, or develop a process by which the assessments are coordi-
 15 nated between the Coast Guard and U.S. Customs and Border Protec-
 16 tion:

17 (A) This section.

18 (B) Section 30513 of this title.

19 (C) Section 70108 of title 46.

20 (2) LIMITATION.—Nothing in paragraph (1) shall be construed to af-
 21 fect or diminish the Secretary’s authority or discretion—

22 (A) to conduct an assessment of a foreign port at any time;

23 (B) to compel the Secretary to conduct an assessment of a for-
 24 eign port so as to ensure that 2 or more assessments are con-
 25 ducted concurrently; or

26 (C) to cancel an assessment of a foreign port if the Secretary
 27 is unable to conduct 2 or more assessments concurrently.

28 (3) MULTIPLE ASSESSMENT REPORT.—The Secretary shall provide
 29 written notice to the Committee on Commerce, Science, and Transpor-
 30 tation of the Senate and the Committees on Transportation and Infra-
 31 structure and Homeland Security of the House of Representatives
 32 whenever the Secretary conducts 2 or more assessments of the same
 33 port within a 3-year period.

34 **Subchapter II—Customs–Trade** 35 **Partnership Against Terrorism**

36 **§ 30511. Establishment**

37 (a) IN GENERAL.—The Secretary, acting through the Commissioner, may
 38 establish a voluntary government-private sector program (to be known as
 39 the “Customs-Trade Partnership Against Terrorism” or “C-TPAT”) to
 40 strengthen and improve the overall security of the international supply chain
 41 and United States border security, and to facilitate the movement of secure

1 cargo through the international supply chain, by providing benefits to par-
2 ticipants meeting or exceeding the program requirements. Participants in
3 C-TPAT shall include Tier 1 participants, Tier 2 participants, and Tier 3
4 participants.

5 (b) REVIEW OF MINIMUM SECURITY REQUIREMENTS.—The Secretary,
6 acting through the Commissioner, shall review the minimum security re-
7 quirements of C-TPAT at least once every year and update requirements
8 as necessary.

9 **§ 30512. Eligible entities**

10 Importers, customs brokers, forwarders, air, sea, and land carriers, con-
11 tract logistics providers, and other entities in the international supply chain
12 and intermodal transportation system are eligible to apply to voluntarily
13 enter into partnerships with the Department under C-TPAT.

14 **§ 30513. Minimum requirements**

15 An applicant seeking to participate in C-TPAT shall—

16 (1) demonstrate a history of moving cargo in the international sup-
17 ply chain;

18 (2) conduct an assessment of its supply chain based upon security
19 criteria established by the Secretary, acting through the Commissioner,
20 including—

21 (A) business partner requirements;

22 (B) container security;

23 (C) physical security and access controls;

24 (D) personnel security;

25 (E) procedural security;

26 (F) security training and threat awareness; and

27 (G) information technology security;

28 (3) implement and maintain security measures and supply chain se-
29 curity practices meeting security criteria established by the Commis-
30 sioner; and

31 (4) meet all other requirements established by the Commissioner, in
32 consultation with the Commercial Operations Advisory Committee.

33 **§ 30514. Tier 1 participants**

34 (a) BENEFITS.—The Secretary, acting through the Commissioner, shall
35 offer limited benefits to a Tier 1 participant who has been certified in ac-
36 cordance with the guidelines referred to in subsection (b). Benefits may in-
37 clude a reduction in the score assigned pursuant to the Automated Tar-
38 geting System of not greater than 20 percent of the high-risk threshold es-
39 tablished by the Secretary.

40 (b) GUIDELINES.—The Secretary, acting through the Commissioner, shall
41 update the guidelines for certifying a C-TPAT participant's security meas-

1 ures and supply chain security practices under this section. The guidelines
2 shall include a background investigation and extensive documentation re-
3 view.

4 (e) TIMEFRAME.—To the extent practicable, the Secretary, acting
5 through the Commissioner, shall complete the Tier 1 certification process
6 within 90 days of receipt of an application for participation in C-TPAT.

7 **§ 30515. Tier 2 participants**

8 (a) VALIDATION.—The Secretary, acting through the Commissioner, shall
9 validate the security measures and supply chain security practices of a Tier
10 1 participant in accordance with the guidelines referred to in subsection (e).
11 The validation shall include on-site assessments at appropriate foreign loca-
12 tions utilized by the Tier 1 participant in its supply chain and shall, to the
13 extent practicable, be completed not later than 1 year after certification as
14 a Tier 1 participant.

15 (b) BENEFITS.—The Secretary, acting through the Commissioner, shall
16 extend benefits to each C-TPAT participant that has been validated as a
17 Tier 2 participant under this section, which may include—

- 18 (1) reduced scores in the Automated Targeting System;
- 19 (2) reduced examinations of cargo; and
- 20 (3) priority searches of cargo.

21 (c) GUIDELINES.—The Secretary, acting through the Commissioner, shall
22 develop a schedule and update the guidelines for validating a participant's
23 security measures and supply chain security practices under this section.

24 **§ 30516. Tier 3 participants**

25 (a) IN GENERAL.—The Secretary, acting through the Commissioner, shall
26 establish a third tier of C-TPAT participation that offers additional bene-
27 fits to participants who demonstrate a sustained commitment to maintain-
28 ing security measures and supply chain security practices that exceed the
29 guidelines established for validation as a Tier 2 participant in C-TPAT
30 under section 30515 of this title.

31 (b) CRITERIA.—The Secretary, acting through the Commissioner, shall
32 designate criteria for validating a C-TPAT participant as a Tier 3 partici-
33 pant under this section. Criteria may include—

- 34 (1) compliance with any additional guidelines established by the Sec-
35 retary that exceed the guidelines established under section 30515 of
36 this title for validating a C-TPAT participant as a Tier 2 participant,
37 particularly with respect to controls over access to cargo throughout
38 the supply chain;
- 39 (2) submission of additional information regarding cargo prior to
40 loading, as determined by the Secretary;

1 (3) utilization of container security devices, technologies, policies, or
2 practices that meet standards and criteria established by the Secretary;
3 and

4 (4) compliance with any other cargo requirements established by the
5 Secretary.

6 (c) BENEFITS.—The Secretary, acting through the Commissioner, in con-
7 sultation with the Commercial Operations Advisory Committee and the Na-
8 tional Maritime Security Advisory Committee, shall extend benefits to each
9 C-TPAT participant that has been validated as a Tier 3 participant under
10 this section, which may include—

11 (1) the expedited release of a Tier 3 participant’s cargo in destina-
12 tion ports within the United States during all threat levels designated
13 by the Secretary;

14 (2) further reduction in examinations of cargo;

15 (3) priority for examinations of cargo; and

16 (4) further reduction in the risk score assigned pursuant to the
17 Automated Targeting System; and

18 (5) inclusion in joint incident management exercises, as appropriate.

19 **§ 30517. Consequences for lack of compliance**

20 (a) IN GENERAL.—If at any time a C-TPAT participant’s security meas-
21 ures and supply chain security practices fail to meet any of the require-
22 ments under this subchapter, the Commissioner may deny the participant
23 benefits otherwise available under this subchapter in whole or in part. The
24 Commissioner shall develop procedures that provide appropriate protections
25 to C-TPAT participants before benefits are revoked. The procedures may
26 not limit the ability of the Commissioner to take actions to protect the na-
27 tional security of the United States.

28 (b) FALSE OR MISLEADING INFORMATION.—If a C-TPAT participant
29 knowingly provides false or misleading information to the Commissioner
30 during the validation process provided for under this subchapter, the Com-
31 missioner shall suspend or expel the participant from C-TPAT for an ap-
32 propriate period of time. The Commissioner, after the completion of the
33 process under subsection (c), may publish in the Federal Register a list of
34 participants who have been suspended or expelled from C-TPAT under this
35 subsection, and may make the list available to C-TPAT participants.

36 (c) RIGHT OF APPEAL.—

37 (1) APPEAL OF DENIAL OF BENEFITS.—A C-TPAT participant may
38 appeal a decision of the Commissioner under subsection (a). The appeal
39 shall be filed with the Secretary not later than 90 days after the date
40 of the decision, and the Secretary shall issue a determination not later
41 than 180 days after the appeal is filed.

(2) APPEALS OF SUSPENSION OR EXPULSION.—A C-TPAT participant may appeal a decision of the Commissioner under subsection (b). The appeal shall be filed with the Secretary not later than 30 days after the date of the decision, and the Secretary shall issue a determination not later than 180 days after the appeal is filed.

§ 30518. Revalidation

The Secretary, acting through the Commissioner, shall develop and implement—

(1) a revalidation process for Tier 2 and Tier 3 participants;

(2) a framework based upon objective criteria for identifying participants for periodic revalidation not less frequently than once during each 4-year period following the initial validation; and

(3) an annual plan for revalidation that includes—

(A) performance measures;

(B) an assessment of the personnel needed to perform the revalidations; and

(C) the number of participants that will be revalidated during the following year.

§ 30519. Noncontainerized cargo

The Secretary, acting through the Commissioner, shall consider the potential for participation in C-TPAT by importers of noncontainerized cargoes that otherwise meet the requirements under this subchapter.

§ 30520. Program management

(a) IN GENERAL.—The Secretary, acting through the Commissioner, shall establish sufficient internal quality controls and record management to support the management systems of C-TPAT. In managing the program, the Secretary shall ensure that the program includes the following:

(1) A 5-year plan to identify outcome-based goals and performance measures of the program.

(2) An annual plan for each fiscal year designed to match available resources to the projected workload.

(3) A standardized work program to be used by agency personnel to carry out the certifications, validations, and revalidations of participants. The Secretary shall keep records and monitor staff hours associated with the completion of each review.

(b) DOCUMENTATION OF REVIEWS.—The Secretary, acting through the Commissioner, shall maintain a record management system to document determinations on the reviews of each C-TPAT participant, including certifications, validations, and revalidations.

(c) CONFIDENTIAL INFORMATION SAFEGUARDS.—In consultation with the Commercial Operations Advisory Committee, the Secretary, acting

1 through the Commissioner, shall develop and implement procedures to en-
 2 sure the protection of confidential data collected, stored, or shared with gov-
 3 ernment agencies or as part of the application, certification, validation, and
 4 revalidation processes.

5 (d) RESOURCE MANAGEMENT STAFFING PLAN.—The Secretary, acting
 6 through the Commissioner, shall—

7 (1) develop a staffing plan to recruit and train staff (including a for-
 8 malized training program) to meet the objectives identified in the stra-
 9 tegic plan of the C-TPAT program; and

10 (2) provide cross-training in post-incident trade resumption for per-
 11 sonnel who administer the C-TPAT program.

12 (e) REPORT TO CONGRESS.—In connection with the President’s annual
 13 budget submission for the Department, the Secretary shall report to the ap-
 14 propriate congressional committees on the progress made by the Commis-
 15 sioner to certify, validate, and revalidate C-TPAT participants. The report
 16 shall be due on the same date that the President’s budget is submitted to
 17 the Congress.

18 **Subchapter III—Miscellaneous Provisions**

19 **§ 30531. Screening and scanning of cargo containers**

20 (a) ONE HUNDRED PERCENT SCREENING OF CARGO CONTAINERS AND
 21 100 PERCENT SCANNING OF HIGH-RISK CONTAINERS.—

22 (1) SCREENING OF CARGO CONTAINERS.—The Secretary shall ensure
 23 that 100 percent of the cargo containers originating outside the United
 24 States and unloaded at a United States seaport undergo a screening
 25 to identify high-risk containers

26 (2) SCANNING OF HIGH-RISK CONTAINERS.—The Secretary shall en-
 27 sure that 100 percent of the containers that have been identified as
 28 high-risk under paragraph (1), or through other means, are scanned
 29 or searched before the containers leave a United States seaport facility.

30 (b) FULL-SCALE IMPLEMENTATION.—

31 (1) IN GENERAL.—A container that was loaded on a vessel in a for-
 32 eign port shall not enter the United States (either directly or via a for-
 33 eign port) unless the container was scanned by nonintrusive imaging
 34 equipment and radiation detection equipment at a foreign port before
 35 it was loaded on a vessel.

36 (2) APPLICATION.—Paragraph (1) shall apply with respect to con-
 37 tainers loaded on a vessel in a foreign country on or after the earlier
 38 of—

39 (A) July 1, 2012; or

40 (B) another date established by the Secretary under paragraph

41 (3).

1 (3) ESTABLISHMENT OF EARLIER DEADLINE.—The Secretary shall
2 establish a date under paragraph (2)(B) pursuant to the lessons
3 learned through the pilot integrated scanning systems established
4 under section 231 of the Security and Accountability For Every Port
5 Act of 2006 (or SAFE Port Act) (Public Law 109–347, 120 Stat.
6 1915).

7 (4) EXTENSIONS.—The Secretary may extend the date specified in
8 subparagraph (A) or (B) of paragraph (2) for 2 years, and may renew
9 the extension in additional 2-year increments, for containers loaded in
10 a port or ports, if the Secretary certifies to Congress that at least 2
11 of the following conditions exist:

12 (A) Systems to scan containers under paragraph (1) are not
13 available for purchase and installation.

14 (B) Systems to scan containers under paragraph (1) do not
15 have a sufficiently low false alarm rate for use in the supply chain.

16 (C) Systems to scan containers under paragraph (1) cannot be
17 purchased, deployed, or operated at ports overseas, including, if
18 applicable, because a port does not have the physical characteris-
19 tics to install a system.

20 (D) Systems to scan containers under paragraph (1) cannot be
21 integrated, as necessary, with existing systems.

22 (E) Use of systems that are available to scan containers under
23 paragraph (1) will significantly impact trade capacity and the flow
24 of cargo.

25 (F) Systems to scan containers under paragraph (1) do not ade-
26 quately provide an automated notification of questionable or high-
27 risk cargo as a trigger for further inspection by appropriately
28 trained personnel.

29 (5) EXEMPTION FOR MILITARY CARGO.—Notwithstanding any other
30 provision of this section, supplies bought by the Secretary of Defense
31 and transported in compliance with section 2631 of title 10 and mili-
32 tary cargo of foreign countries are exempt from the requirements of
33 this section.

34 (6) REPORT ON EXTENSIONS.—An extension under paragraph (4)
35 for a port takes effect on the expiration of the 60-day period beginning
36 on the date the Secretary provides a report to Congress that—

37 (A) states what container traffic will be affected by the exten-
38 sion;

39 (B) provides supporting evidence to support the Secretary’s cer-
40 tification of the basis for the extension; and

1 (C) explains what measures the Secretary is taking to ensure
2 that scanning can be implemented as early as possible at the port
3 or ports that are the subject of the report.

4 (7) REPORT ON RENEWAL OF EXTENSION.—If an extension under
5 paragraph (4) takes effect, the Secretary shall, after 1 year, submit a
6 report to Congress on whether the Secretary expects to seek to renew
7 the extension.

8 (8) SCANNING TECHNOLOGY STANDARDS.—In implementing para-
9 graph (1), the Secretary shall—

10 (A) establish technological and operational standards for sys-
11 tems to scan containers;

12 (B) ensure that the standards are consistent with the global nu-
13 clear detection architecture developed under the Homeland Secu-
14 rity Act of 2002 (Public Law 107–296, 116 Stat. 2135); and

15 (C) coordinate with other Federal agencies that administer
16 scanning or detection programs at foreign ports.

17 (9) INTERNATIONAL TRADE AND OTHER OBLIGATIONS.—In carrying
18 out this subsection, the Secretary shall consult with appropriate Fed-
19 eral departments and agencies and private-sector stakeholders, and en-
20 sure that actions under this section do not violate international trade
21 obligations, and are consistent with the World Customs Organization
22 framework, or other international obligations of the United States.

23 (c) REPORT.—Not later than 6 months after the submission of a report
24 under section 231(d) of the Security and Accountability For Every Port Act
25 of 2006 (or SAFE Port Act) (Public Law 109–347, 120 Stat. 1916), and
26 every 6 months thereafter, the Secretary shall submit a report to the appri-
27 priate congressional committees describing the status of full-scale deploy-
28 ment under subsection (b) and the cost of deploying the system at each fore-
29 eign port at which the integrated scanning systems are deployed.

30 **§ 30532. International cooperation and coordination**

31 (a) INSPECTION TECHNOLOGY AND TRAINING.—The Secretary, in coordi-
32 nation with the Secretary of State, the Secretary of Energy, and appri-
33 priate representatives of other Federal agencies, may provide technical as-
34 sistance, equipment, and training to facilitate the implementation of supply
35 chain security measures at ports designated under the Container Security
36 Initiative.

37 (b) ACQUISITION AND TRAINING.—Unless otherwise prohibited by law,
38 the Secretary may—

39 (1) lease, lend, provide, or otherwise assist in the deployment of non-
40 intrusive inspection and radiation detection equipment at foreign land
41 and sea ports under terms and conditions the Secretary prescribes, in-

cluding nonreimbursable loans or the transfer of ownership of equipment; and

(2) provide training and technical assistance for domestic or foreign personnel responsible for operating or maintaining the equipment.

§ 30533. Information sharing relating to supply chain security cooperation

(a) PURPOSES.—The purposes of this section are—

(1) to establish continuing liaison and to provide for supply chain security cooperation between the Department and the private sector; and

(2) to provide for regular and timely interchange of information between the private sector and the Department concerning developments and security risks in the supply chain environment.

(b) DEVELOPMENT OF SYSTEM.—The Secretary shall develop a system to collect from, and share appropriate risk information relating to the supply chain with, the private-sector entities determined appropriate by the Secretary.

(c) CONSULTATION.—In developing the system under subsection (b), the Secretary shall consult with the Commercial Operations Advisory Committee and a broad range of public- and private-sector entities likely to utilize the system, including importers, exporters, carriers, customs brokers, and freight forwarders, among other parties.

(d) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section shall be construed to limit or otherwise affect the ability of a Federal, State, or local government entity, under applicable law, to obtain supply chain security information, including information lawfully and properly disclosed generally or broadly to the public, and to use the information in any manner permitted by law.

(e) AUTHORITY TO ISSUE WARNINGS.—The Secretary may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential risks to the supply chain as appropriate. In issuing a warning, the Secretary shall take appropriate actions to protect from disclosure—

(1) the source of any voluntarily submitted supply chain security information that forms the basis for the warning; and

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

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.

1 **§ 30701. Designation of liaison office of Department of State**

2 The Secretary of State shall designate a liaison office in the Department
3 of State to assist the Secretary, as appropriate, in negotiating cargo secu-
4 rity-related international agreements.

5 **§ 30702. Homeland Security Science and Technology Advi-**
6 **sory Committee**

7 The Under Secretary for Science and Technology shall utilize the Home-
8 land Security Science and Technology Advisory Committee, as appropriate,
9 to provide outside expertise in advancing cargo security technology.

10 **§ 30703. Research, development, test, and evaluation efforts**
11 **in furtherance of maritime and cargo security**

12 (a) IN GENERAL.—The Secretary shall—

13 (1) direct research, development, testing, and evaluation efforts in
14 furtherance of maritime and cargo security;

15 (2) coordinate with public- and private-sector entities to develop and
16 test technologies, and process innovations in furtherance of these objec-
17 tives; and

18 (3) evaluate the technologies.

19 (b) COORDINATION.—The Secretary, in coordination with the Under Sec-
20 retary for Science and Technology, the Assistant Secretary for Policy, the
21 Commandant of the Coast Guard, the Director for Domestic Nuclear Detec-
22 tion, the Chief Financial Officer, and the heads of other appropriate offices
23 or entities of the Department, shall ensure that—

24 (1) research, development, testing, and evaluation efforts funded by
25 the Department in furtherance of maritime and cargo security are co-
26 ordinated within the Department and with other appropriate Federal
27 agencies to avoid duplication of efforts; and

28 (2) the results of the efforts are shared throughout the Department
29 and with other Federal, State, and local agencies, as appropriate.

30 **Subtitle IV—Transportation Security**
31 **Chapter 401—General**

Sec.

40101. Definitions.

32 **§ 40101. Definitions**

33 (a) DEPARTMENT.—In chapters 403 through 407 of this title, the term
34 “Department” means the Department of Homeland Security.

35 (b) SECRETARY.—In this subtitle, the term “Secretary” means the Sec-
36 retary of Homeland Security.

37 **Chapter 403—Transportation Security**
38 **Planning, Information Sharing, and En-**
39 **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 response.

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. Roles of the Department and the Department of Transportation.

**Subchapter I—Security Planning and
Information Sharing**

§ 40301. National Domestic Preparedness Consortium

(a) IN GENERAL.—The Secretary may establish, operate, and maintain a National Domestic Preparedness Consortium in the Department.

(b) MEMBERS.—The National Domestic Preparedness Consortium consists of—

(1) the Center for Domestic Preparedness;

(2) the National Energetic Materials Research and Testing Center, New Mexico Institute of Mining and Technology;

(3) the National Center for Biomedical Research and Training, Louisiana State University

(4) the National Emergency Response and Rescue Training Center, Texas A&M University;

(5) the National Exercise, Test, and Training Center, Nevada Test Site;

(6) the Transportation Technology Center, Incorporated, in Pueblo, Colorado; and

(7) the National Disaster Preparedness Training Center, University of Hawaii.

(c) DUTIES.—The National Domestic Preparedness Consortium shall identify, develop, test, and deliver training to State, local, and tribal emergency response providers, provide on-site and mobile training at the performance and management and planning levels, and facilitate the delivery of training by the training partners of the Department.

§ 40302. National Transportation Security Center of Excellence

(a) ESTABLISHMENT.—The Secretary shall establish a National Transportation Security Center of Excellence to conduct research and education activities, and to develop or provide professional security training, including the training of transportation employees and transportation professionals.

1 (b) DESIGNATION.—The Secretary shall select one of the institutions
2 identified in subsection (c) as the lead institution responsible for coordi-
3 nating the National Transportation Security Center of Excellence.

4 (c) MEMBER INSTITUTIONS.—

5 (1) CONSORTIUM.—The institution of higher education selected
6 under subsection (b) shall execute agreements with the other institu-
7 tions of higher education identified in this subsection and other institu-
8 tions designated by the Secretary to develop a consortium to assist in
9 accomplishing the goals of the Center.

10 (2) MEMBERS.—The National Transportation Security Center of Ex-
11 cellence consists of—

12 (A) Texas Southern University in Houston, Texas;

13 (B) the National Transit Institute at Rutgers, The State Uni-
14 versity of New Jersey;

15 (C) Tougaloo College;

16 (D) the Connecticut Transportation Institute at the University
17 of Connecticut;

18 (E) the Homeland Security Management Institute, Long Island
19 University;

20 (F) the Mack-Blackwell National Rural Transportation Study
21 Center at the University of Arkansas; and

22 (G) any additional institutions or facilities designated by the
23 Secretary.

24 (3) CERTAIN INCLUSIONS.—To the extent practicable, the Secretary
25 shall ensure that an appropriate number of additional consortium col-
26 leges or universities designated by the Secretary under this subsection
27 are Historically Black Colleges and Universities, Hispanic Serving In-
28 stitutions, and Indian Tribally Controlled Colleges and Universities.

29 **§ 40303. Immunity for reports of suspected terrorist activity**
30 **or suspicious behavior and response**

31 (a) DEFINITIONS.—In this section:

32 (1) AUTHORIZED OFFICIAL.—The term “authorized official”
33 means—

34 (A) an employee or agent of a passenger transportation system
35 or other person with responsibilities relating to the security of the
36 system;

37 (B) an officer, employee, or agent of the Department, the De-
38 partment of Transportation, or the Department of Justice with re-
39 sponsibilities relating to the security of passenger transportation
40 systems; or

41 (C) a Federal, State, or local law enforcement officer.

1 (2) COVERED ACTIVITY.—The term “covered activity” means a sus-
 2 picious transaction, activity, or occurrence that involves, or is directed
 3 against, a passenger transportation system or vehicle or its passengers
 4 indicating that an individual may be engaging, or preparing to engage,
 5 in a violation of law relating to—

6 (A) a threat to a passenger transportation system or passenger
 7 safety or security; or

8 (B) an act of terrorism (as that term is defined in section 3077
 9 of title 18.

10 (3) PASSENGER TRANSPORTATION.—The term “passenger transpor-
 11 tation” means—

12 (A) public transportation, as defined in section 5302 of title 49;

13 (B) transportation by an over-the-road bus, as described in sec-
 14 tion 40701 of this title, and school bus transportation;

15 (C) intercity rail passenger transportation, as defined in section
 16 24102 of title 49;

17 (D) the transportation of passengers onboard a passenger ves-
 18 sel, as defined in section 2101 of title 46;

19 (E) other regularly scheduled waterborne transportation service
 20 of passengers by a vessel of at least 20 gross tons; and

21 (F) air transportation, as defined in section 40102 of title 49,
 22 of passengers.

23 (4) PASSENGER TRANSPORTATION SYSTEM.—The term “passenger
 24 transportation system” means an entity or entities organized to provide
 25 passenger transportation using vehicles, including the infrastructure
 26 used to provide the transportation.

27 (5) VEHICLE.—The term “vehicle” has the meaning given the term
 28 in section 1992(d)(16) of title 18.

29 (b) IMMUNITY FOR REPORTS OF SUSPECTED TERRORIST ACTIVITY OR
 30 SUSPICIOUS BEHAVIOR.—

31 (1) IN GENERAL.—A person who, in good faith and based on objec-
 32 tively reasonable suspicion, makes, or causes to be made, a voluntary
 33 report of covered activity to an authorized official shall be immune
 34 from civil liability under Federal, State, and local law for the report.

35 (2) FALSE REPORTS.—Paragraph (1) shall not apply to any report
 36 that the person knew to be false or was made with reckless disregard
 37 for the truth at the time that person made that report.

38 (c) IMMUNITY FOR RESPONSE.—

39 (1) IN GENERAL.—An authorized official who observes, or receives
 40 a report of, covered activity and takes reasonable action in good faith
 41 to respond to the activity has qualified immunity from civil liability for

1 the action, consistent with applicable law in the relevant jurisdiction.
 2 An authorized official (as defined by subsection (a)(1)(A)) not entitled
 3 to assert the defense of qualified immunity is immune from civil liability
 4 under Federal, State, and local law if the authorized official takes
 5 reasonable action, in good faith, to respond to the reported activity.

6 (2) SAVINGS CLAUSE.—Nothing in this subsection affects the ability
 7 of an authorized official to assert any defense, privilege, or immunity
 8 that would otherwise be available, and this subsection shall not be con-
 9 strued as affecting the defense, privilege, or immunity.

10 (d) ATTORNEY FEES AND COSTS.—A person or authorized official found
 11 to be immune from civil liability under this section is entitled to recover
 12 from the plaintiff all reasonable costs and attorney fees.

13 **Subchapter II—Security Enhancements**

14 **§ 40311. Definitions**

15 In this subchapter:

16 (1) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term “appro-
 17 priate congressional committee” means the Committee on Commerce,
 18 Science, and Transportation, the Committee on Banking, Housing, and
 19 Urban Affairs and the Committee on Homeland Security and Govern-
 20 mental Affairs of the Senate and the Committee on Homeland Security
 21 and the Committee on Transportation and Infrastructure of the House.

22 (2) STATE.—The term “State” means a State, the District of Co-
 23 lumbia, Puerto Rico, the Northern Mariana Islands, the Virgin Islands,
 24 Guam, American Samoa, and any other territory (including a posses-
 25 sion) of the United States.

26 (3) TERRORISM.—The term “terrorism” has the meaning given the
 27 term in section 10101 of this title.

28 (4) UNITED STATES.—The term “United States” means the States,
 29 the District of Columbia, Puerto Rico, the Northern Mariana Islands,
 30 the Virgin Islands, Guam, American Samoa, and any other territory
 31 (including a possession) of the United States.

32 **§ 40312. Authorization of Visible Intermodal Prevention and** 33 **Response teams**

34 (a) IN GENERAL.—The Secretary, acting through the Administrator of
 35 the Transportation Security Administration, may develop Visible Intermodal
 36 Prevention and Response (in this section referred to as “VIPR”) teams to
 37 augment the security of any mode of transportation at any location within
 38 the United States. In forming a VIPR team, the Secretary—

39 (1) may use any asset of the Department, including Federal air mar-
 40 shals, surface transportation security inspectors, canine detection
 41 teams, and advanced screening technology;

1 (2) may determine when a VIPR team shall be deployed, as well as
2 the duration of the deployment;

3 (3) shall, prior to and during the deployment, consult with local se-
4 curity and law enforcement officials in the jurisdiction where the VIPR
5 team is or will be deployed, to develop and agree upon the appropriate
6 operational protocols and provide relevant information about the mis-
7 sion of the VIPR team, as appropriate;

8 (4) shall, prior to and during the deployment, consult with all trans-
9 portation entities directly affected by the deployment of a VIPR team,
10 as appropriate, including railroad carriers, air carriers, airport owners,
11 over-the-road bus operators and terminal owners and operators, motor
12 carriers, public transportation agencies, owners or operators of high-
13 ways, port operators and facility owners, vessel owners and operators,
14 and pipeline operators; and

15 (5) shall require, as appropriate based on risk, in the case of a VIPR
16 team deployed to an airport, that the VIPR team conduct operations—

17 (A) in the sterile area and any other areas to which only indi-
18 viduals issued security credentials have unrestricted access; and

19 (B) in nonsterile areas.

20 (b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be
21 appropriated to the Secretary to carry out this section such sums as nec-
22 essary, including funds to develop not more than 60 VIPR teams, for fiscal
23 years 2016 through 2018.

24 **§ 40313. Surface transportation security inspectors**

25 (a) IN GENERAL.—The Secretary, acting through the Administrator of
26 the Transportation Security Administration, may train, employ, and utilize
27 surface transportation security inspectors.

28 (b) MISSION.—The Secretary shall use surface transportation security in-
29 spectors to assist surface transportation carriers, operators, owners, entities,
30 and facilities to enhance their security against terrorist attack and other se-
31 curity threats and to assist the Secretary in enforcing applicable surface
32 transportation security regulations and directives.

33 (c) AUTHORITIES.—Surface transportation security inspectors employed
34 under this section shall be authorized powers and delegated responsibilities
35 that the Secretary determines appropriate, subject to subsection (e).

36 (d) REQUIREMENTS.—The Secretary shall require that surface transpor-
37 tation security inspectors have relevant transportation experience and other
38 security and inspection qualifications, as determined appropriate.

39 (e) LIMITATIONS.—

40 (1) INSPECTORS.—Surface transportation inspectors shall be prohib-
41 ited from issuing fines to public transportation agencies (as defined in

1 section 40501 of this title) for violations of the Department's regula-
2 tions or orders except through the process described in paragraph (2).

3 (2) CIVIL PENALTIES.—The Secretary shall be prohibited from as-
4 sessing civil penalties against public transportation agencies (as defined
5 in section 40501 of this title) for violations of the Department's regula-
6 tions or orders, except in accordance with the following:

7 (A) In the case of a public transportation agency that is found
8 to be in violation of a regulation or order issued by the Secretary,
9 the Secretary shall seek correction of the violation through a writ-
10 ten notice to the public transportation agency and shall give the
11 public transportation agency reasonable opportunity to correct the
12 violation or propose an alternative means of compliance acceptable
13 to the Secretary.

14 (B) If the public transportation agency does not correct the vio-
15 lation or propose an alternative means of compliance acceptable to
16 the Secretary within a reasonable time period that is specified in
17 the written notice, the Secretary may take any action authorized
18 in sections 11301 through 11316 of this title.

19 (3) LIMITATION ON SECRETARY.—The Secretary shall not initiate
20 civil enforcement actions for violations of administrative and procedural
21 requirements pertaining to the application for, and expenditure of,
22 funds awarded under transportation security grant programs under the
23 Implementing Recommendations of the 9/11 Commission Act of 2007
24 (Public Law 110–53, 121 Stat. 266).

25 (f) COORDINATION.—The Secretary shall ensure that the mission of the
26 surface transportation security inspectors is consistent with any relevant
27 risk assessments required by the Implementing Recommendations of the 9/
28 11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 266) or com-
29 pleted by the Department, the modal plans required under section 11314
30 of this title, the Memorandum of Understanding between the Department
31 and the Department of Transportation on Roles and Responsibilities, dated
32 September 28, 2004, and all subsequent annexes to this Memorandum of
33 Understanding, and other relevant documents setting forth the Depart-
34 ment's transportation security strategy, as appropriate.

35 (g) CONSULTATION.—The Secretary shall periodically consult with the
36 surface transportation entities that are or may be inspected by the surface
37 transportation security inspectors, including, as appropriate, railroad car-
38 riers, over-the-road bus operators and terminal owners and operators, motor
39 carriers, public transportation agencies, owners or operators of highways,
40 and pipeline operators on—

1 (1) the inspectors' duties, responsibilities, authorities, and mission;
2 and

3 (2) strategies to improve transportation security and to ensure com-
4 pliance with transportation security requirements.

5 **§ 40314. Surface transportation security technology infor-**
6 **mation sharing**

7 (a) IN GENERAL.—

8 (1) INFORMATION SHARING.—The Secretary, in consultation with
9 the Secretary of Transportation, shall establish a program to provide
10 appropriate information that the Department has gathered or devel-
11 oped on the performance, use, and testing of technologies that may be
12 used to enhance railroad, public transportation, and surface transpor-
13 tation security to surface transportation entities, including railroad car-
14 riers, over-the-road bus operators and terminal owners and operators,
15 motor carriers, public transportation agencies, owners or operators of
16 highways, pipeline operators, and State, local, and tribal governments
17 that provide security assistance to the entities.

18 (2) DESIGNATION OF QUALIFIED ANTITERRORISM TECHNOLOGIES.—
19 The Secretary shall include in the information provided in paragraph
20 (1) whether the technology is designated as a qualified antiterrorism
21 technology under subchapter IV of chapter 105 of this title, as appro-
22 priate.

23 (b) PURPOSE.—The purpose of the program is to assist eligible grant re-
24 cipients under this subtitle and others, as appropriate, to purchase and use
25 the best technology and equipment available to meet the security needs of
26 the Nation's surface transportation system.

27 (c) COORDINATION.—The Secretary shall ensure that the program estab-
28 lished under this section makes use of and is consistent with other Depart-
29 ment technology testing, information sharing, evaluation, and standards-set-
30 ting programs, as appropriate.

31 **§ 40315. Transportation Security Administration personnel**
32 **limitations**

33 Any statutory limitation on the number of employees in the Transpor-
34 tation Security Administration does not apply to employees carrying out this
35 chapter, chapters 401, 405, and 407 of this title, and titles XII through
36 XV of the Implementing Recommendations of the 9/11 Commission Act of
37 2007 (Public Law 110–53, 121 Stat. 381).

38 **§ 40316. National explosives detection canine team training**
39 **program**

40 (a) DEFINITION OF EXPLOSIVES DETECTION CANINE TEAM.—In this
41 section, the term “explosives detection canine team” means a canine and a

1 canine handler that are trained to detect explosives, radiological materials,
2 chemical, nuclear or biological weapons, or other threats as defined by the
3 Secretary.

4 (b) IN GENERAL.—

5 (1) INCREASED CAPACITY.—The Secretary shall—

6 (A) begin to increase the number of explosives detection canine
7 teams certified by the Transportation Security Administration for
8 the purposes of transportation-related security by up to 200 ca-
9 nine teams annually by the end of 2010; and

10 (B) encourage State, local, and tribal governments and private
11 owners of high-risk transportation facilities to strengthen security
12 through the use of highly trained explosives detection canine
13 teams.

14 (2) WAYS TO INCREASE NUMBER OF EXPLOSIVES DETECTION CA-
15 NINE TEAMS.—The Secretary shall increase the number of explosives
16 detection canine teams by—

17 (A) using the Transportation Security Administration’s Na-
18 tional Explosives Detection Canine Team Training Center, includ-
19 ing expanding and upgrading existing facilities, procuring and
20 breeding additional canines, and increasing staffing and oversight
21 commensurate with the increased training and deployment capa-
22 bilities;

23 (B) partnering with other Federal, State, or local agencies, non-
24 profit organizations, universities, or the private sector to increase
25 the training capacity for canine detection teams;

26 (C) procuring explosives detection canines trained by nonprofit
27 organizations, universities, or the private sector, provided they are
28 trained in a manner consistent with the standards and require-
29 ments developed under subsection (c) or other criteria developed
30 by the Secretary; or

31 (D) a combination of subparagraphs (A), (B), and (C), as ap-
32 propriate.

33 (c) STANDARDS FOR EXPLOSIVES DETECTION CANINE TEAMS.—

34 (1) IN GENERAL.—Based on the feasibility in meeting the ongoing
35 demand for quality explosives detection canine teams, the Secretary
36 shall establish criteria, including canine training curricula, performance
37 standards, and other requirements approved by the Transportation Se-
38 curity Administration necessary to ensure that explosives detection ca-
39 nine teams trained by nonprofit organizations, universities, and private-
40 sector entities are adequately trained and maintained.

1 (2) EXPANSION.—In developing and implementing the curricula, per-
2 formance standards, and other requirements, the Secretary shall—

3 (A) coordinate with key stakeholders, including international,
4 Federal, State, and local officials, and private-sector and academic
5 entities to develop best practice guidelines for a standardized pro-
6 gram, as appropriate;

7 (B) require that explosives detection canine teams trained by
8 nonprofit organizations, universities, or private-sector entities that
9 are used or made available by the Secretary be trained consistent
10 with specific training criteria developed by the Secretary; and

11 (C) review the status of the private-sector programs on at least
12 an annual basis to ensure compliance with training curricula, per-
13 formance standards, and other requirements.

14 (d) DEPLOYMENT.—The Secretary shall—

15 (1) use the additional explosives detection canine teams as part of
16 the Department’s efforts to strengthen security across the Nation’s
17 transportation network, and may use the canine teams on a more lim-
18 ited basis to support other homeland security missions, as determined
19 appropriate by the Secretary;

20 (2) make available explosives detection canine teams to all modes of
21 transportation, for high-risk areas or to address specific threats, on an
22 as-needed basis and as otherwise determined appropriate by the Sec-
23 retary;

24 (3) encourage, but not require, any transportation facility or system
25 to deploy TSA-certified explosives detection canine teams developed
26 under this section; and

27 (4) consider specific needs and training requirements for explosives
28 detection canine teams to be deployed across the Nation’s transpor-
29 tation network, including in venues of multiple modes of transportation,
30 as appropriate.

31 (e) CANINE PROCUREMENT.—The Secretary, acting through the Adminis-
32 trator of the Transportation Security Administration, shall work to ensure
33 that explosives detection canine teams are procured as efficiently as possible
34 and at the best price, while maintaining the needed level of quality, includ-
35 ing, if appropriate, through increased domestic breeding.

36 **§ 40317. Roles of the Department and the Department of**
37 **Transportation**

38 (a) IN GENERAL.—The Secretary is the principal Federal official respon-
39 sible for transportation security.

40 (b) EQUIVALENT ROLES AND RESPONSIBILITIES.—In carrying out this
41 chapter, chapters 401, 405, and 407 of this title, and titles XII through

1 XV of the Implementing Recommendations of the 9/11 Commission Act of
 2 2007 (Public Law 110–53, 121 Stat. 381), the roles and responsibilities of
 3 the Department and the Department of Transportation are the same as
 4 their roles and responsibilities under the following:

5 (1) The Aviation and Transportation Security Act (Public Law
 6 107–71, 115 Stat. 597).

7 (2) The Intelligence Reform and Terrorism Prevention Act of
 8 2004 (Public Law 108–458, 118 Stat. 3638).

9 (3) The National Infrastructure Protection Plan required by
 10 Homeland Security Presidential Directive–7.

11 (4) The Homeland Security Act of 2002 (Public Law 107–296,
 12 116 Stat. 2135).

13 (5) The National Response Plan.

14 (6) Executive Order No. 13416, 71 Fed. Reg. 71033 (Dec. 5,
 15 2006).

16 (7) The Memorandum of Understanding between the Depart-
 17 ment of Homeland Security and the Department of Transporta-
 18 tion on Roles and Responsibilities, dated September 28, 2004,
 19 and any and all subsequent annexes to this Memorandum of Un-
 20 derstanding and other relevant agreements between the two De-
 21 partments.

22 **Chapter 405—Public Transportation** 23 **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. Public transportation security training program.

40507. Public transportation research and development.

40508. Information sharing.

40509. Reporting requirements.

40510. Public transportation employee protections.

40511. Security background checks of covered individuals for public transportation.

40512. Limitation on fines and civil penalties.

24 **§ 40501. Definitions**

25 In this chapter:

26 (1) **APPROPRIATE CONGRESSIONAL COMMITTEE.**—The term “appro-
 27 priate congressional committee” means the Committee on Banking,
 28 Housing, and Urban Affairs and the Committee on Homeland Security
 29 and Governmental Affairs of the Senate and the Committee on Home-
 30 land Security and the Committee on Transportation and Infrastructure
 31 of the House.

32 (2) **DISADVANTAGED BUSINESS CONCERN.**—The term “disadvan-
 33 tagged business concern” means a small business that is owned and con-

1 trolled by socially and economically disadvantaged individuals as de-
2 fined in part 124, title 13, Code of Federal Regulations.

3 (3) FRONTLINE EMPLOYEE.—The term “frontline employee” means
4 an employee of a public transportation agency who is a transit vehicle
5 driver or operator, dispatcher, maintenance or maintenance support
6 employee, station attendant, customer service employee, security em-
7 ployee, or transit police employee, or any other employee who has direct
8 contact with riders on a regular basis, or any other employee of a pub-
9 lic transportation agency that the Secretary determines should receive
10 security training under section 40506 of this title.

11 (4) PUBLIC TRANSPORTATION AGENCY.—The term “public transpor-
12 tation agency” means a publicly owned operator of public transpor-
13 tation eligible to receive Federal assistance under chapter 53 of title
14 49.

15 **§ 40502. National Strategy for Public Transportation Secu-**
16 **urity**

17 (a) NATIONAL STRATEGY.—Based on the previous and ongoing security
18 assessments conducted by the Department and the Department of Trans-
19 portation, the Secretary, consistent with and as required by section 11314
20 of this title, shall develop and implement the modal plan for public transpor-
21 tation, entitled the “National Strategy for Public Transportation Security”
22 (in this section referred to as the “Strategy”).

23 (b) PURPOSE.—

24 (1) GUIDELINES.—In developing the Strategy, the Secretary shall es-
25 tablish guidelines for public transportation security that—

26 (A) minimize security threats to public transportation systems;
27 and

28 (B) maximize the abilities of public transportation systems to
29 mitigate damage resulting from a terrorist attack or other major
30 incident.

31 (2) ASSESSMENTS AND CONSULTATIONS.—In developing the Strat-
32 egy, the Secretary shall—

33 (A) use established and ongoing public transportation security
34 assessments as the basis of the Strategy; and

35 (B) consult with all relevant stakeholders, including public
36 transportation agencies, nonprofit labor organizations representing
37 public transportation employees, emergency responders, public
38 safety officials, and other relevant parties.

39 (c) CONTENTS.—In the Strategy, the Secretary shall describe prioritized
40 goals, objectives, policies, actions, and schedules to improve the security of
41 public transportation.

1 (d) RESPONSIBILITIES.—The Secretary shall include in the Strategy a de-
2 scription of the roles, responsibilities, and authorities of Federal, State, and
3 local agencies, tribal governments, and appropriate stakeholders. The Strat-
4 egy shall also include—

5 (1) the identification of, and a plan to address, gaps and unneces-
6 sary overlaps in the roles, responsibilities, and authorities of Federal
7 agencies; and

8 (2) a process for coordinating existing or future security strategies
9 and plans for public transportation, including—

10 (A) the National Infrastructure Protection Plan required by
11 Homeland Security Presidential Directive–7;

12 (B) Executive Order No. 13416, 71 Fed. Reg. 71033 (Dec. 5,
13 2006); and

14 (C) the Memorandum of Understanding between the Depart-
15 ment and the Department of Transportation on Roles and Respon-
16 sibilities dated September 28, 2004, and subsequent annexes and
17 agreements.

18 (e) ADEQUACY OF EXISTING PLANS AND STRATEGIES.—In developing the
19 Strategy, the Secretary shall use relevant existing risk assessments and
20 strategies developed by the Department or other Federal agencies, including
21 those developed or implemented under section 11314 of this title or Home-
22 land Security Presidential Directive–7.

23 **§ 40503. Security assessments and plans**

24 (a) PUBLIC TRANSPORTATION SECURITY ASSESSMENTS.—

25 (1) SUBMISSION.—The Administrator of the Federal Transit Admin-
26 istration shall submit all public transportation security assessments and
27 all other relevant information to the Secretary.

28 (2) SECRETARIAL REVIEW.—Not later than 60 days after receiving
29 the submission under paragraph (1), the Secretary shall review and
30 augment the security assessments received, and conduct additional se-
31 curity assessments as necessary to ensure that at a minimum, all high
32 risk public transportation agencies, as determined by the Secretary, will
33 have a completed security assessment.

34 (3) CONTENT.—The Secretary shall ensure that each completed se-
35 curity assessment includes—

36 (A) identification of critical assets, infrastructure, and systems,
37 and their vulnerabilities; and

38 (B) identification of any other security weaknesses, including
39 weaknesses in emergency response planning and employee train-
40 ing.

1 (b) BUS AND RURAL PUBLIC TRANSPORTATION SYSTEMS.—The Sec-
2 retary shall—

3 (1) conduct security assessments, based on a representative sample,
4 to determine the specific needs of—

5 (A) local bus-only public transportation systems; and

6 (B) public transportation systems that receive funds under sec-
7 tion 5311 of title 49; and

8 (2) make the representative assessments available for use by simi-
9 larly situated systems.

10 (c) SECURITY PLANS.—

11 (1) REQUIREMENT FOR PLAN.—

12 (A) HIGH RISK AGENCIES.—The Secretary shall require public
13 transportation agencies determined by the Secretary to be at high
14 risk for terrorism to develop a comprehensive security plan. The
15 Secretary shall provide technical assistance and guidance to public
16 transportation agencies in preparing and implementing security
17 plans under this section.

18 (B) OTHER AGENCIES.—Subject to subparagraph (C), the Sec-
19 retary may also establish a security program for public transpor-
20 tation agencies not designated high risk by the Secretary, to assist
21 those public transportation agencies that request assistance, in-
22 cluding—

23 (i) guidance to assist agencies in conducting security as-
24 sessments and preparing and implementing security plans;
25 and

26 (ii) a process for the Secretary to review and approve as-
27 sessments and plans, as appropriate.

28 (C) PLAN NOT REQUIRED.—A public transportation agency that
29 has not been designated high risk may not be required to develop
30 a security plan.

31 (2) CONTENT.—The Secretary shall ensure that security plans in-
32 clude, as appropriate—

33 (A) a prioritized list of all items included in the public transpor-
34 tation agency's security assessment that have not yet been ad-
35 dressed;

36 (B) a detailed list of any additional capital and operational im-
37 provements identified by the Department or the public transpor-
38 tation agency and a certification of the public transportation agen-
39 cy's technical capacity for operating and maintaining security
40 equipment that may be identified in the list;

1 (C) specific procedures to be implemented or used by the public
2 transportation agency in response to a terrorist attack, including
3 evacuation and passenger communication plans and appropriate
4 evacuation and communication measures for the elderly and indi-
5 viduals with disabilities;

6 (D) a coordinated response plan that establishes procedures for
7 appropriate interaction with State and local law enforcement agen-
8 cies, emergency responders, and Federal officials in order to co-
9 ordinate security measures and plans for response in the event of
10 a terrorist attack or other major incident;

11 (E) a strategy and timeline for conducting training under sec-
12 tion 40506 of this title;

13 (F) plans for providing redundant and other appropriate backup
14 systems necessary to ensure the continued operation of critical ele-
15 ments of the public transportation system in the event of a ter-
16 rorist attack or other major incident;

17 (G) plans for providing service capabilities throughout the sys-
18 tem in the event of a terrorist attack or other major incident in
19 the city or region which the public transportation system serves;

20 (H) methods to mitigate damage within a public transportation
21 system in case of an attack on the system, including a plan for
22 communication and coordination with emergency responders; and

23 (I) other actions or procedures as the Secretary determines are
24 appropriate to address the security of the public transportation
25 system.

26 (3) REVIEW.—Not later than 6 months after receiving the plans re-
27 quired under this section, the Secretary shall—

28 (A) review each security plan submitted;

29 (B) require the public transportation agency to make any
30 amendments needed to ensure that the plan meets the require-
31 ments of this section; and

32 (C) approve any security plan that meets the requirements of
33 this section.

34 (4) EXEMPTION.—The Secretary may not require a public transpor-
35 tation agency to develop a security plan under paragraph (1) if the
36 agency does not receive a grant under section 40504 of this title.

37 (5) WAIVER.—The Secretary may waive the exemption provided in
38 paragraph (4) to require a public transportation agency to develop a
39 security plan under paragraph (1) in the absence of grant funds under
40 section 40504 of this title if not less than 3 days after making the de-
41 termination the Secretary provides the appropriate congressional com-

1 mittees and the public transportation agency written notification detail-
2 ing the need for the security plan, the reasons grant funding has not
3 been made available, and the reason the agency has been designated
4 high risk.

5 (d) CONSISTENCY WITH OTHER PLANS.—The Secretary shall ensure that
6 the security plans developed by public transportation agencies under this
7 section are consistent with the security assessments developed by the De-
8 partment and the National Strategy for Public Transportation Security de-
9 veloped under section 40502 of this title.

10 (e) UPDATES.—The Secretary annually shall—

11 (1) update the security assessments referred to in subsection (a);

12 (2) update the security improvement priorities required under sub-
13 section (f); and

14 (3) require public transportation agencies to update the security
15 plans required under subsection (e), as appropriate.

16 (f) SECURITY IMPROVEMENT PRIORITIES.—

17 (1) IN GENERAL.—Each fiscal year, the Secretary, after consultation
18 with management and nonprofit employee labor organizations rep-
19 resenting public transportation employees, as appropriate, and with ap-
20 propriate State and local officials, shall utilize the information devel-
21 oped or received in this section to establish security improvement prior-
22 ities unique to each individual public transportation agency that has
23 been assessed.

24 (2) ALLOCATIONS.—The Secretary shall use the security improve-
25 ment priorities established in paragraph (1) as the basis for allocating
26 risk-based grant funds under section 40504 of this title, unless the Sec-
27 retary notifies the appropriate congressional committees that the Sec-
28 retary has determined an adjustment is necessary to respond to an ur-
29 gent threat or other significant national security factors.

30 (g) SHARED FACILITIES.—The Secretary shall encourage the development
31 and implementation of coordinated assessments and security plans to the ex-
32 tent a public transportation agency shares facilities (such as tunnels,
33 bridges, stations, or platforms) with another public transportation agency,
34 a freight or passenger railroad carrier, or over-the-road bus operator that
35 is geographically close or otherwise co-located.

36 (h) NONDISCLOSURE OF INFORMATION.—

37 (1) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this
38 section shall be construed as authorizing the withholding of any infor-
39 mation from Congress.

40 (2) DISCLOSURE OF INDEPENDENTLY FURNISHED INFORMATION.—

41 Nothing in this section shall be construed as affecting any authority

1 or obligation of a Federal agency to disclose any record or information
2 that the Federal agency obtains from a public transportation agency
3 under any other Federal law.

4 (i) DETERMINATION.—In response to a petition by a public transpor-
5 tation agency or at the discretion of the Secretary, the Secretary may recog-
6 nize existing procedures, protocols, and standards of a public transportation
7 agency that the Secretary determines meet all or part of the requirements
8 of this section regarding security assessments or security plans.

9 **§ 40504. Public transportation security improvement grants**

10 (a) SECURITY ASSISTANCE PROGRAM.—

11 (1) IN GENERAL.—The Secretary shall establish a program for mak-
12 ing grants to eligible public transportation agencies for security im-
13 provements described in subsection (b).

14 (2) ELIGIBILITY.—A public transportation agency is eligible for a
15 grant under this section if the Secretary has performed a security as-
16 sessment or the agency has developed a security plan under section
17 40503 of this title. Grant funds shall only be awarded for permissible
18 uses under subsection (b) to—

- 19 (A) address items included in a security assessment; or
20 (B) further a security plan.

21 (b) USES OF FUNDS.—A recipient of a grant under subsection (a) shall
22 use the grant funds for one or more of the following:

23 (1) CAPITAL USES OF FUNDS, INCLUDING—

- 24 (A) tunnel protection systems;
25 (B) perimeter protection systems, including access control, in-
26 stallation of improved lighting, fencing, and barricades;
27 (C) redundant critical operations control systems;
28 (D) chemical, biological, radiological, or explosive detection sys-
29 tems, including the acquisition of canines used for detection;
30 (E) surveillance equipment;
31 (F) communications equipment, including mobile service equip-
32 ment to provide access to wireless Enhanced 911 (E911) emer-
33 gency services in an underground fixed guideway system;
34 (G) emergency response equipment, including personal protec-
35 tive equipment;
36 (H) fire suppression and decontamination equipment;
37 (I) global positioning or tracking and recovery equipment, and
38 other automated-vehicle-locator-type system equipment;
39 (J) evacuation improvements;

1 (K) purchase and placement of bomb-resistant trash cans
 2 throughout public transportation facilities, including subway exits,
 3 entrances, and tunnels;

4 (L) capital costs associated with security awareness, security
 5 preparedness, and security response training, including training
 6 under section 40506 of this title and exercises under section
 7 40505 of this title;

8 (M) security improvements for public transportation systems,
 9 including extensions thereto, in final design or under construction;

10 (N) security improvements for stations and other public trans-
 11 portation infrastructure, including stations and other public trans-
 12 portation infrastructure owned by State or local governments; and

13 (O) other capital security improvements determined appropriate
 14 by the Secretary.

15 (2) OPERATING USES OF FUNDS, INCLUDING—

16 (A) security training, including training under section 40506 of
 17 this title and training developed by institutions of higher education
 18 and by nonprofit employee labor organizations, for public trans-
 19 portation employees, including frontline employees;

20 (B) live or simulated exercises under section 40505 of this title;

21 (C) public awareness campaigns for enhanced public transpor-
 22 tation security;

23 (D) canine patrols for chemical, radiological, biological, or explo-
 24 sives detection;

25 (E) development of security plans under section 40503 of this
 26 title;

27 (F) overtime reimbursement including reimbursement of State,
 28 local, and tribal governments, for costs for enhanced security per-
 29 sonnel during significant national and international public events;

30 (G) operational costs, including reimbursement of State, local,
 31 and tribal governments for costs for personnel assigned to full-
 32 time or part-time security or counterterrorism duties related to
 33 public transportation, provided that this expense totals no more
 34 than 10 percent of the total grant funds received by a public
 35 transportation agency in any 1 year; and

36 (H) other operational security costs determined appropriate by
 37 the Secretary, excluding routine, ongoing personnel costs, other
 38 than those set forth in this section.

39 (c) SECRETARY'S RESPONSIBILITIES.—In carrying out the responsibilities
 40 under subsection (a), the Secretary shall—

1 (1) determine the requirements for recipients of grants under this
2 section, including application requirements;

3 (2) under subsection (a)(2), select the recipients of grants based
4 solely on risk; and

5 (3) under subsection (b), establish the priorities for which grant
6 funds may be used under this section.

7 (d) DISTRIBUTION OF GRANTS.—The Secretary and the Secretary of
8 Transportation shall determine the most effective and efficient way to dis-
9 tribute grant funds to the recipients of grants determined by the Secretary
10 under subsection (a). Subject to the determination made by the Secretaries,
11 the Secretary may transfer funds to the Secretary of Transportation for the
12 purposes of disbursing funds to the grant recipient.

13 (e) GRANT SUBJECT TO CERTAIN TERMS AND CONDITIONS.—Except as
14 otherwise specifically provided in this section, a grant provided under this
15 section is subject to the terms and conditions applicable to a grant made
16 under section 5307 of title 49, as in effect on January 1, 2007, and other
17 terms and conditions determined necessary by the Secretary.

18 (f) LIMITATION ON USES OF FUNDS.—Grants made under this section
19 may not be used to make any State or local government cost-sharing con-
20 tribution under any other Federal law.

21 (g) ANNUAL REPORTS.—Each recipient of a grant under this section
22 shall report annually to the Secretary on the use of the grant funds.

23 (h) GUIDELINES ON USE OF CONTRACTORS AND SUBCONTRACTORS.—
24 Before the distribution of funds to recipients of grants, the Secretary shall
25 issue guidelines to ensure that, to the extent that recipients of grants under
26 this section use contractors or subcontractors, the recipients shall use small,
27 minority, women-owned, or disadvantaged business concerns as contractors
28 or subcontractors to the extent practicable.

29 (i) COORDINATION WITH STATE HOMELAND SECURITY PLANS.—In es-
30 tablishing security improvement priorities under section 40503 of this title
31 and in awarding grants for capital security improvements and operational
32 security improvements under subsection (b), the Secretary shall act consist-
33 ently with relevant State homeland security plans.

34 (j) MULTISTATE TRANSPORTATION SYSTEMS.—In cases in which a public
35 transportation system operates in more than one State, the Secretary shall
36 give appropriate consideration to the risks of the entire system, including
37 those portions of the States into which the system crosses, in establishing
38 security improvement priorities under section 40503 of this title and in
39 awarding grants for capital security improvements and operational security
40 improvements under subsection (b).

1 (k) CONGRESSIONAL NOTIFICATION.—Not later than 3 days before the
2 award of any grant under this section, the Secretary shall notify simulta-
3 neously the appropriate congressional committees of the intent to award the
4 grant.

5 (l) RETURN OF MISSPENT GRANT FUNDS.—The Secretary shall establish
6 a process to require the return of any misspent grant funds received under
7 this section determined to have been spent for a purpose other than those
8 specified in the grant award.

9 **§ 40505. Security exercises**

10 (a) IN GENERAL.—The Secretary shall establish a program for con-
11 ducting security exercises for public transportation agencies for the purpose
12 of assessing and improving the capabilities of entities described in sub-
13 section (b) to prevent, prepare for, mitigate against, respond to, and recover
14 from acts of terrorism.

15 (b) COVERED ENTITIES.—Entities to be assessed under the program in-
16 clude—

17 (1) Federal, State, and local agencies and tribal governments;

18 (2) public transportation agencies;

19 (3) governmental and nongovernmental emergency response pro-
20 viders and law enforcement personnel, including transit police; and

21 (4) any other organization or entity that the Secretary determines
22 appropriate.

23 (c) REQUIREMENTS.—The Secretary shall ensure that the program—

24 (1) requires, for public transportation agencies that the Secretary
25 considers appropriate, exercises to be conducted that are—

26 (A) scaled and tailored to the needs of specific public transpor-
27 tation systems, and include taking into account the needs of the
28 elderly and individuals with disabilities;

29 (B) live;

30 (C) coordinated with appropriate officials;

31 (D) as realistic as practicable and based on current risk assess-
32 ments, including credible threats, vulnerabilities, and con-
33 sequences;

34 (E) inclusive, as appropriate, of frontline employees and man-
35 agers; and

36 (F) consistent with the National Incident Management System,
37 the National Response Plan, the National Infrastructure Protec-
38 tion Plan, the National Preparedness Guidance, the National Pre-
39 paredness Goal, and other national initiatives of this type;

40 (2) provides that exercises described in paragraph (1) will be—

1 (A) evaluated by the Secretary against clear and consistent per-
2 formance measures;

3 (B) assessed by the Secretary to learn best practices, which
4 shall be shared with appropriate Federal, State, local, and tribal
5 officials, governmental and nongovernmental emergency response
6 providers, law enforcement personnel, including railroad and trans-
7 sit police, and appropriate stakeholders; and

8 (C) followed by remedial action by covered entities in response
9 to lessons learned;

10 (3) involves individuals in neighborhoods around the infrastructure
11 of a public transportation system; and

12 (4) assists State, local, and tribal governments and public transpor-
13 tation agencies in designing, implementing, and evaluating exercises
14 that conform to the requirements of paragraph (2).

15 (d) NATIONAL EXERCISE PROGRAM.—The Secretary shall ensure that the
16 exercise program developed under subsection (a) is a component of the na-
17 tional exercise program established under section 20508 of this title.

18 (e) FERRY SYSTEM EXEMPTION.—This section does not apply to a ferry
19 system for which drills are required to be conducted under section 70103
20 of title 46.

21 **§ 40506. Public transportation security training program**

22 (a) APPLICABILITY.—A public transportation agency that receives a grant
23 award under this chapter shall develop and implement a security training
24 program under this section.

25 (b) IN GENERAL.—The Secretary shall develop and issue detailed final
26 regulations for a public transportation security training program to prepare
27 public transportation employees, including frontline employees, for potential
28 security threats and conditions.

29 (c) CONSULTATION.—The Secretary shall develop the final regulations
30 under subsection (b) in consultation with—

31 (1) appropriate law enforcement, fire service, security, and terrorism
32 experts;

33 (2) representatives of public transportation agencies; and

34 (3) nonprofit employee labor organizations representing public trans-
35 portation employees or emergency response personnel.

36 (d) PROGRAM ELEMENTS.—The final regulations developed under sub-
37 section (b) shall require security training programs to include, at a min-
38 imum, elements to address the following:

39 (1) Determination of the seriousness of any occurrence or threat.

40 (2) Crew and passenger communication and coordination.

1 (3) Appropriate responses to defend oneself, including using non-
2 lethal defense devices.

3 (4) Use of personal protective devices and other protective equip-
4 ment.

5 (5) Evacuation procedures for passengers and employees, including
6 individuals with disabilities and the elderly.

7 (6) Training related to behavioral and psychological understanding
8 of, and responses to, terrorist incidents, including the ability to cope
9 with hijacker behavior, and passenger responses.

10 (7) Live situational training exercises regarding various threat condi-
11 tions, including tunnel evacuation procedures.

12 (8) Recognition and reporting of dangerous substances and sus-
13 picious packages, persons, and situations.

14 (9) Understanding security incident procedures, including procedures
15 for communicating with governmental and nongovernmental emergency
16 response providers and for on-scene interaction with emergency re-
17 sponse providers.

18 (10) Operation and maintenance of security equipment and systems.

19 (11) Other security training activities that the Secretary considers
20 appropriate.

21 (e) REQUIRED PROGRAMS.—

22 (1) DEVELOPMENT AND SUBMISSION TO SECRETARY.—Not later
23 than 90 days after a public transportation agency meets the require-
24 ments under subsection (a), the public transportation agency shall de-
25 velop a security training program in accordance with the regulations
26 developed under subsection (b) and submit the program to the Sec-
27 retary for approval.

28 (2) APPROVAL.—Not later than 60 days after receiving a security
29 training program proposal under this subsection, the Secretary shall
30 approve the program or require the public transportation agency that
31 developed the program to make any revisions to the program that the
32 Secretary determines necessary for the program to meet the require-
33 ments of the regulations. A public transportation agency shall respond
34 to the Secretary's comments within 30 days after receiving them.

35 (3) TRAINING.—Not later than 1 year after the Secretary approves
36 a security training program proposal under this subsection, the public
37 transportation agency that developed the program shall complete the
38 training of all employees covered under the program.

39 (4) UPDATES OF REGULATIONS AND PROGRAM REVISIONS.—The
40 Secretary shall periodically review and update, as appropriate, the
41 training regulations issued under subsection (b) to reflect new or

1 changing security threats. Each public transportation agency shall re-
2 vise its training program accordingly and provide additional training as
3 necessary to its workers within a reasonable time after the regulations
4 are updated.

5 (f) LONG-TERM TRAINING REQUIREMENT.—A public transportation
6 agency required to develop a security training program under this section
7 shall provide routine and ongoing training for employees covered under the
8 program, regardless of whether the public transportation agency receives
9 subsequent grant awards.

10 (g) NATIONAL TRAINING PROGRAM.—The Secretary shall ensure that the
11 training program developed under subsection (b) is a component of the na-
12 tional training program established under section 20508 of this title.

13 (h) FERRY EXEMPTION.—This section shall not apply to a ferry system
14 for which training is required to be conducted under section 70103 of title
15 46.

16 **§ 40507. Public transportation research and development**

17 (a) ESTABLISHMENT OF RESEARCH AND DEVELOPMENT PROGRAM.—The
18 Secretary shall carry out, through the Homeland Security Advanced Re-
19 search Projects Agency in the Science and Technology Directorate and in
20 consultation with the Transportation Security Administration and the Fed-
21 eral Transit Administration, a research and development program to im-
22 prove the security of transportation systems.

23 (b) AWARDING OF GRANTS AND CONTRACTS.—The Secretary shall award
24 grants or contracts to public or private entities to conduct research and
25 demonstrate technologies and methods to reduce and deter terrorist threats
26 or mitigate damages resulting from terrorist attacks against public trans-
27 portation systems.

28 (c) USE OF FUNDS.—Grants or contracts awarded under this section—

29 (1) shall be coordinated with activities of the Homeland Security Ad-
30 vanced Research Projects Agency; and

31 (2) may be used to—

32 (A) research chemical, biological, radiological, or explosive detec-
33 tion systems that do not significantly impede passenger access;

34 (B) research imaging technologies;

35 (C) conduct product evaluations and testing;

36 (D) improve security and redundancy for critical communica-
37 tions, electrical power, and computer and train control systems;

38 (E) develop technologies for securing tunnels, transit bridges,
39 and aerial structures;

40 (F) research technologies that mitigate damages in the event of
41 a cyberattack; and

1 (G) research other technologies or methods for reducing or de-
2 terring terrorist attacks against public transportation systems, or
3 mitigating damage from attacks.

4 (d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES.—

5 (1) CONSULTATION.—In carrying out research and development
6 projects under this section, the Secretary shall consult with the Chief
7 Privacy Officer of the Department and the Officer for Civil Rights and
8 Civil Liberties of the Department, as appropriate, and in accordance
9 with section 10543 of this title.

10 (2) PRIVACY IMPACT ASSESSMENTS.—In accordance with sections
11 10543 and 11505 of this title, the Chief Privacy Officer shall conduct
12 privacy impact assessments and the Officer for Civil Rights and Civil
13 Liberties shall conduct reviews, as appropriate, for research and devel-
14 opment initiatives developed under this section.

15 (e) REPORTING REQUIREMENT.—Each entity that is awarded a grant or
16 contract under this section shall report annually to the Department on the
17 use of grant or contract funds received under this section to ensure that
18 the awards made are expended in accordance with the purposes of this
19 chapter and the priorities developed by the Secretary.

20 (f) COORDINATION.—The Secretary shall ensure that the research is con-
21 sistent with the priorities established in the National Strategy for Public
22 Transportation Security and is coordinated, to the extent practicable, with
23 other Federal, State, local, tribal, and private-sector public transportation,
24 railroad, commuter railroad, and over-the-road bus research initiatives to le-
25 verage resources and avoid unnecessary duplicative efforts.

26 (g) RETURN OF MISSPENT GRANT OR CONTRACT FUNDS.—If the Sec-
27 retary determines that a grantee or contractor used any portion of the grant
28 or contract funds received under this section for a purpose other than the
29 allowable uses specified under subsection (c), the grantee or contractor shall
30 return that amount to the Treasury.

31 **§ 40508. Information sharing**

32 (a) INTELLIGENCE SHARING.—The Secretary shall ensure that the De-
33 partment of Transportation receives appropriate and timely notification of
34 all credible terrorist threats against public transportation assets in the
35 United States.

36 (b) INFORMATION SHARING AND ANALYSIS CENTER.—

37 (1) AUTHORIZATION.—The Secretary shall provide for the reasonable
38 costs of the Information Sharing and Analysis Center for Public Trans-
39 portation (in this subsection referred to as the “ISAC”).

40 (2) PARTICIPATION.—The Secretary—

1 (A) shall require public transportation agencies that the Sec-
2 retary determines to be at high risk of terrorist attack to partici-
3 pate in the ISAC;

4 (B) shall encourage all other public transportation agencies to
5 participate in the ISAC;

6 (C) shall encourage the participation of nonprofit employee
7 labor organizations representing public transportation employees,
8 as appropriate; and

9 (D) shall not charge a fee for participating in the ISAC.

10 **§ 40509. Reporting requirements**

11 (a) ANNUAL REPORT TO CONGRESS.—

12 (1) IN GENERAL.—Not later than March 31 of each year, the Sec-
13 retary shall submit a report, containing the information described in
14 paragraph (2), to the appropriate congressional committees.

15 (2) CONTENTS.—The report submitted under paragraph (1) shall in-
16 clude—

17 (A) a description of the implementation of the provisions of this
18 chapter;

19 (B) the amount of funds appropriated to carry out the provi-
20 sions of this chapter that have not been expended or obligated;

21 (C) the National Strategy for Public Transportation Security
22 required under section 40502 of this title;

23 (D) an estimate of the cost to implement the National Strategy
24 for Public Transportation Security, which shall break out the ag-
25 gregated total cost of needed capital and operational security im-
26 provements for fiscal years 2017 and 2018; and

27 (E) the state of public transportation security in the United
28 States, which shall include detailing the status of security assess-
29 ments, the progress being made around the country in developing
30 prioritized lists of security improvements necessary to make public
31 transportation facilities and passengers more secure, the progress
32 being made by agencies in developing security plans and how those
33 plans differ from the security assessments, and a prioritized list
34 of security improvements being compiled by other agencies, as well
35 as a random sample of an equal number of large- and small-scale
36 projects currently underway.

37 (3) FORMAT.—The Secretary may submit the report in both classi-
38 fied and redacted formats if the Secretary determines that it is appro-
39 priate or necessary.

40 (b) ANNUAL REPORT TO CHIEF EXECUTIVE OFFICERS.—

1 (1) IN GENERAL.—Not later than March 31 of each year, the Sec-
 2 retary shall submit a report to the chief executive officer of each State
 3 with a public transportation agency that has received a grant under
 4 this chapter.

5 (2) CONTENTS.—The report submitted under paragraph (1) shall
 6 specify—

7 (A) the amount of grant funds distributed to each public trans-
 8 portation agency; and

9 (B) the use of the grant funds.

10 **§ 40510. Public transportation employee protections**

11 (a) IN GENERAL.—A public transportation agency, a contractor or a sub-
 12 contractor of the agency, or an officer or employee of the agency, shall not
 13 discharge, demote, suspend, reprimand, or in any other way discriminate
 14 against an employee if the discrimination is due, in whole or in part, to the
 15 employee’s lawful, good faith act done, or perceived by the employer to have
 16 been done or about to be done—

17 (1) to provide information, directly cause information to be provided,
 18 or otherwise directly assist in any investigation regarding any conduct
 19 that the employee reasonably believes constitutes a violation of any
 20 Federal law, rule, or regulation relating to public transportation safety
 21 or security, or fraud, waste, or abuse of Federal grants or other public
 22 funds intended to be used for public transportation safety or security,
 23 if the information or assistance is provided to, or an investigation stem-
 24 ming from the provided information is conducted by—

25 (A) a Federal, State, or local regulatory or law enforcement
 26 agency (including an office of the Inspector General under the In-
 27 spector General Act of 1978 (Public Law 95–452, 5 U.S.C.
 28 App.);

29 (B) a member of Congress, a committee of Congress, or the
 30 Government Accountability Office; or

31 (C) an individual with supervisory authority over the employee,
 32 or another individual who has the authority to investigate, dis-
 33 cover, or terminate the misconduct;

34 (2) to refuse to violate or assist in the violation of any Federal law,
 35 rule, or regulation relating to public transportation safety or security;

36 (3) to file a complaint or directly cause to be brought a proceeding
 37 relating to the enforcement of this section or to testify in that pro-
 38 ceeding;

39 (4) to cooperate with a safety or security investigation by the Sec-
 40 retary of Transportation, the Secretary, or the National Transportation
 41 Safety Board; or

1 (5) to furnish information to the Secretary of Transportation, the
2 Secretary, the National Transportation Safety Board, or another Fed-
3 eral, State, or local regulatory or law enforcement agency as to the
4 facts relating to any accident or incident resulting in injury or death
5 to an individual or damage to property occurring in connection with
6 public transportation.

7 (b) HAZARDOUS SAFETY OR SECURITY CONDITIONS.—

8 (1) IN GENERAL.—A public transportation agency, a contractor or
9 a subcontractor of the agency, or an officer or employee of the agency,
10 shall not discharge, demote, suspend, reprimand, or in any other way
11 discriminate against an employee for—

12 (A) reporting a hazardous safety or security condition;

13 (B) refusing to work when confronted by a hazardous safety or
14 security condition related to the performance of the employee's du-
15 ties, if the conditions described in paragraph (2) exist; or

16 (C) refusing to authorize the use of any safety- or security-re-
17 lated equipment, track, or structures, if the employee is respon-
18 sible for the inspection or repair of the equipment, track, or struc-
19 tures, when the employee believes that the equipment, track, or
20 structures are in a hazardous safety or security condition, if the
21 conditions described in paragraph (2) exist.

22 (2) PROTECTED REFUSAL.—A refusal is protected under subpara-
23 graphs (B) and (C) of paragraph (1) if—

24 (A) the refusal is made in good faith and no reasonable alter-
25 native to the refusal is available to the employee;

26 (B) a reasonable individual in the circumstances then con-
27 fronting the employee would conclude that—

28 (i) the hazardous condition presents an imminent danger of
29 death or serious injury; and

30 (ii) the urgency of the situation does not allow sufficient
31 time to eliminate the danger without the refusal; and

32 (C) the employee, where possible, has notified the public trans-
33 portation agency of the existence of the hazardous condition and
34 the intention not to perform further work, or not to authorize the
35 use of the hazardous equipment, track, or structures, unless the
36 condition is corrected immediately or the equipment, track, or
37 structures are repaired properly or replaced.

38 (3) LIMITED APPLICABILITY.—Only paragraph (1)(A) applies to se-
39 curity personnel, including transit police, employed or utilized by a pub-
40 lic transportation agency to protect riders, equipment, assets, or facili-
41 ties.

1 (c) ENFORCEMENT ACTION.—

2 (1) FILING AND NOTIFICATION.—An individual who believes that he
3 or she has been discharged or otherwise discriminated against by a per-
4 son in violation of subsection (a) or (b) may, not later than 180 days
5 after the date on which the violation occurs, file (or have a person file
6 on his or her behalf) a complaint with the Secretary of Labor alleging
7 the discharge or discrimination. On receipt of a complaint filed under
8 this paragraph, the Secretary of Labor shall notify, in writing, the indi-
9 vidual named in the complaint and the individual's employer of the fil-
10 ing of the complaint, the allegations contained in the complaint, the
11 substance of evidence supporting the complaint, and the opportunities
12 that will be afforded to the individual under paragraph (2).

13 (2) INVESTIGATION; PRELIMINARY ORDER.—

14 (A) IN GENERAL.—Not later than 60 days after the date of re-
15 ceipt of a complaint filed under paragraph (1) and after affording
16 the individual named in the complaint an opportunity to submit
17 to the Secretary of Labor a written response to the complaint and
18 an opportunity to meet with a representative of the Secretary of
19 Labor to present statements from witnesses, the Secretary of
20 Labor shall conduct an investigation and determine whether there
21 is reasonable cause to believe that the complaint has merit and no-
22 tify, in writing, the complainant and the person alleged to have
23 committed a violation of subsection (a) or (b) of the Secretary of
24 Labor's findings. If the Secretary of Labor concludes that there
25 is a reasonable cause to believe that a violation of subsection (a)
26 or (b) has occurred, the Secretary of Labor shall accompany the
27 Secretary of Labor's findings with a preliminary order providing
28 the relief prescribed by paragraph (3)(B). Not later than 30 days
29 after the date of notification of findings under this paragraph, ei-
30 ther the person alleged to have committed the violation or the
31 complainant may file objections to the findings or preliminary
32 order, or both, and request a hearing on the record. The filing of
33 objections shall not operate to stay a reinstatement remedy con-
34 tained in the preliminary order. Hearings shall be conducted expe-
35 ditiously. If a hearing is not requested in the 30-day period, the
36 preliminary order shall be deemed a final order that is not subject
37 to judicial review.

38 (B) REQUIREMENTS.—

39 (i) REQUIRED SHOWING BY COMPLAINANT.—The Secretary
40 of Labor shall dismiss a complaint filed under this subsection
41 and shall not conduct an investigation otherwise required

1 under subparagraph (A) unless the complainant makes a
2 prima facie showing that any behavior described in subsection
3 (a) or (b) was a contributing factor in the unfavorable per-
4 sonnel action alleged in the complaint.

5 (ii) SHOWING BY EMPLOYER.—Notwithstanding a finding
6 by the Secretary of Labor that the complainant has made the
7 showing required under clause (i), no investigation otherwise
8 required under paragraph (A) shall be conducted if the em-
9 ployer demonstrates, by clear and convincing evidence, that
10 the employer would have taken the same unfavorable per-
11 sonnel action in the absence of that behavior.

12 (iii) CRITERION FOR DETERMINATION BY SECRETARY OF
13 LABOR.—The Secretary of Labor may determine that a viola-
14 tion of subsection (a) or (b) has occurred only if the com-
15 plainant demonstrates that any behavior described in sub-
16 section (a) or (b) was a contributing factor in the unfavorable
17 personnel action alleged in the complaint.

18 (iv) PROHIBITION.—Relief may not be ordered under para-
19 graph (A) if the employer demonstrates by clear and con-
20 vincing evidence that the employer would have taken the same
21 unfavorable personnel action in the absence of that behavior.

22 (3) FINAL ORDER.—

23 (A) DEADLINE FOR ISSUANCE; SETTLEMENT AGREEMENTS.—
24 Not later than 120 days after the date of conclusion of a hearing
25 under paragraph (2), the Secretary of Labor shall issue a final
26 order providing the relief prescribed by this paragraph or denying
27 the complaint. At any time before issuance of a final order, a pro-
28 ceeding under this subsection may be terminated on the basis of
29 a settlement agreement entered into by the Secretary of Labor,
30 the complainant, and the person alleged to have committed the
31 violation.

32 (B) REMEDY.—If, in response to a complaint filed under para-
33 graph (1), the Secretary of Labor determines that a violation of
34 subsection (a) or (b) has occurred, the Secretary of Labor shall
35 order the person who committed the violation to—

36 (i) take affirmative action to abate the violation; and

37 (ii) provide the remedies described in subsection (d).

38 (C) ORDER.—If an order is issued under subparagraph (B), the
39 Secretary of Labor, at the request of the complainant, shall assess
40 against the person against whom the order is issued a sum equal
41 to the aggregate amount of all costs and expenses (including attor-

1 ney and expert witness fees) reasonably incurred, as determined
2 by the Secretary of Labor, by the complainant for, or in connec-
3 tion with, bringing the complaint on which the order was issued.

4 (D) FRIVOLOUS COMPLAINTS.—If the Secretary of Labor finds
5 that a complaint under paragraph (1) is frivolous or has been
6 brought in bad faith, the Secretary of Labor may award to the
7 prevailing employer reasonable attorney fees not exceeding \$1,000.

8 (4) REVIEW.—

9 (A) APPEAL TO COURT OF APPEALS.—A person adversely af-
10 fected or aggrieved by an order issued under paragraph (3) may
11 obtain review of the order in the United States Court of Appeals
12 for the circuit in which the violation, with respect to which the
13 order was issued, allegedly occurred or the circuit in which the
14 complainant resided on the date of the violation. The petition for
15 review must be filed not later than 60 days after the date of the
16 issuance of the final order of the Secretary of Labor. Review shall
17 conform to chapter 7 of title 5. The commencement of proceedings
18 under this subparagraph shall not, unless ordered by the court,
19 operate as a stay of the order.

20 (B) LIMITATION ON COLLATERAL ATTACK.—An order of the
21 Secretary of Labor with respect to which review could have been
22 obtained under subparagraph (A) shall not be subject to judicial
23 review in any criminal or other civil proceeding.

24 (5) ENFORCEMENT OF ORDER BY SECRETARY OF LABOR.—When a
25 person fails to comply with an order issued under paragraph (3), the
26 Secretary of Labor may file a civil action in the United States district
27 court for the district in which the violation was found to occur to en-
28 force the order. In actions brought under this paragraph, the district
29 courts have jurisdiction to grant all appropriate relief including injunc-
30 tive relief and compensatory damages.

31 (6) ENFORCEMENT OF ORDER BY PARTIES.—

32 (A) COMMENCEMENT OF ACTION.—An individual on whose be-
33 half an order was issued under paragraph (3) may commence a
34 civil action against the person to whom the order was issued to
35 require compliance with the order. The appropriate United States
36 district court has jurisdiction, without regard to the amount in
37 controversy or the citizenship of the parties, to enforce the order.

38 (B) ATTORNEY FEES.—The court, in issuing a final order under
39 this paragraph, may award costs of litigation (including reasonable
40 attorney and expert witness fees) to any party when the court de-
41 termines an award is appropriate.

1 (7) DE NOVO REVIEW.—With respect to a complaint under para-
2 graph (1), if the Secretary of Labor has not issued a final decision
3 within 210 days after the filing of the complaint and if the delay is
4 not due to the bad faith of the employee, the employee may bring an
5 original action at law or equity for de novo review in the appropriate
6 district court of the United States, which has jurisdiction over the ac-
7 tion without regard to the amount in controversy, and which action
8 shall, at the request of either party to the action, be tried by the court
9 with a jury. The action shall be governed by the same legal burdens
10 of proof specified in paragraph (2)(B) for review by the Secretary of
11 Labor.

12 (d) REMEDIES.—

13 (1) IN GENERAL.—An employee prevailing in any action under sub-
14 section (c) is entitled to all relief necessary to make the employee
15 whole.

16 (2) DAMAGES.—Relief in an action under subsection (c) (including
17 an action described in subsection (c)(7)) includes—

18 (A) reinstatement with the same seniority status that the em-
19 ployee would have had, but for the discrimination;

20 (B) any backpay, with interest; and

21 (C) compensatory damages, including compensation for any spe-
22 cial damages sustained as a result of the discrimination, including
23 litigation costs, expert witness fees, and reasonable attorney fees.

24 (3) PUNITIVE DAMAGES.—Relief in an action under subsection (c)
25 may include punitive damages in an amount not to exceed \$250,000.

26 (e) ELECTION OF REMEDIES.—An employee may not seek protection
27 under both this section and another provision of law for the same allegedly
28 unlawful act of the public transportation agency.

29 (f) NO PREEMPTION.—Nothing in this section preempts or diminishes
30 any other safeguards against discrimination, demotion, discharge, suspen-
31 sion, threats, harassment, reprimand, retaliation, or other manner of dis-
32 crimination provided by Federal or State law.

33 (g) RIGHTS RETAINED BY EMPLOYEE.—Nothing in this section shall be
34 construed to diminish the rights, privileges, or remedies of an employee
35 under Federal or State law or under a collective bargaining agreement. The
36 rights and remedies in this section may not be waived by an agreement, pol-
37 icy, form, or condition of employment.

38 (h) DISCLOSURE OF IDENTITY.—

39 (1) IN GENERAL.—Except as provided in paragraph (2), or with the
40 written consent of the employee, the Secretary of Transportation or the

1 Secretary may not disclose the name of an employee who has provided
2 information described in subsection (a)(1).

3 (2) EXCEPTION.— The Secretary of Transportation or the Secretary
4 shall disclose to the Attorney General the name of an employee de-
5 scribed in paragraph (1) if the matter is referred to the Attorney Gen-
6 eral for enforcement. The Secretary making the disclosure shall provide
7 reasonable advance notice to the affected employee if disclosure of that
8 individual’s identity or identifying information is to occur.

9 (i) PROCESS FOR REPORTING SECURITY PROBLEMS TO THE DEPART-
10 MENT.—

11 (1) ESTABLISHMENT OF PROCESS.—The Secretary shall establish
12 through regulations after an opportunity for notice and comment, and
13 provide information to the public regarding, a process by which a per-
14 son may submit a report to the Secretary regarding public transpor-
15 tation security problems, deficiencies, or vulnerabilities.

16 (2) ACKNOWLEDGMENT OF RECEIPT.—If a report submitted under
17 paragraph (1) identifies the person making the report, the Secretary
18 shall respond promptly to the person and acknowledge receipt of the
19 report.

20 (3) STEPS TO ADDRESS PROBLEM.—The Secretary shall review and
21 consider the information provided in a report submitted under para-
22 graph (1) and shall take appropriate steps to address any problems or
23 deficiencies identified.

24 **§ 40511. Security background checks of covered individuals**
25 **for public transportation**

26 (a) DEFINITIONS.—In this section:

27 (1) COVERED INDIVIDUAL.—The term “covered individual” means
28 an employee of a public transportation agency or a contractor or sub-
29 contractor of a public transportation agency.

30 (2) SECURITY BACKGROUND CHECK.—The term “security back-
31 ground check” means reviewing the following for the purpose of identi-
32 fying an individual who may pose a threat to transportation security,
33 national security, or of terrorism:

34 (A) Relevant criminal history databases.

35 (B) In the case of an alien (as defined in section 101 of the
36 Immigration and Nationality Act (8 U.S.C. 1101)), the relevant
37 databases to determine the status of the alien under the immigra-
38 tion laws of the United States.

39 (C) Other relevant information or databases, as determined by
40 the Secretary.

41 (b) GUIDANCE.—

1 (1) IN GENERAL.—Guidance, recommendations, suggested action
2 items, and other widely disseminated voluntary action items issued by
3 the Secretary to a public transportation agency or a contractor or sub-
4 contractor of a public transportation agency relating to performing a
5 security background check of a covered individual shall contain rec-
6 ommendations on the appropriate scope and application of a security
7 background check, including the time period covered, the types of dis-
8 qualifying offenses, and a redress process for adversely impacted cov-
9 ered individuals consistent with subsections (c) and (d).

10 (2) ADEQUATE REDRESS PROCESS.—If a public transportation agen-
11 cy or a contractor or subcontractor of a public transportation agency
12 performs a security background check on a covered individual to fulfill
13 guidance issued by the Secretary under paragraph (1), the Secretary
14 shall not consider the guidance fulfilled unless an adequate redress
15 process as described in subsection (d) is provided to covered individ-
16 uals.

17 (c) REQUIREMENTS.—If the Secretary issues a rule, regulation or direc-
18 tive requiring a public transportation agency or contractor or subcontractor
19 of a public transportation agency to perform a security background check
20 of a covered individual, then the Secretary shall prohibit a public transpor-
21 tation agency or contractor or subcontractor of a public transportation
22 agency from making an adverse employment decision, including removal or
23 suspension of the employee, due to the rule, regulation, or directive with re-
24 spect to a covered individual unless the public transportation agency or con-
25 tractor or subcontractor of a public transportation agency determines that
26 the covered individual—

27 (1) has been convicted of, has been found not guilty of by reason
28 of insanity, or is under want, warrant, or indictment for a permanent
29 disqualifying criminal offense listed in part 1572 of title 49, Code of
30 Federal Regulations;

31 (2) was convicted of or found not guilty by reason of insanity of an
32 interim disqualifying criminal offense listed in part 1572 of title 49,
33 Code of Federal Regulations, within 7 years of the date that the public
34 transportation agency or contractor or subcontractor of the public
35 transportation agency performs the security background check; or

36 (3) was incarcerated for an interim disqualifying criminal offense
37 listed in part 1572 of title 49, Code of Federal Regulations, and re-
38 leased from incarceration within 5 years of the date that the public
39 transportation agency or contractor or subcontractor of a public trans-
40 portation agency performs the security background check.

1 (d) REDRESS PROCESS.—If the Secretary issues a rule, regulation, or di-
2 rective requiring a public transportation agency or contractor or subcon-
3 tractor of a public transportation agency to perform a security background
4 check of a covered individual, the Secretary shall—

5 (1) provide an adequate redress process for a covered individual sub-
6 jected to an adverse employment decision, including removal or suspen-
7 sion of the employee, due to the rule, regulation, or directive that is
8 consistent with the appeals and waiver process established for appli-
9 cants for commercial motor vehicle hazardous materials endorsements
10 and transportation workers at ports, as required by section 70105(c)
11 of title 46; and

12 (2) have the authority to order an appropriate remedy, including re-
13 instatement of the covered individual, should the Secretary determine
14 that a public transportation agency or contractor or subcontractor of
15 a public transportation agency wrongfully made an adverse employment
16 decision regarding a covered individual pursuant to the rule, regulation,
17 or directive.

18 (e) FALSE STATEMENTS.—A public transportation agency or a contractor
19 or subcontractor of a public transportation agency may not knowingly mis-
20 represent to an employee or other relevant person, including an arbiter in-
21 volved in a labor arbitration, the scope, application, or meaning of rules,
22 regulations, directives, or guidance issued by the Secretary related to secu-
23 rity background check requirements for covered individuals when conducting
24 a security background check. The Secretary shall issue a regulation that
25 prohibits a public transportation agency or a contractor or subcontractor of
26 a public transportation agency from knowingly misrepresenting to an em-
27 ployee or other relevant person, including an arbiter involved in a labor arbi-
28 tration, the scope, application, or meaning of rules, regulations, directives,
29 or guidance issued by the Secretary related to security background check
30 requirements for covered individuals when conducting a security background
31 check.

32 (f) RIGHTS AND RESPONSIBILITIES.—Nothing in this section shall be
33 construed to abridge a public transportation agency's or a contractor or
34 subcontractor of a public transportation agency's rights or responsibilities
35 to make adverse employment decisions permitted by other Federal, State,
36 or local laws. Nothing in the section shall be construed to abridge rights
37 and responsibilities of covered individuals, a public transportation agency,
38 or a contractor or subcontractor of a public transportation agency under
39 any other Federal, State, or local laws or collective bargaining agreement.

40 (g) NO PREEMPTION OF FEDERAL OR STATE LAW.—Nothing in this sec-
41 tion shall be construed to preempt a Federal, State, or local law that re-

1 quires criminal history background checks, immigration status checks, or
2 other background checks of covered individuals.

3 (h) STATUTORY CONSTRUCTION.—Nothing in this section shall be con-
4 strued to affect the process for review established under section 70105(c)
5 of title 46, including regulations issued under that section.

6 **§ 40512. Limitation on fines and civil penalties**

7 (a) INSPECTORS.—Surface transportation inspectors shall be prohibited
8 from issuing fines to public transportation agencies for violations of the De-
9 partment’s regulations or orders except through the process described in
10 subsection (b)

11 (b) CIVIL PENALTIES.—The Secretary shall be prohibited from assessing
12 civil penalties against public transportation agencies for violations of the
13 Department’s regulations or orders, except in accordance with the following:

14 (1) VIOLATION OF REGULATION OR ORDER.—In the case of a public
15 transportation agency that is found to be in violation of a regulation
16 or order issued by the Secretary, the Secretary shall seek correction of
17 the violation through a written notice to the public transportation agen-
18 cy and shall give the public transportation agency reasonable oppor-
19 tunity to correct the violation or propose an alternative means of com-
20 pliance acceptable to the Secretary.

21 (2) NO CORRECTION OR PROPOSED ALTERNATIVE COMPLIANCE.—If
22 the public transportation agency does not correct the violation or pro-
23 pose an alternative means of compliance acceptable to the Secretary
24 within a reasonable time period that is specified in the written notice,
25 the Secretary may take an action authorized in chapter 113 of this
26 title.

27 (c) LIMITATION ON SECRETARY.—The Secretary shall not initiate civil
28 enforcement actions for violations of administrative and procedural require-
29 ments pertaining to the application for and expenditure of funds awarded
30 under transportation security grant programs under this chapter.

31 **Chapter 407—Surface Transportation**
32 **Security**

Sec.

Subchapter I—General

- 40701. Definitions.
- 40702. Oversight and grant procedures.
- 40703. Public awareness and outreach.

Subchapter II—Railroad Security

- 40711. Railroad transportation security risk assessment and National Strategy.
- 40712. Railroad carrier assessments and plans.
- 40713. Railroad security assistance.
- 40714. Systemwide Amtrak security upgrades.
- 40715. Railroad carrier exercises.
- 40716. Railroad security training program.
- 40717. Railroad security research and development.
- 40718. Railroad tank car security testing.
- 40719. Security background checks of covered individuals.

40720. International railroad security program.

Subchapter III—Over-the-Road Bus Security

40731. Assessments and plans.

40732. Assistance.

40733. Exercises.

40734. Training program.

40735. Research and development.

Subchapter IV—Hazardous Material and Pipeline Security

40741. Railroad routing of security-sensitive materials.

40742. Railroad security-sensitive material tracking.

40743. Motor carrier security-sensitive material tracking.

40744. Use of transportation security card in hazmat licensing.

40745. Pipeline security inspections and enforcement.

40746. Pipeline security and incident recovery plan.

Subchapter I—General

§ 40701. Definitions

In this chapter:

(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 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 States,
33 the District of Columbia, Puerto Rico, the Northern Mariana Islands,
34 the Virgin Islands, Guam, American Samoa, and any other territory
35 (including a possession) of the United States.

36 **§ 40702. Oversight and grant procedures**

37 (a) SECRETARIAL OVERSIGHT.—The Secretary, in coordination with the
38 Secretary of Transportation for grants awarded to Amtrak, shall establish
39 necessary procedures, including monitoring and audits, to ensure that
40 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 those specified in the
2 grant award. The Secretary shall take all necessary actions to recover those
3 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 **§ 40703. 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 **Subchapter II—Railroad Security**

23 **§ 40711. Railroad transportation security risk assessment 24 and National Strategy**

25 (a) RISK ASSESSMENT.—The Secretary shall establish a Federal task
26 force, including the Transportation Security Administration and other agen-
27 cies in the Department, the Department of Transportation, and other ap-
28 propriate Federal agencies, to complete a nationwide risk assessment of a
29 terrorist attack on railroad carriers. The assessment shall include—

30 (1) a methodology for conducting the risk assessment, including
31 timelines, that addresses how the Department will work with the enti-
32 ties described in subsection (c) and make use of existing Federal exper-
33 tise in the Department, the Department of Transportation, and other
34 appropriate agencies;

35 (2) identification and evaluation of critical assets and infrastructure,
36 including tunnels used by railroad carriers in high-threat urban areas;

37 (3) identification of risks to those assets and infrastructure;

38 (4) identification of risks that are specific to the transportation of
39 hazardous materials via railroad;

1 (5) identification of risks to passenger and cargo security, transpor-
2 tation infrastructure protection systems, operations, communications
3 systems, and any other area identified by the assessment;

4 (6) an assessment of employee training and emergency response
5 planning;

6 (7) an assessment of public and private operational recovery plans,
7 taking into account the plans for the maritime sector required under
8 section 70103 of title 46, to expedite, to the maximum extent prac-
9 ticable, the return of an adversely affected railroad transportation sys-
10 tem or facility to its normal performance level after a major terrorist
11 attack or other security event on that system or facility; and

12 (8) an account of actions taken or planned by both public and pri-
13 vate entities to address identified railroad security issues and an as-
14 sessment of the effective integration of the actions.

15 (b) NATIONAL STRATEGY.—

16 (1) REQUIREMENT.—Based upon the assessment conducted under
17 subsection (a), the Secretary, consistent with and as required by sec-
18 tion 11314 of this title, shall develop and implement the modal plan
19 for railroad transportation, entitled the “National Strategy for Rail-
20 road Transportation Security”.

21 (2) CONTENTS.—The modal plan shall include prioritized goals, ac-
22 tions, objectives, policies, mechanisms, and schedules for, at a min-
23 imum—

24 (A) improving the security of railroad tunnels, railroad bridges,
25 railroad switching and car storage areas, other railroad infrastruc-
26 ture and facilities, information systems, and other areas identified
27 by the Secretary as posing significant railroad-related risks to
28 public safety and the movement of interstate commerce, taking
29 into account the impact that a proposed security measure might
30 have on the provision of railroad service or on operations served
31 or otherwise affected by railroad service;

32 (B) deploying equipment and personnel to detect security
33 threats, including those posed by explosives and hazardous chem-
34 ical, biological, and radioactive substances, and appropriate coun-
35 termeasures;

36 (C) consistent with section 40716 of this title, training railroad
37 employees in terrorism prevention, preparedness, passenger evacu-
38 ation, and response activities;

39 (D) conducting public outreach campaigns for railroads regard-
40 ing security, including educational initiatives designed to inform

1 the public on how to prevent, prepare for, respond to, and recover
2 from a terrorist attack on railroad transportation;

3 (E) providing additional railroad security support for railroads
4 at high or severe threat levels of alert;

5 (F) ensuring, in coordination with freight and intercity and
6 commuter passenger railroads, the continued movement of freight
7 and passengers in the event of an attack affecting the railroad sys-
8 tem, including the possibility of rerouting traffic due to the loss
9 of critical infrastructure, such as a bridge, tunnel, yard, or station;

10 (G) coordinating existing and planned railroad security initia-
11 tives undertaken by the public and private sectors;

12 (H) assessing—

13 (i) the usefulness of covert testing of railroad security sys-
14 tems;

15 (ii) the ability to integrate security into infrastructure de-
16 sign; and

17 (iii) the implementation of random searches of passengers
18 and baggage; and

19 (I) identifying the immediate and long-term costs of measures
20 that may be required to address those risks and public- and pri-
21 vate-sector sources to fund the measures.

22 (3) RESPONSIBILITIES.—The Secretary shall include in the modal
23 plan a description of the roles, responsibilities, and authorities of Fed-
24 eral, State, and local agencies, government-sponsored entities, tribal
25 governments, and appropriate stakeholders described in subsection (c).
26 The plan also shall include—

27 (A) the identification of, and a plan to address, gaps and unnec-
28 essary overlaps in the roles, responsibilities, and authorities de-
29 scribed in this paragraph;

30 (B) a methodology for how the Department will work with the
31 entities described in subsection (c), and make use of existing Fed-
32 eral expertise within the Department, the Department of Trans-
33 portation, and other appropriate agencies;

34 (C) a process for facilitating security clearances for the purpose
35 of intelligence and information sharing with the entities described
36 in subsection (c), as appropriate;

37 (D) a strategy and timeline, coordinated with the research and
38 development program established under section 40717 of this title,
39 for the Department, the Department of Transportation, other ap-
40 propriate Federal agencies, and private entities to research and
41 develop new technologies for securing railroad systems; and

1 (E) a process for coordinating existing or future security strate-
2 gies and plans for railroad transportation, including—

3 (i) the National Infrastructure Protection Plan required by
4 Homeland Security Presidential Directive–7;

5 (ii) Executive Order No. 13416, 71 Fed. Reg. 71033 (Dec.
6 5, 2006); and

7 (iii) the Memorandum of Understanding between the De-
8 partment and the Department of Transportation on Roles
9 and Responsibilities, dated September 28, 2004, subsequent
10 annexes to this Memorandum of Understanding, and other
11 relevant agreements between the two Departments.

12 (c) CONSULTATION WITH STAKEHOLDERS.—In developing the National
13 Strategy required under this section, the Secretary shall consult with rail-
14 road management, nonprofit employee organizations representing railroad
15 employees, owners or lessors of railroad cars used to transport hazardous
16 materials, emergency responders, offerors of security-sensitive materials,
17 public safety officials, and other relevant parties.

18 (d) ADEQUACY OF EXISTING PLANS AND STRATEGIES.—In developing
19 the risk assessment and National Strategy required under this section, the
20 Secretary shall utilize relevant existing plans, strategies, and risk assess-
21 ments developed by the Department or other Federal agencies, including
22 those developed or implemented under section 11314 of this title, or Home-
23 land Security Presidential Directive–7, and, as appropriate, assessments de-
24 veloped by other public and private stakeholders.

25 (e) ANNUAL UPDATES.—Consistent with the requirements of section
26 11314 of this title, the Secretary shall update the assessment and National
27 Strategy each year and transmit a report, which may be submitted in both
28 classified and redacted formats, to the appropriate congressional committees
29 containing the updated assessment and recommendations.

30 **§ 40712. Railroad carrier assessments and plans**

31 (a) IN GENERAL.—The Secretary shall issue regulations that—

32 (1) require each railroad carrier assigned to a high-risk tier under
33 this section to—

34 (A) conduct a vulnerability assessment under subsections (c)
35 and (d); and

36 (B) prepare, submit to the Secretary for approval, and imple-
37 ment a security plan under this section that addresses security
38 performance requirements; and

39 (2) establish standards and guidelines, based on and consistent with
40 the risk assessment and National Strategy for Railroad Transportation
41 Security developed under section 40711 of this title, for developing and

1 implementing the vulnerability assessments and security plans for rail-
2 road carriers assigned to high-risk tiers.

3 (b) NON HIGH-RISK PROGRAMS.—The Secretary may establish a security
4 program for railroad carriers not assigned to a high-risk tier, including—

5 (1) guidance for the carriers in conducting vulnerability assessments
6 and preparing and implementing security plans, as determined appro-
7 priate by the Secretary; and

8 (2) a process to review and approve the assessments and plans, as
9 appropriate.

10 (c) SUBMISSION OF ASSESSMENTS AND SECURITY PLANS.—The vulner-
11 ability assessments and security plans required by the regulations for rail-
12 road carriers assigned to a high-risk tier shall be completed and submitted
13 to the Secretary for review and approval.

14 (d) VULNERABILITY ASSESSMENTS.—

15 (1) REQUIREMENTS.—The Secretary shall provide technical assist-
16 ance and guidance to railroad carriers in conducting vulnerability as-
17 sessments under this section and shall require that each vulnerability
18 assessment of a railroad carrier assigned to a high-risk tier under this
19 section, include, as applicable—

20 (A) identification and evaluation of critical railroad carrier as-
21 sets and infrastructure, including platforms, stations, intermodal
22 terminals, tunnels, bridges, switching and storage areas, and infor-
23 mation systems as appropriate;

24 (B) identification of the vulnerabilities of those assets and infra-
25 structure;

26 (C) identification of strengths and weaknesses in—

27 (i) physical security;

28 (ii) passenger and cargo security, including the security of
29 security-sensitive materials being transported by railroad or
30 stored on railroad property;

31 (iii) programmable electronic devices, computers, or other
32 automated systems which are used in providing the transpor-
33 tation;

34 (iv) alarms, cameras, and other protection systems;

35 (v) communications systems and utilities needed for rail-
36 road security purposes, including dispatching and notification
37 systems;

38 (vi) emergency response planning;

39 (vii) employee training; and

40 (viii) other matters the Secretary determines appropriate;

41 and

1 (D) identification of redundant and backup systems required to
2 ensure the continued operation of critical elements of a railroad
3 carrier's system in the event of an attack or other incident, includ-
4 ing disruption of commercial electric power or a communications
5 network.

6 (2) THREAT INFORMATION.—The Secretary shall provide in a timely
7 manner to the appropriate employees of a railroad carrier, as des-
8 ignated by the railroad carrier, threat information that is relevant to
9 the carrier when preparing and submitting a vulnerability assessment
10 and security plan, including an assessment of the most likely methods
11 that could be used by terrorists to exploit weaknesses in railroad secu-
12 rity.

13 (e) SECURITY PLANS.—

14 (1) REQUIREMENTS.—The Secretary shall provide technical assist-
15 ance and guidance to railroad carriers in preparing and implementing
16 security plans under this section, and shall require that each security
17 plan of a railroad carrier assigned to a high-risk tier under this section
18 include, as applicable—

19 (A) identification of a security coordinator having authority—

20 (i) to implement security actions under the plan;

21 (ii) to coordinate security improvements; and

22 (iii) to receive immediate communications from appropriate
23 Federal officials regarding railroad security;

24 (B) a list of needed capital and operational improvements;

25 (C) procedures to be implemented or used by the railroad car-
26 rier in response to a terrorist attack, including evacuation and
27 passenger communication plans that include individuals with dis-
28 abilities as appropriate;

29 (D) identification of steps taken with State and local law en-
30 forcement agencies, emergency responders, and Federal officials to
31 coordinate security measures and plans for response to a terrorist
32 attack;

33 (E) a strategy and timeline for conducting training under sec-
34 tion 40716 of this title;

35 (F) enhanced security measures to be taken by the railroad car-
36 rier when the Secretary declares a period of heightened security
37 risk;

38 (G) plans for providing redundant and backup systems required
39 to ensure the continued operation of critical elements of the rail-
40 road carrier's system in the event of a terrorist attack or other
41 incident;

1 (H) a strategy for implementing enhanced security for ship-
2 ments of security-sensitive materials, including plans for quickly
3 locating and securing the shipments in the event of a terrorist at-
4 tack or security incident; and

5 (I) other actions or procedures the Secretary determines are ap-
6 propriate to address the security of railroad carriers.

7 (2) SECURITY COORDINATOR REQUIREMENTS.—The Secretary shall
8 require that the individual serving as the security coordinator identified
9 in paragraph (1)(A) is a citizen of the United States. The Secretary
10 may waive this requirement with respect to an individual if the Sec-
11 retary determines that it is appropriate to do so based on a background
12 check of the individual and a review of the consolidated terrorist
13 watchlist.

14 (3) CONSISTENCY WITH OTHER PLANS.—The Secretary shall ensure
15 that the security plans developed by railroad carriers under this section
16 are consistent with the risk assessment and National Strategy for Rail-
17 road Transportation Security developed under section 40711 of this
18 title.

19 (f) DEADLINE FOR REVIEW PROCESS.—Not later than 6 months after re-
20 ceiving the assessments and plans required under this section, the Secretary
21 shall—

22 (1) review each vulnerability assessment and security plan submitted
23 to the Secretary under subsection (c);

24 (2) require amendments to a security plan that does not meet the
25 requirements of this section; and

26 (3) approve a vulnerability assessment or security plan that meets
27 the requirements of this section.

28 (g) TIER ASSIGNMENT.—

29 (1) IN GENERAL.—Utilizing the risk assessment and National Strat-
30 egy for Railroad Transportation Security required under section 40711
31 of this title, the Secretary shall assign each railroad carrier to a risk-
32 based tier established by the Secretary.

33 (2) PROVIDING INFORMATION.—The Secretary may request, and a
34 railroad carrier shall provide, information necessary for the Secretary
35 to assign a railroad carrier to the appropriate tier under this sub-
36 section.

37 (3) NOTIFICATION.—Not later than 60 days after the date a railroad
38 carrier is assigned to a tier under this subsection, the Secretary shall
39 notify the railroad carrier of the tier to which it is assigned and the
40 reasons for the assignment.

1 (4) HIGH-RISK TIERS.—At least one of the tiers established by the
2 Secretary under this subsection shall be designated a tier for high-risk
3 railroad carriers.

4 (5) REASSIGNMENT.—The Secretary may reassign a railroad carrier
5 to another tier, as appropriate, in response to changes in risk. The Sec-
6 retary shall notify the railroad carrier not later than 60 days after the
7 reassignment and provide the railroad carrier with the reasons for the
8 reassignment.

9 (h) NONDISCLOSURE OF INFORMATION.—

10 (1) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this
11 section shall be construed as authorizing the withholding of information
12 from Congress.

13 (2) DISCLOSURE OF INDEPENDENTLY FURNISHED INFORMATION.—
14 Nothing in this section shall be construed as affecting the authority or
15 obligation of a Federal agency to disclose a record or information that
16 the Federal agency obtains from a railroad carrier under another Fed-
17 eral law.

18 (i) EXISTING PROCEDURES, PROTOCOLS, AND STANDARDS.—

19 (1) DETERMINATION.—In response to a petition by a railroad carrier
20 or at the discretion of the Secretary, the Secretary may determine that
21 existing procedures, protocols, and standards meet all or part of the
22 requirements of this section, including regulations issued under sub-
23 section (a), regarding vulnerability assessments and security plans.

24 (2) ELECTION.—Upon review and written determination by the Sec-
25 retary that existing procedures, protocols, or standards of a railroad
26 carrier satisfy the requirements of this section, the railroad carrier may
27 elect to comply with those procedures, protocols, or standards instead
28 of the requirements of this section.

29 (3) PARTIAL APPROVAL.—If the Secretary determines that the exist-
30 ing procedures, protocols, or standards of a railroad carrier satisfy only
31 part of the requirements of this section, the Secretary may accept the
32 submission, but shall require submission by the railroad carrier of addi-
33 tional information relevant to the vulnerability assessment and security
34 plan of the railroad carrier to ensure that the remaining requirements
35 of this section are fulfilled.

36 (4) NOTIFICATION.—If the Secretary determines that particular ex-
37 isting procedures, protocols, or standards of a railroad carrier under
38 this subsection do not satisfy the requirements of this section, the Sec-
39 retary shall provide to the railroad carrier a written notification that
40 includes an explanation of the determination.

1 (5) REVIEW.—Nothing in this subsection shall relieve the Secretary
2 of the obligation—

3 (A) to review the vulnerability assessment and security plan
4 submitted by a railroad carrier under this section; and

5 (B) to approve or disapprove each submission on an individual
6 basis.

7 (j) PERIODIC EVALUATION BY RAILROAD CARRIERS REQUIRED.—

8 (1) SUBMISSION.—Not later than 3 years after the date on which
9 a vulnerability assessment or security plan required to be submitted to
10 the Secretary under subsection (c) is approved, and at least once every
11 5 years after the approval (or on another schedule the Secretary may
12 establish by regulation), a railroad carrier who submitted a vulner-
13 ability assessment and security plan and who is still assigned to the
14 high-risk tier must submit to the Secretary an evaluation of the ade-
15 quacy of the vulnerability assessment and security plan that includes
16 a description of material changes made to the vulnerability assessment
17 or security plan.

18 (2) REVIEW.—Not later than 180 days after the date on which an
19 evaluation is submitted, the Secretary shall review the evaluation and
20 notify the railroad carrier submitting the evaluation of the Secretary's
21 approval or disapproval of the evaluation.

22 (k) SHARED FACILITIES.—The Secretary may permit under this section
23 the development and implementation of coordinated vulnerability assess-
24 ments and security plans to the extent that a railroad carrier shares faci-
25 lities with, or is co-located with, other transportation entities or providers
26 that are required to develop vulnerability assessments and security plans
27 under Federal law.

28 (l) CONSULTATION.—In carrying out this section, the Secretary shall con-
29 sult with railroad carriers, nonprofit employee labor organizations represen-
30 tation railroad employees, and public safety and law enforcement officials.

31 **§ 40713. Railroad security assistance**

32 (a) SECURITY IMPROVEMENT GRANTS.—

33 (1) IN GENERAL.—The Secretary, in consultation with the Adminis-
34 trator of the Transportation Security Administration and other appro-
35 priate agencies or officials, may make grants to railroad carriers, the
36 Alaska Railroad, security-sensitive materials offerors who ship by rail-
37 road, owners of railroad cars used in the transportation of security-sen-
38 sitive materials, State and local governments (for railroad passenger fa-
39 cilities and infrastructure not owned by Amtrak), and Amtrak for
40 intercity passenger railroad and freight railroad security improvements
41 described in subsection (b) as approved by the Secretary.

1 (2) GRANT ELIGIBILITY.—A railroad carrier is eligible for a grant
2 under this section if the carrier has completed a vulnerability assess-
3 ment and developed a security plan that the Secretary has approved
4 under section 40712 of this title.

5 (3) USE OF GRANTS.—A recipient of a grant under this section may
6 use grant funds only for permissible uses under subsection (b) to fur-
7 ther a railroad security plan that meets the requirements of paragraph
8 (2).

9 (4) GRANTS FOR ASSESSMENTS AND PLANS.—Notwithstanding the
10 requirement for eligibility and uses of funds in paragraphs (2) and (3),
11 a railroad carrier is eligible for a grant under this section if the carrier
12 uses the funds solely for the development of assessments or security
13 plans under section 40712.

14 (b) USES OF FUNDS.—A recipient of a grant under this section shall use
15 the grant funds for one or more of the following:

16 (1) Security and redundancy for critical communications, computer,
17 and train control systems essential for secure railroad operations.

18 (2) Accommodation of railroad cargo or passenger security inspection
19 facilities, related infrastructure, and operations at or near United
20 States international borders or other ports of entry.

21 (3) The security of security-sensitive materials transportation by rail-
22 road.

23 (4) Chemical, biological, radiological, or explosive detection, including
24 canine patrols for detection.

25 (5) The security of intercity passenger railroad stations, trains, and
26 infrastructure, including security capital improvement projects that the
27 Secretary determines enhance railroad station security.

28 (6) Technologies to reduce the vulnerabilities of railroad cars, includ-
29 ing structural modification of railroad cars transporting security-sen-
30 sitive materials to improve their resistance to acts of terrorism.

31 (7) The sharing of intelligence and information about security
32 threats.

33 (8) To obtain train tracking and communications equipment, includ-
34 ing equipment that is interoperable with Federal, State, and local agen-
35 cies and tribal governments.

36 (9) To hire, train, and employ police and security officers, including
37 canine units, assigned to full-time security or counterterrorism duties
38 related to railroad transportation.

39 (10) Overtime reimbursement, including reimbursement of State,
40 local, and tribal governments for costs, for enhanced security personnel
41 assigned to duties related to railroad security during periods of high

1 or severe threat levels and National Special Security Events or other
2 periods of heightened security as determined by the Secretary.

3 (11) Perimeter protection systems, including access control, installa-
4 tion of improved lighting, fencing, and barricades at railroad facilities.

5 (12) Tunnel protection systems.

6 (13) Passenger evacuation and evacuation-related capital improve-
7 ments.

8 (14) Railroad security inspection technologies, including verified vis-
9 ual inspection technologies using hand-held readers.

10 (15) Surveillance equipment.

11 (16) Cargo or passenger screening equipment.

12 (17) Emergency response equipment, including fire suppression and
13 decontamination equipment, personal protective equipment, and
14 defibrillators.

15 (18) Operating and capital costs associated with security awareness,
16 preparedness, and response training, including training under section
17 40716 of this title, and training developed by universities, institutions
18 of higher education, and nonprofit employee labor organizations, for
19 railroad employees, including frontline employees.

20 (19) Live or simulated exercises, including exercises described in sec-
21 tion 40715 of this title.

22 (20) Public awareness campaigns for enhanced railroad security.

23 (21) Development of assessments or security plans under section
24 40712 of this title.

25 (22) Other security improvements—

26 (A) identified, required, or recommended under sections 40711
27 and 40712 of this title, including infrastructure, facilities, and
28 equipment upgrades; or

29 (B) that the Secretary considers appropriate.

30 (c) DEPARTMENTAL RESPONSIBILITIES.—In carrying out the responsibil-
31 ities under subsection (a), the Secretary shall—

32 (1) determine the requirements for recipients of grants;

33 (2) establish priorities for uses of funds for grant recipients;

34 (3) award the funds authorized by this section based on risk, as
35 identified by the plans required under sections 40711 and 40712 of
36 this title;

37 (4) take into account whether stations or facilities are used by com-
38 muter railroad passengers as well as intercity railroad passengers in re-
39 viewing grant applications;

40 (5) encourage non-Federal financial participation in projects funded
41 by grants; and

1 (6) not later than 5 business days after awarding a grant to Amtrak
 2 under this section, transfer grant funds to the Secretary of Transpor-
 3 tation to be disbursed to Amtrak.

4 (d) MULTIYEAR AWARDS.—Grant funds awarded under this section may
 5 be awarded for projects that span multiple years.

6 (e) LIMITATION ON USES OF FUNDS.—A grant made under this section
 7 may not be used to make a State or local government cost-sharing contribu-
 8 tion under any other Federal law.

9 (f) ANNUAL REPORTS.—Each recipient of a grant under this section shall
 10 report annually to the Secretary on the use of grant funds.

11 (g) SUBJECT TO CERTAIN STANDARDS.—A recipient of a grant under
 12 this section and section 40714 of this title shall be required to comply with
 13 the standards of section 24312 of title 49, as in effect on January 1, 2007,
 14 with respect to the project, in the same manner as Amtrak is required to
 15 comply with the standards for construction work financed under an agree-
 16 ment made under section 24308(a) of title 49.

17 **§ 40714. Systemwide Amtrak security upgrades**

18 (a) IN GENERAL.—

19 (1) GRANTS.—Subject to subsection (b), the Secretary, in consulta-
 20 tion with the Administrator of the Transportation Security Administra-
 21 tion, may make grants to Amtrak under this section.

22 (2) GENERAL PURPOSES.—The Secretary may make grants for the
 23 purposes of—

- 24 (A) protecting underwater and underground assets and systems;
- 25 (B) protecting high-risk and high-consequence assets identified
 26 through system-wide risk assessments;
- 27 (C) providing counterterrorism or security training;
- 28 (D) providing both visible and unpredictable deterrence; and
- 29 (E) conducting emergency preparedness drills and exercises.

30 (3) SPECIFIC PROJECTS.—The Secretary shall make grants—

- 31 (A) to secure major tunnel access points and ensure tunnel in-
 32 tegrity in New York, New Jersey, Maryland, and Washington, DC;
- 33 (B) to secure Amtrak trains;
- 34 (C) to secure Amtrak stations;
- 35 (D) to obtain a watchlist identification system approved by the
 36 Secretary;
- 37 (E) to obtain train tracking and interoperable communications
 38 systems that are coordinated with Federal, State, and local agen-
 39 cies and tribal governments to the maximum extent possible;

1 (F) to hire, train, and employ police and security officers, in-
2 cluding canine units, assigned to full-time security or counterter-
3 rorism duties related to railroad transportation;

4 (G) for operating and capital costs associated with security
5 awareness, preparedness, and response training, including training
6 under section 40716 of this title, and training developed by univer-
7 sities, institutions of higher education, and nonprofit employee
8 labor organizations, for railroad employees, including frontline em-
9 ployees; and

10 (H) for live or simulated exercises, including exercises described
11 in section 40715 of this title.

12 (b) CONDITIONS.—The Secretary shall award grants to Amtrak under
13 this section for projects contained in a system-wide security plan approved
14 by the Secretary developed under section 40712 of this title. Not later than
15 5 business days after awarding a grant to Amtrak under this section, the
16 Secretary shall transfer the grant funds to the Secretary of Transportation
17 to be disbursed to Amtrak.

18 (c) EQUITABLE GEOGRAPHIC ALLOCATION.—The Secretary shall ensure
19 that, subject to meeting the highest security needs on Amtrak’s entire sys-
20 tem and consistent with the risk assessment required under section 40711
21 of this title and Amtrak’s vulnerability assessment and security plan devel-
22 oped under section 40712 of this title, stations and facilities located outside
23 of the Northeast Corridor receive an equitable share of the security funds
24 authorized by this section.

25 **§ 40715. Railroad carrier exercises**

26 (a) IN GENERAL.—The Secretary shall establish a program for con-
27 ducting security exercises for railroad carriers for the purpose of assessing
28 and improving the capabilities of entities described in subsection (b) to pre-
29 vent, prepare for, mitigate, respond to, and recover from acts of terrorism.

30 (b) COVERED ENTITIES.—Entities to be assessed under the program in-
31 clude—

32 (1) Federal, State, and local agencies and tribal governments;

33 (2) railroad carriers;

34 (3) governmental and nongovernmental emergency response pro-
35 viders, law enforcement agencies, and railroad and transit police, as ap-
36 propriate; and

37 (4) any other organization or entity that the Secretary determines
38 appropriate.

39 (c) REQUIREMENTS.—The Secretary shall ensure that the program—

40 (1) consolidates existing security exercises for railroad carriers ad-
41 ministered by the Department and the Department of Transportation,

1 as jointly determined by the Secretary and the Secretary of Transpor-
2 tation, unless the Secretary waives this consolidation requirement as
3 appropriate;

4 (2) consists of exercises that are—

5 (A) scaled and tailored to the needs of the carrier, including ad-
6 dressing the needs of the elderly and individuals with disabilities;

7 (B) live, in the case of the facilities most at risk to a terrorist
8 attack;

9 (C) coordinated with appropriate officials;

10 (D) as realistic as practicable and based on current risk assess-
11 ments, including credible threats, vulnerabilities, and con-
12 sequences;

13 (E) inclusive, as appropriate, of railroad frontline employees;
14 and

15 (F) consistent with the National Incident Management System,
16 the National Response Plan, the National Infrastructure Protec-
17 tion Plan, the National Preparedness Guidance, the National Pre-
18 paredness Goal, and other national initiatives of this type;

19 (3) provides that exercises described in paragraph (2) will be—

20 (A) evaluated by the Secretary against clear and consistent per-
21 formance measures;

22 (B) assessed by the Secretary to identify best practices, which
23 shall be shared, as appropriate, with railroad carriers, nonprofit
24 employee organizations that represent railroad carrier employees,
25 Federal, State, local, and tribal officials, governmental and non-
26 governmental emergency response providers, law enforcement per-
27 sonnel, including railroad carrier and transit police, and other
28 stakeholders; and

29 (C) used to develop recommendations, as appropriate, from the
30 Secretary to railroad carriers on remedial action to be taken in re-
31 sponse to lessons learned;

32 (4) allows for proper advanced notification of communities and local
33 governments in which exercises are held, as appropriate; and

34 (5) assists State, local, and tribal governments and railroad carriers
35 in designing, implementing, and evaluating additional exercises that
36 conform to the requirements of paragraph (1).

37 (d) NATIONAL EXERCISE PROGRAM.—The Secretary shall ensure that the
38 exercise program developed under subsection (c) is a component of the na-
39 tional exercise program established under section 20508 of this title.

1 **§ 40716. Railroad security training program**

2 (a) IN GENERAL.—The Secretary shall develop and issue regulations for
3 a training program to prepare railroad frontline employees for potential se-
4 curity threats and conditions. The regulations shall take into consideration
5 current security training requirements or best practices.

6 (b) CONSULTATION.—The Secretary shall develop the regulations under
7 subsection (a) in consultation with—

8 (1) appropriate law enforcement, fire service, emergency response,
9 security, and terrorism experts;

10 (2) railroad carriers;

11 (3) railroad shippers; and

12 (4) nonprofit employee labor organizations representing railroad em-
13 ployees or emergency response personnel.

14 (c) PROGRAM ELEMENTS.—The regulations developed under subsection
15 (a) shall require security training programs described in subsection (a) to
16 include, at a minimum, elements to address the following, as applicable:

17 (1) Determination of the seriousness of an occurrence or threat.

18 (2) Crew and passenger communication and coordination.

19 (3) Appropriate responses to defend or protect oneself.

20 (4) Use of personal and other protective equipment.

21 (5) Evacuation procedures for passengers and railroad employees, in-
22 cluding individuals with disabilities and the elderly.

23 (6) Psychology, behavior, and methods of terrorists, including obser-
24 vation and analysis.

25 (7) Training related to psychological responses to terrorist incidents,
26 including the ability to cope with hijacker behavior and passenger re-
27 sponses.

28 (8) Live situational training exercises regarding various threat condi-
29 tions, including tunnel evacuation procedures.

30 (9) Recognition and reporting of dangerous substances, suspicious
31 packages, and situations.

32 (10) Understanding security incident procedures, including proce-
33 dures for communicating with governmental and nongovernmental
34 emergency response providers and for on-scene interaction with emer-
35 gency response providers.

36 (11) Operation and maintenance of security equipment and systems.

37 (12) Other security training activities that the Secretary considers
38 appropriate.

39 (d) SUBMITTING PROGRAM TO SECRETARY FOR APPROVAL.—Each rail-
40 road carrier shall develop a security training program under this section and
41 submit the program to the Secretary for approval. Not later than 60 days

1 after receiving a security training program proposal under this subsection,
2 the Secretary shall approve the program or require the railroad carrier that
3 developed the program to make revisions to the program that the Secretary
4 considers necessary for the program to meet the requirements of this sec-
5 tion. A railroad carrier shall respond to the Secretary's comments within 30
6 days after receiving them.

7 (e) TRAINING.—Not later than 1 year after the Secretary approves a se-
8 curity training program under subsection (d), the railroad carrier that devel-
9 oped the program shall complete the training of all railroad frontline em-
10 ployees who were hired by a carrier more than 30 days preceding the ap-
11 proval date. For employees employed by a carrier for fewer than 30 days
12 preceding the approval date, training shall be completed within the first 60
13 days of employment.

14 (f) UPDATES OF REGULATIONS AND PROGRAM REVISIONS.—The Sec-
15 retary periodically shall review and update as appropriate the training regu-
16 lations issued under subsection (a) to reflect new or changing security
17 threats. Each railroad carrier shall revise its training program accordingly
18 and provide additional training as necessary to its frontline employees with-
19 in a reasonable time after the regulations are updated.

20 (g) PROGRAM COMPONENT OF NATIONAL TRAINING PROGRAM.—The
21 Secretary shall ensure that the training program developed under subsection
22 (a) is a component of the national training program established under sec-
23 tion 20508 of this title.

24 (h) OTHER EMPLOYEES.—The Secretary shall issue guidance and best
25 practices for a railroad shipper employee security program containing the
26 elements listed under subsection (c).

27 **§ 40717. Railroad security research and development**

28 (a) ESTABLISHMENT OF RESEARCH AND DEVELOPMENT PROGRAM.—The
29 Secretary, acting through the Under Secretary for Science and Technology
30 and the Administrator of the Transportation Security Administration, shall
31 carry out a research and development program for the purpose of improving
32 the security of railroad transportation systems.

33 (b) ELIGIBLE PROJECTS.—The research and development program may
34 include projects—

35 (1) to reduce the vulnerability of passenger trains, stations, and
36 equipment to explosives and hazardous chemical, biological, and radio-
37 active substances, including the development of technology to screen
38 passengers in large numbers at peak commuting times with minimal in-
39 terference and disruption;

40 (2) to test new emergency response and recovery techniques and
41 technologies, including those used at international borders;

- 1 (3) to develop improved railroad security technologies, including—
 2 (A) technologies for sealing or modifying railroad tank cars;
 3 (B) automatic inspection of railroad cars;
 4 (C) communication-based train control systems;
 5 (D) emergency response training, including training in a tunnel
 6 environment;
 7 (E) security and redundancy for critical communications, elec-
 8 trical power, computer, and train control systems; and
 9 (F) technologies for securing bridges and tunnels;
 10 (4) to test wayside detectors that can detect tampering;
 11 (5) to support enhanced security for the transportation of security-
 12 sensitive materials by railroad;
 13 (6) to mitigate damages in the event of a cyberattack; and
 14 (7) to address other vulnerabilities and risks identified by the Sec-
 15 retary.
- 16 (e) COORDINATION WITH OTHER RESEARCH INITIATIVES.—The Sec-
 17 retary—
- 18 (1) shall ensure that the research and development program is con-
 19 sistent with the National Strategy for Railroad Transportation Security
 20 developed under section 40711 of this title and other transportation se-
 21 curity research and development programs required by section 30304
 22 and chapters 401 through 407 of this title;
- 23 (2) shall, to the extent practicable, coordinate the research and de-
 24 velopment activities of the Department with other ongoing research and
 25 development security-related initiatives, including research being con-
 26 ducted by—
- 27 (A) the Department of Transportation, including University
 28 Transportation Centers and other institutes, centers, and simula-
 29 tors funded by the Department of Transportation;
- 30 (B) the National Academy of Sciences;
- 31 (C) the Technical Support Working Group;
- 32 (D) other Federal departments and agencies; and
- 33 (E) other Federal and private research laboratories, research
 34 entities, and universities and institutions of higher education, in-
 35 cluding Historically Black Colleges and Universities, Hispanic
 36 Serving Institutions, or Indian Tribally Controlled Colleges and
 37 Universities;
- 38 (3) shall carry out a research and development project authorized by
 39 this section through a reimbursable agreement with an appropriate
 40 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, or enter into cooperative agreements, con-
6 tracts, other transactions, or reimbursable agreements with, the entities
7 described in paragraph (2) and eligible grant recipients under section
8 40713 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 railroad carriers willing to contribute both physical space
12 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 10543 of this title.

19 (2) PRIVACY IMPACT ASSESSMENTS.—In accordance with sections
20 10543 and 11505 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, for 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 **§ 40718. Railroad tank car security testing**

26 (a) VULNERABILITY ASSESSMENT.—

27 (1) LIKELY METHODS AND SUCCESS.—The Secretary shall assess the
28 likely methods of a deliberate terrorist attack against a railroad tank
29 car used to transport toxic-inhalation-hazard materials, and for each
30 method assessed, the degree to which it may be successful in causing
31 death, injury, or serious adverse effects to human health, the environ-
32 ment, critical infrastructure, national security, the national economy, or
33 public welfare.

34 (2) THREATS.—In carrying out paragraph (1), the Secretary shall
35 consider the most current threat information as to likely methods of
36 a successful terrorist attack on a railroad tank car transporting toxic-
37 inhalation-hazard materials, and may consider the following:

38 (A) Explosive devices placed along the tracks or attached to a
39 railroad tank car.

40 (B) The use of missiles, grenades, rockets, mortars, or other
41 high-caliber weapons against a railroad tank car.

1 (3) PHYSICAL TESTING.—In developing the assessment required
 2 under paragraph (1), the Secretary shall conduct physical testing of the
 3 vulnerability of railroad tank cars used to transport toxic-inhalation-
 4 hazard materials to different methods of a deliberate attack, using
 5 technical information and criteria to evaluate the structural integrity
 6 of railroad tank cars.

7 (b) DISPERSION MODELING.—

8 (1) IN GENERAL.—The Secretary, acting through the National Infra-
 9 structure Simulation and Analysis Center, shall conduct an air disper-
 10 sion modeling analysis of release scenarios of toxic-inhalation-hazard
 11 materials resulting from a terrorist attack on a loaded railroad tank
 12 car carrying these materials in urban and rural environments.

13 (2) CONSIDERATIONS.—The analysis under this subsection shall take
 14 into account the following considerations:

15 (A) The most likely means of attack and the resulting dispersal
 16 rate.

17 (B) Different times of day, to account for differences in cloud
 18 coverage and other atmospheric conditions in the environment
 19 being modeled.

20 (C) Differences in population size and density.

21 (D) Historically accurate wind speeds, temperatures, and wind
 22 directions.

23 (E) Differences in dispersal rates or other relevant factors re-
 24 lated to whether a railroad tank car is in motion or stationary.

25 (F) Emergency response procedures by local officials.

26 (G) Other considerations the Secretary believes would develop
 27 an accurate, plausible dispersion model for toxic-inhalation-hazard
 28 materials released from a railroad tank car as a result of a ter-
 29 rorist act.

30 (3) CONSULTATION.—In conducting the dispersion modeling under
 31 paragraph (1), the Secretary shall consult with the Secretary of Trans-
 32 portation, hazardous materials experts, railroad carriers, nonprofit em-
 33 ployee labor organizations representing railroad employees, appropriate
 34 State, local, and tribal officials, and other Federal agencies, as appro-
 35 priate.

36 (4) INFORMATION SHARING.—On completion of the analysis required
 37 under paragraph (1), the Secretary shall share the information devel-
 38 oped with the appropriate stakeholders, given appropriate information
 39 protection provisions as may be required by the Secretary.

40 **§ 40719. Security background checks of covered individuals**

41 (a) DEFINITIONS.—In this section:

1 (1) COVERED INDIVIDUAL.—The term “covered individual” means
2 an employee of a railroad carrier or a contractor or subcontractor of
3 a railroad carrier.

4 (2) SECURITY BACKGROUND CHECK.—The term “security back-
5 ground check” means for the purpose of identifying individuals who
6 may pose a threat to transportation security or national security, or of
7 terrorism—

8 (A) relevant criminal history databases;

9 (B) in the case of an alien (as defined in section 101 of the Im-
10 migration and Nationality Act (8 U.S.C. 1101), the relevant data-
11 bases to determine the status of the alien under the immigration
12 laws of the United States; and

13 (C) other relevant information or databases, as determined by
14 the Secretary.

15 (b) GUIDANCE.—

16 (1) IN GENERAL.—Guidance, recommendations, suggested action
17 items, and other widely disseminated voluntary action items issued by
18 the Secretary to a railroad carrier or a contractor or subcontractor of
19 a railroad carrier relating to performing a security background check
20 of a covered individual shall contain recommendations on the appro-
21 priate scope and application of a security background check, including
22 the time period covered, the types of disqualifying offenses, and a re-
23 dress process for adversely impacted covered individuals consistent with
24 subsections (c) and (d).

25 (2) UPDATE OF EXISTING GUIDANCE.—Guidance, recommendations,
26 suggested action items, and other widely disseminated voluntary action
27 items issued by the Secretary prior to August, 3, 2007, to a railroad
28 carrier or a contractor or subcontractor of a railroad carrier relating
29 to performing a security background check of a covered individual shall
30 be updated in compliance with paragraph (1).

31 (3) NECESSARY REDRESS PROCEDURE.—If a railroad carrier or a
32 contractor or subcontractor of a railroad carrier performs a security
33 background check on a covered individual to fulfill guidance issued by
34 the Secretary under paragraph (1) or (2), the Secretary shall not con-
35 sider the guidance fulfilled unless an adequate redress process as de-
36 scribed in subsection (d) is provided to covered individuals.

37 (c) REQUIREMENTS.—If the Secretary issues a rule, regulation, or direc-
38 tive requiring a railroad carrier or contractor or subcontractor of a railroad
39 carrier to perform a security background check of a covered individual, the
40 Secretary shall prohibit the railroad carrier or contractor or subcontractor
41 of a railroad carrier from making an adverse employment decision, including

1 removal or suspension of the covered individual, due to the rule, regulation,
2 or directive with respect to a covered individual unless the railroad carrier
3 or contractor or subcontractor of a railroad carrier determines that the covered
4 individual—

5 (1) has been convicted of, has been found not guilty by reason of
6 insanity, or is under warrant, or indictment for a permanent dis-
7 qualifying criminal offense listed in part 1572 of title 49, Code of Fed-
8 eral Regulations;

9 (2) was convicted of or found not guilty by reason of insanity of an
10 interim disqualifying criminal offense listed in part 1572 of title 49,
11 Code of Federal Regulations, within 7 years of the date that the rail-
12 road carrier or contractor or subcontractor of a railroad carrier per-
13 forms the security background check; or

14 (3) was incarcerated for an interim disqualifying criminal offense
15 listed in part 1572 of title 49, Code of Federal Regulations, and re-
16 leased from incarceration within 5 years of the date that the railroad
17 carrier or contractor or subcontractor of a railroad carrier performs the
18 security background check.

19 (d) REDRESS PROCESS.—If the Secretary issues a rule, regulation, or di-
20 rective requiring a railroad carrier or contractor or subcontractor of a rail-
21 road carrier to perform a security background check of a covered individual,
22 the Secretary shall—

23 (1) provide an adequate redress process for a covered individual sub-
24 jected to an adverse employment decision, including removal or suspen-
25 sion of the employee, due to the rule, regulation, or directive that is
26 consistent with the appeals and waiver process established for appli-
27 cants for commercial motor vehicle hazardous materials endorsements
28 and transportation employees at ports, as required by section 70105(c)
29 of title 46; and

30 (2) have the authority to order an appropriate remedy, including re-
31 instatement of the covered individual, should the Secretary determine
32 that a railroad carrier or contractor or subcontractor of a railroad car-
33 rier wrongfully made an adverse employment decision regarding a cov-
34 ered individual pursuant to the rule, regulation, or directive.

35 (e) FALSE STATEMENTS.—A railroad carrier or a contractor or subcon-
36 tractor of a railroad carrier may not knowingly misrepresent to an employee
37 or other relevant person, including an arbiter involved in a labor arbitration,
38 the scope, application, or meaning of rules, regulations, directives, or guid-
39 ance issued by the Secretary related to security background check require-
40 ments for covered individuals when conducting a security background check.
41 The Secretary shall issue a regulation that prohibits a railroad carrier or

1 a contractor or subcontractor of a railroad carrier from knowingly misrepresenting to an employee or other relevant person, including an arbiter involved in a labor arbitration, the scope, application, or meaning of rules, regulations, directives, or guidance issued by the Secretary related to security background check requirements for covered individuals when conducting a security background check.

7 (f) RIGHTS AND RESPONSIBILITIES.—Nothing in this section shall be construed to abridge a railroad carrier’s or a contractor or subcontractor of a railroad carrier’s rights or responsibilities to make adverse employment decisions permitted by other Federal, State, or local laws. Nothing in this section shall be construed to abridge rights and responsibilities of covered individuals, a railroad carrier, or a contractor or subcontractor of a railroad carrier, under other Federal, State, or local laws or under a collective bargaining agreement.

15 (g) NO PREEMPTION OF FEDERAL OR STATE LAW.—Nothing in this section shall be construed to preempt a Federal, State, or local law that requires criminal history background checks, immigration status checks, or other background checks, of covered individuals.

19 (h) PROCESS FOR REVIEW NOT AFFECTED.—Nothing in this section shall be construed to affect the process for review established under section 70105(c) of title 46, including regulations issued under that section.

22 **§ 40720. International railroad security program**

23 (a) DEFINITIONS.—In this section:

24 (1) INSPECTION.—The term “inspection” means the comprehensive process used by U.S. Customs and Border Protection to assess goods entering the United States to appraise them for duty purposes, to detect the presence of restricted or prohibited items, and to ensure compliance with all applicable laws.

29 (2) INTERNATIONAL SUPPLY CHAIN.—The term “international supply chain” means the end-to-end process for shipping goods to or from the United States, beginning at the point of origin (including manufacturer, supplier, or vendor) through a point of distribution to the destination.

34 (3) RADIATION DETECTION EQUIPMENT.—The term “radiation detection equipment” means technology that is capable of detecting or identifying nuclear and radiological material or nuclear and radiological explosive devices.

38 (b) IN GENERAL.—

39 (1) DETECTION SYSTEM.—The Secretary shall develop a system to detect both undeclared passengers and contraband, with a primary

1 focus on the detection of nuclear and radiological materials entering
2 the United States by railroad.

3 (2) SYSTEM REQUIREMENTS.—In developing the system under para-
4 graph (1), the Secretary may, in consultation with the Domestic Nu-
5 clear Detection Office, U.S. Customs and Border Protection, and
6 Transportation Security Administration—

7 (A) deploy radiation detection equipment and nonintrusive im-
8 aging equipment at locations where railroad shipments cross an
9 international border to enter the United States;

10 (B) consider the integration of radiation detection technologies
11 with other nonintrusive inspection technologies where feasible;

12 (C) ensure appropriate training, operations, and response proto-
13 cols are established for Federal, State, and local personnel;

14 (D) implement alternative procedures to check railroad ship-
15 ments at locations where the deployment of nonintrusive inspection
16 imaging equipment is determined to not be practicable;

17 (E) ensure, to the extent practicable, that the technologies de-
18 ployed can detect terrorists or weapons, including weapons of mass
19 destruction; and

20 (F) take other actions, as appropriate, to develop the system.

21 (c) ADDITIONAL INFORMATION.—The Secretary shall—

22 (1) identify and seek the submission of additional data elements for
23 improved high-risk targeting related to the movement of cargo through
24 the international supply chain utilizing a railroad prior to importation
25 into the United States;

26 (2) utilize data collected and maintained by the Secretary of Trans-
27 portation in the targeting of high-risk cargo identified under paragraph
28 (1); and

29 (3) analyze the data provided in this subsection to identify high-risk
30 cargo for inspection.

31 **Subchapter III—Over-the-Road Bus** 32 **Security**

33 **§ 40731. Assessments and plans**

34 (a) IN GENERAL.—The Secretary shall issue regulations that—

35 (1) require each over-the-road bus operator assigned to a high-risk
36 tier under this section—

37 (A) to conduct a vulnerability assessment under subsections (c)
38 and (d); and

39 (B) to prepare, submit to the Secretary for approval, and imple-
40 ment a security plan under subsection (e); and

1 (2) establish standards and guidelines for developing and imple-
2 menting the vulnerability assessments and security plans for carriers
3 assigned to high-risk tiers consistent with this section.

4 (b) NON HIGH-RISK PROGRAMS.—The Secretary may establish a security
5 program for over-the-road bus operators not assigned to a high-risk tier, in-
6 cluding—

7 (1) guidance for operators in conducting vulnerability assessments
8 and preparing and implementing security plans, as determined appro-
9 priate by the Secretary; and

10 (2) a process to review and approve the assessments and plans, as
11 appropriate.

12 (c) SUBMISSION OF ASSESSMENTS AND SECURITY PLANS.—The vulner-
13 ability assessments and security plans required by the regulations for over-
14 the-road bus operators assigned to a high-risk tier shall be completed and
15 submitted to the Secretary for review and approval.

16 (d) VULNERABILITY ASSESSMENTS.—

17 (1) REQUIREMENTS.—The Secretary shall provide technical assist-
18 ance and guidance to over-the-road bus operators in conducting vulner-
19 ability assessments under this section and shall require that each vul-
20 nerability assessment of an operator assigned to a high-risk tier under
21 this section includes, as appropriate—

22 (A) identification and evaluation of critical assets and infra-
23 structure, including platforms, stations, terminals, and information
24 systems;

25 (B) identification of the vulnerabilities to those assets and infra-
26 structure; and

27 (C) identification of weaknesses in—

28 (i) physical security;

29 (ii) passenger and cargo security;

30 (iii) the security of programmable electronic devices, com-
31 puters, or other automated systems which are used in pro-
32 viding over-the-road bus transportation;

33 (iv) alarms, cameras, and other protection systems;

34 (v) communications systems and utilities needed for over-
35 the-road bus security purposes, including dispatching systems;

36 (vi) emergency response planning;

37 (vii) employee training; and

38 (viii) other matters the Secretary determines appropriate.

39 (2) THREAT INFORMATION.—The Secretary shall provide in a timely
40 manner to the appropriate employees of an over-the-road bus operator,
41 as designated by the over-the-road bus operator, threat information

1 that is relevant to the operator when preparing and submitting a vul-
2 nerability assessment and security plan, including an assessment of the
3 most likely methods that could be used by terrorists to exploit weak-
4 nesses in over-the-road bus security.

5 (e) SECURITY PLANS.—

6 (1) REQUIREMENTS.—The Secretary shall provide technical assist-
7 ance and guidance to over-the-road bus operators in preparing and im-
8 plementing security plans under this section and shall require that each
9 security plan of an over-the-road bus operator assigned to a high-risk
10 tier under this section includes, as appropriate—

11 (A) the identification of a security coordinator having author-
12 ity—

13 (i) to implement security actions under the plan;

14 (ii) to coordinate security improvements; and

15 (iii) to receive communications from appropriate Federal
16 officials regarding over-the-road bus security;

17 (B) a list of needed capital and operational improvements;

18 (C) procedures to be implemented or used by the over-the-road
19 bus operator in response to a terrorist attack, including evacuation
20 and passenger communication plans that include individuals with
21 disabilities, as appropriate;

22 (D) the identification of steps taken with State and local law
23 enforcement agencies, emergency responders, and Federal officials
24 to coordinate security measures and plans for response to a ter-
25 rorist attack;

26 (E) a strategy and timeline for conducting training under sec-
27 tion 40734 of this title;

28 (F) enhanced security measures to be taken by the over-the-
29 road bus operator when the Secretary declares a period of height-
30 ened security risk;

31 (G) plans for providing redundant and backup systems required
32 to ensure the continued operation of critical elements of the over-
33 the-road bus operator's system in the event of a terrorist attack
34 or other incident; and

35 (H) other actions or procedures the Secretary determines are
36 appropriate to address the security of over-the-road bus operators.

37 (2) SECURITY COORDINATOR REQUIREMENTS.—The Secretary shall
38 require that the individual serving as the security coordinator identified
39 in paragraph (1)(A) is a citizen of the United States. The Secretary
40 may waive this requirement with respect to an individual if the Sec-
41 retary determines that it is appropriate to do so based on a background

1 check of the individual and a review of the consolidated terrorist
2 watchlist.

3 (f) DEADLINE FOR REVIEW PROCESS.—Not later than 6 months after re-
4 ceiving the assessments and plans required under this section, the Secretary
5 shall—

6 (1) review each vulnerability assessment and security plan submitted
7 to the Secretary under subsection (c);

8 (2) require amendments to a security plan that does not meet the
9 requirements of this section; and

10 (3) approve a vulnerability assessment or security plan that meets
11 the requirements of this section.

12 (g) TIER ASSIGNMENT.—

13 (1) IN GENERAL.—The Secretary shall assign each over-the-road bus
14 operator to a risk-based tier established by the Secretary.

15 (2) PROVIDING INFORMATION.—The Secretary may request, and an
16 over-the-road bus operator shall provide, information necessary for the
17 Secretary to assign an over-the-road bus operator to the appropriate
18 tier under this subsection.

19 (3) NOTIFICATION.—Not later than 60 days after the date an over-
20 the-road bus operator is assigned to a tier under this section, the Sec-
21 retary shall notify the operator of the tier to which it is assigned and
22 the reasons for the assignment.

23 (4) HIGH-RISK TIERS.—At least one of the tiers established by the
24 Secretary under this section shall be a tier designated for high-risk
25 over-the-road bus operators.

26 (5) REASSIGNMENT.—The Secretary may reassign an over-the-road
27 bus operator to another tier, as appropriate, in response to changes in
28 risk, and the Secretary shall notify the over-the-road bus operator with-
29 in 60 days after the reassignment and provide the operator with the
30 reasons for the reassignment.

31 (h) EXISTING PROCEDURES, PROTOCOLS, AND STANDARDS.—

32 (1) DETERMINATION.—In response to a petition by an over-the-road
33 bus operator or at the discretion of the Secretary, the Secretary may
34 determine that existing procedures, protocols, and standards meet all
35 or part of the requirements of this section regarding vulnerability as-
36 sessments and security plans.

37 (2) ELECTION.—On review and written determination by the Sec-
38 retary that existing procedures, protocols, or standards of an over-the-
39 road bus operator satisfy the requirements of this section, the over-the-
40 road bus operator may elect to comply with those procedures, protocols,
41 or standards instead of the requirements of this section.

1 (3) PARTIAL APPROVAL.—If the Secretary determines that the exist-
2 ing procedures, protocols, or standards of an over-the-road bus oper-
3 ator satisfy only part of the requirements of this section, the Secretary
4 may accept a submission, but shall require submission by the operator
5 of additional information relevant to the vulnerability assessment and
6 security plan of the operator to ensure that the remaining requirements
7 of this section are fulfilled.

8 (4) NOTIFICATION.—If the Secretary determines that particular ex-
9 isting procedures, protocols, or standards of an over-the-road bus oper-
10 ator under this subsection do not satisfy the requirements of this sec-
11 tion, the Secretary shall provide to the operator a written notification
12 that includes an explanation of the reasons for non-acceptance.

13 (5) REVIEW.—Nothing in this subsection shall relieve the Secretary
14 of the obligation—

15 (A) to review the vulnerability assessment and security plan
16 submitted by an over-the-road bus operator under this section; and

17 (B) to approve or disapprove each submission on an individual
18 basis.

19 (i) PERIODIC EVALUATION BY OVER-THE-ROAD BUS PROVIDER RE-
20 QUIRED.—

21 (1) SUBMISSION.—Not later than 3 years after the date on which
22 a vulnerability assessment or security plan required to be submitted to
23 the Secretary under subsection (c) is approved, and at least once every
24 5 years thereafter (or on another schedule the Secretary may establish
25 by regulation), an over-the-road bus operator who submitted a vulner-
26 ability assessment and security plan and who is still assigned to the
27 high-risk tier shall also submit to the Secretary an evaluation of the
28 adequacy of the vulnerability assessment and security plan that in-
29 cludes a description of material changes made to the vulnerability as-
30 sessment or security plan.

31 (2) REVIEW.—Not later than 180 days after the date on which an
32 evaluation is submitted, the Secretary shall review the evaluation and
33 notify the over-the-road bus operator submitting the evaluation of the
34 Secretary's approval or disapproval of the evaluation.

35 (j) SHARED FACILITIES.—The Secretary may permit under this section
36 the development and implementation of coordinated vulnerability assess-
37 ments and security plans to the extent that an over-the-road bus operator
38 shares facilities with, or is co-located with, other transportation entities or
39 providers that are required to develop vulnerability assessments and security
40 plans under Federal law.

41 (k) NONDISCLOSURE OF INFORMATION.—

1 (1) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this
2 section shall be construed as authorizing the withholding of information
3 from Congress.

4 (2) DISCLOSURE OF INDEPENDENTLY FURNISHED INFORMATION.—
5 Nothing in this section shall be construed as affecting the authority or
6 obligation of a Federal agency to disclose a record or information that
7 the Federal agency obtains from an over-the-road bus operator under
8 any other Federal law.

9 **§ 40732. Assistance**

10 (a) IN GENERAL.—The Secretary shall establish a program for making
11 grants to eligible private operators providing transportation by an over-the-
12 road bus for security improvements described in subsection (b).

13 (b) USES OF FUNDS.—A recipient of a grant received under subsection
14 (a) shall use the grant funds for one or more of the following:

15 (1) Constructing and modifying terminals, garages, and facilities, in-
16 cluding terminals and other over-the-road bus facilities owned by State
17 or local governments, to increase their security.

18 (2) Modifying over-the-road buses to increase their security.

19 (3) Protecting or isolating the driver of an over-the-road bus.

20 (4) Acquiring, upgrading, installing, or operating equipment, soft-
21 ware, or accessorial services for collection, storage, or exchange of pas-
22 senger and driver information through ticketing systems or other
23 means and for information links with government agencies, for security
24 purposes.

25 (5) Installing cameras and video surveillance equipment on over-the-
26 road buses and at terminals, garages, and over-the-road bus facilities.

27 (6) Establishing and improving an emergency communications sys-
28 tem linking drivers and over-the-road buses to the recipient's oper-
29 ations center or linking the operations center to law enforcement and
30 emergency personnel.

31 (7) Implementing and operating passenger screening programs for
32 weapons and explosives.

33 (8) Public awareness campaigns for enhanced over-the-road bus se-
34 curity.

35 (9) Operating and capital costs associated with over-the-road bus se-
36 curity awareness, preparedness, and response training, including train-
37 ing under section 40734 of this title and training developed by institu-
38 tions of higher education and by nonprofit employee labor organiza-
39 tions, for over-the-road bus employees, including frontline employees.

40 (10) Chemical, biological, radiological, or explosive detection, includ-
41 ing canine patrols for detection.

1 (11) Overtime reimbursement, including reimbursement of State,
2 local, and tribal governments for costs, for enhanced security personnel
3 assigned to duties related to over-the-road bus security during periods
4 of high or severe threat levels, National Special Security Events, or
5 other periods of heightened security as determined by the Secretary.

6 (12) Live or simulated exercises, including those described in section
7 40733 of this title.

8 (13) Operational costs to hire, train, and employ police and security
9 officers, including canine units, assigned to full-time security or
10 counterterrorism duties related to over-the-road bus transportation, in-
11 cluding reimbursement of State, local, and tribal government costs for
12 the personnel.

13 (14) Development of assessments or security plans under section
14 40731 of this title.

15 (15) Other improvements the Secretary considers appropriate.

16 (e) DUE CONSIDERATION.—In making grants under this section, the Sec-
17 retary shall prioritize grant funding based on security risks to bus pas-
18 sengers and the ability of a project to reduce, or enhance response to, that
19 risk, and shall not penalize private operators of over-the-road buses that
20 took measures to enhance over-the-road bus transportation security prior to
21 September 11, 2001.

22 (d) SECRETARY'S RESPONSIBILITIES.—In carrying out the responsibilities
23 under subsection (a), the Secretary shall—

24 (1) determine the requirements for recipients of grants under this
25 section, including application requirements;

26 (2) select grant recipients;

27 (3) award the funds authorized by this section based on risk, as
28 identified by the plans required under section 40731 of this title or an
29 assessment or plan described in subsection (f)(2); and

30 (4) under subsection (c), establish priorities for the use of funds for
31 grant recipients.

32 (e) DISTRIBUTION OF GRANTS.—The Secretary and the Secretary of
33 Transportation shall determine the most effective and efficient way to dis-
34 tribute grant funds to the recipients of grants determined by the Secretary
35 under subsection (a). Subject to the determination made by the Secretaries,
36 the Secretary may transfer funds to the Secretary of Transportation for the
37 purposes of disbursing funds to the grant recipient.

38 (f) ELIGIBILITY.—

39 (1) IN GENERAL.—A private operator providing transportation by an
40 over-the-road bus is eligible for a grant under this section if the oper-
41 ator has completed a vulnerability assessment and developed a security

1 plan that the Secretary has approved under section 40731 of this title.
2 Grant funds may only be used for permissible uses under subsection
3 (b) to further an over-the-road bus security plan.

4 (2) INTERIM ELIGIBILITY.—Notwithstanding the requirements for
5 eligibility and uses in paragraph (1), the Secretary may award grants
6 under this section for over-the-road bus security improvements listed
7 under subsection (b) based on over-the-road bus vulnerability assess-
8 ments and security plans that the Secretary considers sufficient for the
9 purposes of this section but have not been approved by the Secretary
10 under section 40731 of this title

11 (g) GRANT TERMS AND CONDITIONS.—Except as otherwise specifically
12 provided in this section, a grant made under this section shall be subject
13 to the terms and conditions applicable to subrecipients who provide over-
14 the-road bus transportation under 5311(f) of title 49 and other terms and
15 conditions that the Secretary determines are necessary.

16 (h) LIMITATION ON USES OF FUNDS.—A grant made under this section
17 may not be used to make a State or local government cost-sharing contribu-
18 tion under any other Federal law.

19 (i) ANNUAL REPORTS.—Each recipient of a grant under this section shall
20 report annually to the Secretary on the use of the grant funds.

21 (j) CONSULTATION.—In carrying out this section, the Secretary shall con-
22 sult with over-the-road bus operators and nonprofit employee labor organi-
23 zations representing over-the-road bus employees and public safety and law
24 enforcement officials.

25 **§ 40733. Exercises**

26 (a) IN GENERAL.—The Secretary shall establish a program for con-
27 ducting security exercises for over-the-road bus transportation for the pur-
28 pose of assessing and improving the capabilities of entities described in sub-
29 section (b) to prevent, prepare for, mitigate, respond to, and recover from
30 acts of terrorism.

31 (b) COVERED ENTITIES.—Entities to be assessed under the program in-
32 clude—

33 (1) Federal, State, and local agencies and tribal governments;

34 (2) over-the-road bus operators and over-the-road bus terminal own-
35 ers and operators;

36 (3) governmental and nongovernmental emergency response pro-
37 viders and law enforcement agencies; and

38 (4) other organizations or entities that the Secretary determines ap-
39 propriate.

40 (c) REQUIREMENTS.—The Secretary shall ensure that the program—

1 (1) consolidates existing security exercises for over-the-road bus op-
2 erators and terminals administered by the Department and the Depart-
3 ment of Transportation, as jointly determined by the Secretary and the
4 Secretary of Transportation, unless the Secretary waives this consolida-
5 tion requirement, as appropriate;

6 (2) consists of exercises that are—

7 (A) scaled and tailored to the needs of the over-the-road bus op-
8 erators and terminals, including addressing the needs of the elder-
9 ly and individuals with disabilities;

10 (B) live, in the case of the facilities most at risk to a terrorist
11 attack;

12 (C) coordinated with appropriate officials;

13 (D) as realistic as practicable and based on current risk assess-
14 ments, including credible threats, vulnerabilities, and con-
15 sequences;

16 (E) inclusive, as appropriate, of over-the-road bus frontline em-
17 ployees; and

18 (F) consistent with the National Incident Management System,
19 the National Response Plan, the National Infrastructure Protec-
20 tion Plan, the National Preparedness Guidance, the National Pre-
21 paredness Goal, and other such national initiatives;

22 (3) provides that exercises described in paragraph (2) will be—

23 (A) evaluated by the Secretary against clear and consistent per-
24 formance measures;

25 (B) assessed by the Secretary to identify best practices, which
26 shall be shared, as appropriate, with operators providing over-the-
27 road bus transportation, nonprofit employee organizations that
28 represent over-the-road bus employees, Federal, State, local, and
29 tribal officials, governmental and nongovernmental emergency re-
30 sponse providers, and law enforcement personnel; and

31 (C) used to develop recommendations, as appropriate, provided
32 to over-the-road bus operators and terminal owners and operators
33 on remedial action to be taken in response to lessons learned;

34 (4) allows for proper advanced notification of communities and local
35 governments in which exercises are held, as appropriate; and

36 (5) assists State, local, and tribal governments and over-the-road bus
37 operators and terminal owners and operators in designing, imple-
38 menting, and evaluating additional exercises that conform to the re-
39 quirements of paragraph (2).

40 (d) CONSISTENT WITH NATIONAL EXERCISE PROGRAM.—The Secretary
41 shall ensure that the exercise program developed under subsection (c) is

1 consistent with the national exercise program established under section
2 20508 of this title.

3 **§ 40734. Training program**

4 (a) IN GENERAL.—The Secretary shall develop and issue regulations for
5 an over-the-road bus training program to prepare over-the-road bus front-
6 line employees for potential security threats and conditions. The regulations
7 shall take into consideration current security training requirements or best
8 practices.

9 (b) CONSULTATION.—The Secretary shall develop regulations under sub-
10 section (a) in consultation with—

- 11 (1) appropriate law enforcement, fire service, emergency response,
12 security, and terrorism experts;
- 13 (2) operators providing over-the-road bus transportation; and
- 14 (3) nonprofit employee labor organizations representing over-the-road
15 bus employees and emergency response personnel.

16 (c) PROGRAM ELEMENTS.—The regulations developed under subsection
17 (a) shall require security training programs, to include, at a minimum, ele-
18 ments to address the following, as applicable:

- 19 (1) Determination of the seriousness of an occurrence or threat.
- 20 (2) Driver and passenger communication and coordination.
- 21 (3) Appropriate responses to defend or protect oneself.
- 22 (4) Use of personal and other protective equipment.
- 23 (5) Evacuation procedures for passengers and over-the-road bus em-
24 ployees, including individuals with disabilities and the elderly.
- 25 (6) Psychology, behavior, and methods of terrorists, including obser-
26 vation and analysis.
- 27 (7) Training related to psychological responses to terrorist incidents,
28 including the ability to cope with hijacker behavior and passenger re-
29 sponses.
- 30 (8) Live situational training exercises regarding various threat condi-
31 tions, including tunnel evacuation procedures.
- 32 (9) Recognition and reporting of dangerous substances, suspicious
33 packages, and situations.
- 34 (10) Understanding security incident procedures, including proce-
35 dures for communicating with emergency response providers and for
36 on-scene interaction with emergency response providers.
- 37 (11) Operation and maintenance of security equipment and systems.
- 38 (12) Other security training activities that the Secretary considers
39 appropriate.

40 (d) REQUIRED PROGRAMS.—

1 (1) DEVELOPMENT AND SUBMISSION TO SECRETARY.—Not later
2 than 90 days after the Secretary issues the regulations under sub-
3 section (a), each over-the-road bus operator shall develop a security
4 training program in accordance with the regulations and submit the
5 program to the Secretary for approval.

6 (2) APPROVAL.—Not later than 60 days after receiving a security
7 training program proposal under this subsection, the Secretary shall
8 approve the program or require the over-the-road bus operator that de-
9 veloped the program to make revisions to the program that the Sec-
10 retary considers necessary for the program to meet the requirements
11 of the regulations. An over-the-road bus operator shall respond to the
12 Secretary's comments not later than 30 days after receiving them.

13 (3) TRAINING.—Not later than 1 year after the Secretary approves
14 a security training program under this subsection, the over-the-road
15 bus operator that developed the program shall complete the training of
16 all over-the-road bus frontline employees who were hired by the oper-
17 ator more than 30 days preceding the approval date. For employees
18 employed by an operator for fewer than 30 days preceding the approval
19 date, training shall be completed within the first 60 days of employ-
20 ment.

21 (4) UPDATES OF REGULATIONS AND PROGRAM REVISIONS.—The
22 Secretary shall periodically review and update, as appropriate, the
23 training regulations issued under subsection (a) to reflect new or
24 changing security threats. Each over-the-road bus operator shall revise
25 its training program accordingly and provide additional training as nec-
26 essary to its employees within a reasonable time after the regulations
27 are updated.

28 (e) NATIONAL TRAINING PROGRAM.—The Secretary shall ensure that the
29 training program developed under subsection (a) is a component of the na-
30 tional training program established under section 20508 of this title.

31 **§ 40735. Research and development**

32 (a) IN GENERAL.—The Secretary, acting through the Under Secretary
33 for Science and Technology and the Administrator of the Transportation
34 Security Administration, shall carry out a research and development pro-
35 gram for the purpose of improving the security of over-the-road buses.

36 (b) ELIGIBLE PROJECTS.—The research and development program may
37 include projects—

38 (1) to reduce the vulnerability of over-the-road buses, stations, termi-
39 nals, and equipment to explosives and hazardous chemical, biological,
40 and radioactive substances, including the development of technology to

1 screen passengers in large numbers with minimal interference and dis-
2 ruption;

3 (2) to test new emergency response and recovery techniques and
4 technologies, including those used at international borders;

5 (3) to develop improved technologies, including those for—

6 (A) emergency response training, including training in a tunnel
7 environment, if appropriate; and

8 (B) security and redundancy for critical communications, elec-
9 trical power, computer, and over-the-road bus control systems; and

10 (4) to address other vulnerabilities and risks identified by the Sec-
11 retary.

12 (c) COORDINATION WITH OTHER RESEARCH INITIATIVES.—The Sec-
13 retary—

14 (1) shall ensure that the research and development program is con-
15 sistent with the other transportation security research and development
16 programs required by section 30304 and chapters 401 through 407 of
17 this title;

18 (2) shall, to the extent practicable, coordinate the research and de-
19 velopment activities of the Department with other ongoing research and
20 development security-related initiatives, including research being con-
21 ducted by—

22 (A) the Department of Transportation, including University
23 Transportation Centers and other institutes, centers, and simula-
24 tors funded by the Department of Transportation;

25 (B) the National Academy of Sciences;

26 (C) the Technical Support Working Group;

27 (D) other Federal departments and agencies; and

28 (E) other Federal and private research laboratories, research
29 entities, and institutions of higher education, including Historically
30 Black Colleges and Universities, Hispanic Serving Institutions,
31 and Indian Tribally Controlled Colleges and Universities;

32 (3) shall carry out a research and development project authorized by
33 this section through a reimbursable agreement with an appropriate
34 Federal agency, if the agency—

35 (A) is currently sponsoring a research and development project
36 in a similar area; or

37 (B) has a unique facility or capability that would be useful in
38 carrying out the project;

39 (4) may award grants and enter into cooperative agreements, con-
40 tracts, other transactions, or reimbursable agreements to the entities

1 described in paragraph (2) and eligible recipients under section 40732
2 of this title; and

3 (5) shall make reasonable efforts to enter into memoranda of under-
4 standing, contracts, grants, cooperative agreements, or other trans-
5 actions with private operators providing over-the-road bus transpor-
6 tation willing to contribute assets, physical space, and other resources.

7 (d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES.—

8 (1) CONSULTATION.—In carrying out research and development
9 projects under this section, the Secretary shall consult with the Chief
10 Privacy Officer of the Department and the Officer for Civil Rights and
11 Civil Liberties of the Department as appropriate and under section
12 10543 of this title.

13 (2) PRIVACY IMPACT ASSESSMENTS.—In accordance with sections
14 10543 and 11505 of this title, the Chief Privacy Officer shall conduct
15 privacy impact assessments and the Officer for Civil Rights and Civil
16 Liberties shall conduct reviews, as appropriate, for research and devel-
17 opment initiatives developed under this section that the Secretary de-
18 termines could have an impact on privacy, civil rights, or civil liberties.

19 **Subchapter IV—Hazardous Material and** 20 **Pipeline Security**

21 **§ 40741. Railroad routing of security-sensitive materials**

22 (a) DEFINITIONS.—In this section:

23 (1) HIGH-CONSEQUENCE TARGET.—The term “high-consequence tar-
24 get” means a property, natural resource, location, area, or other target
25 designated by the Secretary that is a viable terrorist target of national
26 significance, which may include a facility or specific critical infrastruc-
27 ture, the attack of which by railroad could result in—

28 (A) catastrophic loss of life;

29 (B) significant damage to national security or defense capabili-
30 ties; or

31 (C) national economic harm.

32 (2) ROUTE.—The term “route” includes storage facilities and track-
33 age used by railroad cars in transportation in commerce.

34 (b) SECURITY-SENSITIVE MATERIALS COMMODITY DATA.—The Secretary
35 of Transportation shall, by regulation, require each railroad carrier trans-
36 porting security-sensitive materials in commerce to, no later than 90 days
37 after the end of each calendar year, compile security-sensitive materials
38 commodity data. The data must be collected by route, line segment, or se-
39 ries of line segments, as aggregated by the railroad carrier. Within the rail-
40 road-carrier-selected route, the commodity data must identify the geographic

1 location of the route and the total number of shipments by the United Na-
2 tions identification number for the security-sensitive materials.

3 (c) RAILROAD TRANSPORTATION ROUTE ANALYSIS FOR SECURITY-SEN-
4 SITIVE MATERIALS.—The Secretary of Transportation shall ensure that the
5 regulation issued under this section requires each railroad carrier trans-
6 porting security-sensitive materials in commerce to, for each calendar year,
7 provide a written analysis of the safety and security risks for the transpor-
8 tation routes identified in the security-sensitive materials commodity data
9 collected as required by subsection (b). The safety and security risks present
10 shall be analyzed for the route, railroad facilities, railroad storage facilities,
11 and high-consequence targets along or in proximity to the route.

12 (d) ALTERNATIVE ROUTE ANALYSIS FOR SECURITY-SENSITIVE MATE-
13 RIALS.—The Secretary of Transportation shall ensure that the regulation
14 issued under this section requires each railroad carrier transporting secu-
15 rity-sensitive materials in commerce to—

16 (1) for each calendar year—

17 (A) identify practicable alternative routes over which the rail-
18 road carrier has authority to operate as compared to the current
19 route for a shipment analyzed under subsection (c); and

20 (B) perform a safety and security risk assessment of the alter-
21 native route for comparison to the route analysis specified in sub-
22 section (c);

23 (2) ensure that the analysis under paragraph (1) includes—

24 (A) identification of safety and security risks for an alternative
25 route;

26 (B) comparison of those risks identified under subparagraph
27 (A) to the primary railroad transportation route, including the risk
28 of a catastrophic release from a shipment traveling along the alter-
29 nate route compared to the primary route;

30 (C) remediation or mitigation measures implemented on the pri-
31 mary or alternative route; and

32 (D) potential economic effects of using an alternative route; and

33 (3) consider when determining the practicable alternative routes
34 under paragraph (1)(A) the use of interchange agreements with other
35 railroad carriers.

36 (e) ALTERNATIVE ROUTE SELECTION FOR SECURITY-SENSITIVE MATE-
37 RIALS.—The Secretary of Transportation shall ensure that the regulation
38 issued under this section requires each railroad carrier transporting secu-
39 rity-sensitive materials in commerce to use the analysis required by sub-
40 sections (c) and (d) to select the safest and most secure route to be used
41 in transporting security-sensitive materials.

1 (f) REVIEW.—The Secretary of Transportation shall ensure that the regu-
2 lation issued under this section requires each railroad carrier transporting
3 security-sensitive materials in commerce to annually review and select the
4 practicable route posing the least overall safety and security risk under this
5 section. The railroad carrier must retain in writing all route review and se-
6 lection decision documentation and restrict the distribution, disclosure, and
7 availability of information contained in the route analysis to appropriate
8 persons. This documentation should include, but is not limited to, compara-
9 tive analyses, charts, graphics, or railroad system maps.

10 (g) RETROSPECTIVE ANALYSIS.—The Secretary of Transportation shall
11 ensure that the regulation issued under this section requires each railroad
12 carrier transporting security-sensitive materials in commerce to, not less
13 than once every 3 years, analyze the route selection determinations required
14 under this section. The analysis shall include a comprehensive, system-wide
15 review of all operational changes, infrastructure modifications, traffic ad-
16 justments, changes in the nature of high-consequence targets located along
17 or in proximity to the route, or other changes affecting the safety and secu-
18 rity of the movements of security-sensitive materials that were implemented
19 since the previous analysis was completed.

20 (h) CONSULTATION.—In carrying out subsection (c), railroad carriers
21 transporting security-sensitive materials in commerce shall seek relevant in-
22 formation from State, local, and tribal officials, as appropriate, regarding
23 security risks to high-consequence targets along or in proximity to a route
24 used by a railroad carrier to transport security-sensitive materials.

25 **§ 40742. Railroad security-sensitive material tracking**

26 (a) IN GENERAL.— In conjunction with the research and development
27 program established under section 40717 of this title and consistent with
28 the results of research relating to wireless and other tracking technologies,
29 the Secretary, in consultation with the Administrator of the Transportation
30 Security Administration, shall develop a program that will encourage the
31 equipping of railroad cars transporting security-sensitive materials, as de-
32 fined in section 40701 of this title, with technology that provides—

33 (1) car position location and tracking capabilities; and

34 (2) notification of railroad car depressurization, breach, unsafe tem-
35 perature, or release of hazardous materials, as appropriate.

36 (b) COORDINATION.—In developing the program required by subsection
37 (a), the Secretary shall—

38 (1) consult with the Secretary of Transportation to coordinate the
39 program with ongoing or planned efforts for railroad car tracking at
40 the Department of Transportation; and

1 (2) ensure that the program is consistent with recommendations and
2 findings of the Department of Homeland Security’s hazardous material
3 railroad tank car tracking pilot programs.

4 **§ 40743. Motor carrier security-sensitive material tracking**

5 (a) COMMUNICATIONS.—

6 (1) IN GENERAL.—Consistent with the findings of the Transpor-
7 tation Security Administration’s hazardous materials truck security
8 pilot program, the Secretary, through the Administrator of the Trans-
9 portation Security Administration and in consultation with the Sec-
10 retary of Transportation, shall develop a program to facilitate the
11 tracking of motor carrier shipments of security-sensitive materials and
12 to equip vehicles used in the shipments with technology that provides—

13 (A) frequent or continuous communications;

14 (B) vehicle position location and tracking capabilities; and

15 (C) a feature that allows a driver of the vehicles to broadcast
16 an emergency distress signal.

17 (2) CONSIDERATIONS.—In developing the program required by para-
18 graph (1), the Secretary shall—

19 (A) consult with the Secretary of Transportation to coordinate
20 the program with ongoing or planned efforts for motor carrier or
21 security-sensitive materials tracking at the Department of Trans-
22 portation;

23 (B) take into consideration the recommendations and findings
24 of the report on the hazardous material safety and security oper-
25 ational field test released by the Federal Motor Carrier Safety Ad-
26 ministration on November 11, 2004; and

27 (C) evaluate—

28 (i) new information related to the costs and benefits of de-
29 ploying, equipping, and utilizing tracking technology, includ-
30 ing portable tracking technology, for motor carriers trans-
31 porting security-sensitive materials not included in the haz-
32 ardous material safety and security operational field test re-
33 port released by the Federal Motor Carrier Safety Adminis-
34 tration on November 11, 2004;

35 (ii) the ability of tracking technology to resist tampering
36 and disabling;

37 (iii) the capability of tracking technology to collect, display,
38 and store information regarding the movement of shipments
39 of security-sensitive materials by commercial motor vehicles;

1 (iv) the appropriate range of contact intervals between the
2 tracking technology and a commercial motor vehicle trans-
3 porting security-sensitive materials;

4 (v) technology that allows the installation by a motor car-
5 rier of concealed electronic devices on commercial motor vehi-
6 cles that can be activated by law enforcement authorities to
7 disable the vehicle or alert emergency response resources to
8 locate and recover security-sensitive materials in the event of
9 loss or theft of the materials;

10 (vi) whether installation of the technology described in
11 clause (v) should be incorporated into the program under
12 paragraph (1);

13 (vii) the costs, benefits, and practicality of the technology
14 described in clause (v) in the context of the overall benefit to
15 national security, including commerce in transportation; and

16 (viii) other systems and information that the Secretary de-
17 termines appropriate.

18 (b) LIMITATION.—The Secretary may not mandate the installation or uti-
19 lization of a technology described under this section without additional con-
20 gressional authority provided after August 3, 2007.

21 **§ 40744. Use of transportation security card in hazmat li-**
22 **censing**

23 (a) BACKGROUND CHECK.—An individual who has a valid transportation
24 employee identification card issued by the Secretary under section 70105 of
25 title 46, is deemed to have met the background records check required
26 under section 5103a of title 49.

27 (b) STATE REVIEW.—Nothing in this subsection prevents or preempts a
28 State from conducting a criminal records check of an individual who has
29 applied for a license to operate a motor vehicle transporting in commerce
30 a hazardous material.

31 **§ 40745. Pipeline security inspections and enforcement**

32 (a) IN GENERAL.—Consistent with the Annex to the Memorandum of
33 Understanding executed on August 9, 2006, between the Department of
34 Transportation and the Department, the Secretary, in consultation with the
35 Secretary of Transportation, shall establish a program for reviewing pipeline
36 operator adoption of recommendations of the September 5, 2002, Depart-
37 ment of Transportation Research and Special Programs Administration's
38 Pipeline Security Information Circular, including the review of pipeline secu-
39 rity plans and critical facility inspections.

40 (b) REVIEW AND INSPECTION.—The Secretary and the Secretary of
41 Transportation shall develop and implement a plan for reviewing the pipe-

1 line security plans and for inspecting the critical facilities of the 100 most
 2 critical pipeline operators covered by the September 5, 2002, circular, where
 3 the facilities have not been inspected for security purposes since September
 4 5, 2002, by either the Department or the Department of Transportation.

5 (c) COMPLIANCE REVIEW METHODOLOGY.—In reviewing pipeline oper-
 6 ator compliance under subsections (a) and (b), risk assessment methodolo-
 7 gies shall be used to prioritize risks and to target inspection and enforce-
 8 ment actions to the highest risk pipeline assets.

9 (d) REGULATIONS.—The Secretary and the Secretary of Transportation
 10 shall develop and transmit to pipeline operators security recommendations
 11 for natural gas and hazardous liquid pipelines and pipeline facilities. If the
 12 Secretary determines that regulations are appropriate, the Secretary shall
 13 consult with the Secretary of Transportation on the extent of risk and ap-
 14 propriate mitigation measures, and the Secretary or the Secretary of Trans-
 15 portation, consistent with the Annex to the Memorandum of Understanding
 16 executed on August 9, 2006, shall promulgate regulations and carry out
 17 necessary inspection and enforcement actions. Regulations shall incorporate
 18 the guidance provided to pipeline operators by the September 5, 2002, De-
 19 partment of Transportation Research and Special Programs Administra-
 20 tion’s Pipeline Security Information Circular and contain additional require-
 21 ments as necessary based upon the results of the inspections performed
 22 under subsection (b). The regulations shall include the imposition of civil
 23 penalties for noncompliance.

24 **§ 40746. Pipeline security and incident recovery plan**

25 (a) IN GENERAL.—The Secretary, in consultation with the Secretary of
 26 Transportation and the Administrator of the Pipeline and Hazardous Mate-
 27 rials Safety Administration, and in accordance with the Annex to the Memo-
 28 randum of Understanding executed on August 9, 2006, the National Strat-
 29 egy for Transportation Security, and Homeland Security Presidential Direc-
 30 tive–7, shall develop a pipeline security and incident recovery protocols plan.
 31 The plan shall include—

32 (1) a security plan for the Government to provide increased security
 33 support to the most critical interstate and intrastate natural gas and
 34 hazardous liquid transmission pipeline infrastructure and operations as
 35 determined under section 40745 of this title when—

36 (A) the pipeline infrastructure or operations are under severe
 37 security threat levels of alert; or

38 (B) specific security threat information relating to the pipeline
 39 infrastructure or operations exists; and

40 (2) an incident recovery protocol plan, developed in conjunction with
 41 interstate and intrastate transmission and distribution pipeline opera-

1 tors and terminals and facilities operators connected to pipelines, to de-
 2 velop protocols to ensure the continued transportation of natural gas
 3 and hazardous liquids to essential markets and for essential public
 4 health or national defense uses in the event of an incident affecting the
 5 interstate and intrastate natural gas and hazardous liquid transmission
 6 and distribution pipeline system, including protocols for restoring es-
 7 sential services supporting pipelines and granting access to pipeline op-
 8 erators for pipeline infrastructure repair, replacement, or bypass fol-
 9 lowing an incident.

10 (b) EXISTING PRIVATE- AND PUBLIC-SECTOR EFFORTS.—The plan shall
 11 take into account actions taken or planned by both private and public enti-
 12 ties to address identified pipeline security issues and assess the effective in-
 13 tegration of the actions.

14 (c) CONSULTATION.—In developing the plan under subsection (a), the
 15 Secretary shall consult with the Secretary of Transportation, interstate and
 16 intrastate transmission and distribution pipeline operators, nonprofit em-
 17 ployee organizations representing pipeline employees, emergency responders,
 18 offerors, State pipeline safety agencies, public safety officials, and other rel-
 19 evant parties.

20 **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. Security screening program.

40930. Federal flight deck officer program.

40931. Deputation of State and local law enforcement officers.

40932. Airport security improvement projects.

40933. Repair station security.

40934. Deployment and use of detection equipment at airport screening checkpoints.

40935. Appeal and redress process for passengers wrongly delayed or prohibited from board-
 ing a flight.

40936. Expedited screening for severely injured or disabled members of the armed forces and
 severely injured or disabled veterans.

40937. Honor Flight program.

Subchapter III—Administration and Personnel

- 40951. Federal Security Managers.
- 40952. Foreign Security Liaison Officers.
- 40953. Employment standards and training.
- 40954. Employment investigations and restrictions.
- 40955. Prohibition on transferring duties and powers.
- 40956. Reports.
- 40957. Training to operate certain aircraft.
- 40958. Security service fee.
- 40959. Immunity for reporting suspicious activities.
- 40960. Performance goals and objectives.
- 40961. 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 40929 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 Transportation Security Administration, who shall have the power to order the dismissal of an individual performing screening.

(c) CHECKED BAGGAGE DEADLINE.—A system must be in operation to screen all checked baggage at all airports in the United States as soon as practicable.

(d) EXPLOSIVES DETECTION SYSTEMS.—

(1) IN GENERAL.—The Administrator shall take all necessary action to ensure that—

(A) explosives detection systems are deployed as soon as possible to ensure that all United States airports described in section 40913(c) of this title have sufficient explosives detection systems to screen all checked baggage and that as soon as the systems are

1 in place at an airport, all checked baggage at the airport is
2 screened by those systems;

3 (B) all systems deployed under subparagraph (A) are fully uti-
4 lized; and

5 (C) if explosives detection equipment at an airport is unavail-
6 able, all checked baggage is screened by an alternative means.

7 (2) PRECLEARANCE AIRPORTS.—

8 (A) DEFINITION OF AVIATION SECURITY PRECLEARANCE
9 AGREEMENT.—In this paragraph, the term “aviation security
10 preclearance agreement” means an agreement that delineates and
11 implements security standards and protocols that are determined
12 by the Administrator, in coordination with U.S. Customs and Bor-
13 der Protection, to be comparable to those of the United States and
14 therefore sufficiently effective to enable passengers to deplane into
15 sterile areas of airports in the United States.

16 (B) IN GENERAL.—For a flight or flight segment originating at
17 an airport outside the United States and traveling to the United
18 States with respect to which checked baggage has been screened
19 in accordance with an aviation security preclearance agreement be-
20 tween the United States and the country in which the airport is
21 located, the Administrator may, in coordination with U.S. Customs
22 and Border Protection, determine whether the baggage must be
23 re-screened in the United States by an explosives detection system
24 before the baggage continues on any additional flight or flight seg-
25 ment.

26 (C) RESCREENING REQUIREMENT.—If the Administrator deter-
27 mines that the government of a foreign country has not main-
28 tained security standards and protocols comparable to those of the
29 United States at airports at which preclearance operations have
30 been established in accordance with this paragraph, the Adminis-
31 trator shall ensure that Transportation Security Administration
32 personnel rescreen passengers arriving from those airports and
33 their property in the United States before the passengers are per-
34 mitted into sterile area of airports in the United States.

35 (D) REPORT.—The Administrator shall submit to the Com-
36 mittee on Homeland Security of the House of Representatives, the
37 Committee on Commerce, Science, and Transportation of the Sen-
38 ate, and the Committee on Homeland Security and Governmental
39 Affairs of the Senate an annual report on the re-screening of bag-
40 gage under this paragraph. Each report shall include the following
41 for the year covered by the report:

1 (i) A list of airports outside the United States from which
2 a flight or flight segment traveled to the United States for
3 which the Administrator determined, in accordance with the
4 authority under subparagraph (B), that checked baggage was
5 not required to be re-screened in the United States by an ex-
6 plosives detection system before the baggage continued on an
7 additional flight or flight segment.

8 (ii) The amount of Federal savings generated from the ex-
9 ercise of the authority.

10 (e) CARGO DEADLINE.—A system must be in operation to screen, inspect,
11 or otherwise ensure the security of all cargo that is to be transported in
12 all-cargo aircraft in air transportation and intrastate air transportation as
13 soon as practicable.

14 (f) AIR CARGO ON PASSENGER AIRCRAFT.—

15 (1) DEFINITION OF SCREENING.—In this subsection, the term
16 “screening” means a physical examination or nonintrusive methods of
17 assessing whether cargo poses a threat to transportation security, in-
18 cluding x-ray systems, explosives detection systems, explosives trace de-
19 tection, explosives detection canine teams certified by the Transpor-
20 tation Security Administration, or a physical search together with
21 manifest verification.

22 (2) IN GENERAL.—The Secretary shall establish a system to screen
23 100 percent of cargo transported on passenger aircraft operated by an
24 air carrier or foreign air carrier in air transportation or intrastate air
25 transportation to ensure the security of all passenger aircraft carrying
26 cargo.

27 (3) MINIMUM STANDARDS.—The system referred to in paragraph (2)
28 shall require, at a minimum, that equipment, technology, procedures,
29 personnel, or other methods approved by the Administrator, are used
30 to screen cargo carried on passenger aircraft described in paragraph
31 (2) to provide a level of security commensurate with the level of secu-
32 rity for the screening of passenger checked baggage.

33 (4) ADDITIONAL CARGO SCREENING METHODS.—

34 (A) IN GENERAL.—The Administrator may approve additional
35 methods to ensure that the cargo does not pose a threat to trans-
36 portation security and to assist in meeting the requirements of
37 this subsection.

38 (B) MINIMUM REQUIREMENTS.—The additional cargo screening
39 methods shall not include solely performing a review of informa-
40 tion about the contents of cargo or verifying the identity of a ship-
41 per of the cargo that is not performed in conjunction with other

1 security methods authorized under this subsection, including
2 whether a known shipper is registered in the known shipper data-
3 base.

4 (C) CERTIFICATION PROGRAM.—The additional cargo screening
5 methods may include a program to certify the security methods
6 used by shippers under paragraphs (2) and (3) and alternative
7 screening methods pursuant to exemptions referred to in sub-
8 section (b) of section 1602 of the Implementing Recommendations
9 of the 9/11 Commission Act of 2007 (Public Law 110–53, 121
10 Stat. 479).

11 (5) REGULATIONS.—The Secretary shall, by regulation, implement
12 this subsection in accordance with the provisions of chapter 5 of title
13 5.

14 (g) DEPLOYMENT OF ARMED LAW ENFORCEMENT PERSONNEL.—

15 (1) IN GENERAL.—The Administrator shall order the deployment of
16 law enforcement personnel authorized to carry firearms at each airport
17 security screening location to ensure passenger safety and national se-
18 curity.

19 (2) MINIMUM REQUIREMENTS.—Except at airports required to enter
20 into agreements under subsection (c), the Administrator shall order the
21 deployment of at least one law enforcement officer at each airport secu-
22 rity screening location. At the 100 largest airports in the United
23 States, in terms of annual passenger enplanements for the most recent
24 calendar year for which data are available, the Secretary shall order
25 the deployment of additional law enforcement personnel at airport secu-
26 rity screening locations if the Administrator determines that the addi-
27 tional deployment is necessary to ensure passenger safety and national
28 security.

29 (h) EXEMPTIONS AND ADVISING CONGRESS ON REGULATIONS.—The Ad-
30 ministrator—

31 (1) may exempt from this section air transportation operations, ex-
32 cept scheduled passenger operations of an air carrier providing air
33 transportation under a certificate issued under section 41102 of title
34 49 or a permit issued under section 41302 of title 49; and

35 (2) shall advise Congress of a regulation to be prescribed under this
36 section at least 30 days before the effective date of the regulation, un-
37 less the Administrator decides an emergency exists requiring the regu-
38 lation to become effective in fewer than 30 days and notifies Congress
39 of that decision.

40 (i) BLAST-RESISTANT CARGO CONTAINERS.—

41 (1) IN GENERAL.—The Administrator shall—

1 (A) evaluate the results of the blast-resistant cargo container
2 pilot program that was initiated before August 3, 2007; and

3 (B) prepare and distribute through the Aviation Security Advi-
4 sory Committee to the appropriate Committees of Congress and
5 air carriers a report on that evaluation which may contain non-
6 classified and classified sections.

7 (2) ACQUISITION, MAINTENANCE, AND REPLACEMENT.—On comple-
8 tion and consistent with the results of the evaluation that paragraph
9 (1)(A) requires, the Administrator shall—

10 (A) develop and implement a program, as the Administrator de-
11 termines appropriate, to acquire, maintain, and replace blast-re-
12 sistant cargo containers;

13 (B) pay for the program; and

14 (C) make available blast-resistant cargo containers to air car-
15 riers under paragraph (3).

16 (3) DISTRIBUTION TO AIR CARRIERS.—The Administrator shall make
17 available blast-resistant cargo containers to air carriers for use on a
18 risk managed basis as determined by the Secretary.

19 (j) GENERAL AVIATION AIRPORT SECURITY PROGRAM.—

20 (1) IN GENERAL.—The Administrator shall—

21 (A) develop a standardized threat and vulnerability assessment
22 program for general aviation airports (as defined in section
23 47134(m) of title 49); and

24 (B) implement a program to perform the assessments on a risk-
25 managed basis at general aviation airports.

26 (2) GRANT PROGRAM.—The Administrator shall complete a study of
27 the feasibility of a program, based on a risk-managed approach, to pro-
28 vide grants to operators of general aviation airports (as defined in sec-
29 tion 47134(m) of title 49) for projects to upgrade security at the air-
30 ports. If the Secretary determines that a program is feasible, the Sec-
31 retary shall establish a program.

32 (3) REQUIRED SUBMISSIONS BY GENERAL AVIATION AIRCRAFT.—The
33 Administrator shall develop a risk-based system under which—

34 (A) general aviation aircraft, as identified by the Administrator,
35 in coordination with the Administrator of the Federal Aviation Ad-
36 ministration, are required to submit passenger information and
37 advance notification requirements for U. S. Customs and Border
38 Protection before entering United States airspace; and

39 (B) the information is checked against appropriate databases.

1 (4) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to
2 be appropriated to the Administrator such sums as may be necessary
3 to carry out paragraphs (2) and (3).

4 (k) LIMITATIONS ON USE OF ADVANCED IMAGING TECHNOLOGY FOR
5 SCREENING PASSENGERS.—

6 (1) DEFINITIONS.—In this subsection:

7 (A) ADVANCED IMAGING TECHNOLOGY.—The term “advanced
8 imaging technology”—

9 (i) means a device used in the screening of passengers that
10 creates a visual image of an individual showing the surface
11 of the skin and revealing other objects on the body; and

12 (ii) may include devices using backscatter x-rays or milli-
13 meter waves and devices referred to as “whole-body imaging
14 technology” or “body scanning machines”.

15 (B) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term
16 “appropriate congressional committees” means—

17 (i) the Committee on Commerce, Science, and Transpor-
18 tation and the Committee on Homeland Security and Govern-
19 mental Affairs of the Senate; and

20 (ii) the Committee on Homeland Security of the House of
21 Representatives.

22 (C) AUTOMATIC TARGET RECOGNITION SOFTWARE.—The term
23 “automatic target recognition software” means software installed
24 on an advanced imaging technology that produces a generic image
25 of the individual being screened that is the same as the images
26 produced for all other screened individuals.

27 (2) USE OF ADVANCED IMAGING TECHNOLOGY.—The Administrator
28 shall ensure that an advanced imaging technology used for the screen-
29 ing of passengers under this section—

30 (A) is equipped with and employs automatic target recognition
31 software; and

32 (B) complies with other requirements the Administrator deter-
33 mines necessary to address privacy considerations.

34 (3) EXTENSION.—

35 (A) IN GENERAL.—The Administrator may extend the deadline
36 specified in paragraph (2), if the Administrator determines that—

37 (i) an advanced imaging technology equipped with auto-
38 matic target recognition software is not substantially as effec-
39 tive at screening passengers as an advanced imaging technol-
40 ogy without the software; or

41 (ii) additional testing of the software is necessary.

1 (B) DURATION OF EXTENSIONS.—The Administrator may issue
 2 one or more extensions under subparagraph (A). The duration of
 3 each extension may not exceed one year.

4 (4) REPORTS.—

5 (A) IN GENERAL.—Not later than 60 days after the date on
 6 which the Administrator issues any extension under paragraph
 7 (3), the Administrator shall submit to the appropriate congres-
 8 sional committees a report on the implementation of this sub-
 9 section.

10 (B) ELEMENTS.—A report submitted under subparagraph (A)
 11 shall include the following:

12 (i) A description of all matters the Administrator considers
 13 relevant to the implementation of the requirements of this
 14 subsection.

15 (ii) The status of compliance by the Transportation Secu-
 16 rity Administration with the requirements.

17 (iii) If the Transportation Security Administration is not in
 18 full compliance with the requirements—

19 (I) the reasons for the noncompliance; and

20 (II) a timeline depicting when the Administrator ex-
 21 pects the Transportation Security Administration to
 22 achieve full compliance.

23 (C) SECURITY CLASSIFICATION.—To the greatest extent prac-
 24 ticable, a report prepared under subparagraph (A) shall be sub-
 25 mitted in an unclassified format. If necessary, the report may in-
 26 clude a classified annex.

27 **§ 40912. Refusal to transport passengers and property**

28 (a) MANDATORY REFUSAL.—The Administrator shall prescribe regula-
 29 tions requiring an air carrier, intrastate air carrier, or foreign air carrier
 30 to refuse to transport—

31 (1) a passenger who does not consent to a search under section
 32 40911(a) of this title establishing whether the passenger is carrying
 33 unlawfully a dangerous weapon, explosive, or other destructive sub-
 34 stance; or

35 (2) property of a passenger who does not consent to a search of the
 36 property establishing whether the property unlawfully contains a dan-
 37 gerous weapon, explosive, or other destructive substance.

38 (b) PERMISSIVE REFUSAL.—Subject to regulations of the Administrator,
 39 an air carrier, intrastate air carrier, or foreign air carrier may refuse to
 40 transport a passenger or property the carrier decides is, or might be, inim-
 41 ical to safety.

1 (c) AGREEING TO CONSENT TO SEARCH.—An agreement to carry pas-
2 sengers or property in air transportation or intrastate air transportation by
3 an air carrier, intrastate air carrier, or foreign air carrier is deemed to in-
4 clude an agreement that the passenger or property will not be carried if con-
5 sent to search the passenger or property for a purpose referred to in this
6 section is not given.

7 **§ 40913. Air transportation security**

8 (a) DEFINITION OF LAW ENFORCEMENT PERSONNEL.—In this section,
9 “law enforcement personnel” means individuals—

10 (1) authorized to carry and use firearms;

11 (2) vested with the degree of the police power of arrest the Secretary
12 considers necessary to carry out this section; and

13 (3) identifiable by appropriate indicia of authority.

14 (b) PROTECTION AGAINST VIOLENCE AND PIRACY.—The Administrator
15 shall prescribe regulations to protect passengers and property on an aircraft
16 operating in air transportation or intrastate air transportation against an
17 act of criminal violence or aircraft piracy. When prescribing a regulation
18 under this subsection, the Administrator shall—

19 (1) consult with the Secretary of Transportation, the Attorney Gen-
20 eral, the heads of other departments, agencies, and instrumentalities of
21 the United States Government, and State and local authorities;

22 (2) consider whether a proposed regulation is consistent with—

23 (A) protecting passengers; and

24 (B) the public interest in promoting air transportation and
25 intrastate air transportation;

26 (3) to the maximum extent practicable, require a uniform procedure
27 for searching and detaining passengers and property to ensure—

28 (A) their safety; and

29 (B) courteous and efficient treatment by an air carrier, an
30 agent or employee of an air carrier, and Government, State, and
31 local law enforcement personnel carrying out this section; and

32 (4) consider the extent to which a proposed regulation will carry out
33 this section.

34 (c) SECURITY PROGRAMS.—

35 (1) IN GENERAL.—The Administrator shall prescribe regulations
36 under subsection (b) that require each operator of an airport regularly
37 serving an air carrier holding a certificate issued by the Secretary of
38 Transportation to establish an air transportation security program that
39 provides a law enforcement presence and capability at each of those
40 airports that is adequate to ensure the safety of passengers. The regu-
41 lations shall authorize the operator to use the services of qualified

1 State, local, and private law enforcement personnel. When the Adminis-
2 trator decides, after being notified by an operator in the form the Ad-
3 ministrator prescribes, that not enough qualified State, local, and pri-
4 vate law enforcement personnel are available to carry out subsection
5 (b), the Administrator may authorize the operator to use, on a reim-
6 bursable basis, personnel employed by the Administrator, or by another
7 department, agency, or instrumentality of the Government with the
8 consent of the head of the department, agency, or instrumentality, to
9 supplement State, local, and private law enforcement personnel. When
10 deciding whether additional personnel are needed, the Administrator
11 shall consider the number of passengers boarded at the airport, the ex-
12 tent of anticipated risk of criminal violence or aircraft piracy at the air-
13 port or to the air carrier aircraft operations at the airport, and the
14 availability of qualified State or local law enforcement personnel at the
15 airport.

16 (2) INCLUSION OF AIRPORT TENANT SECURITY PROGRAM.—

17 (A) IN GENERAL.—The Administrator may approve a security
18 program of an airport operator, or an amendment to an existing
19 program, that incorporates a security program of an airport ten-
20 ant (except an air carrier separately complying with part 108 or
21 129 of title 14, Code of Federal Regulations) having access to a
22 secured area of the airport, if the program or amendment incor-
23 porates—

24 (i) the measures the tenant will use, within the tenant's
25 leased areas or areas designated for the tenant's exclusive use
26 under an agreement with the airport operator, to carry out
27 the security requirements imposed by the Administrator on
28 the airport operator under the access control system require-
29 ments of section 107.14 of title 14, Code of Federal Regula-
30 tions, or under other requirements of part 107 of title 14;
31 and

32 (ii) the methods the airport operator will use to monitor
33 and audit the tenant's compliance with the security require-
34 ments and provides that the tenant will be required to pay
35 monetary penalties to the airport operator if the tenant fails
36 to carry out a security requirement under a contractual provi-
37 sion or requirement imposed by the airport operator.

38 (B) OPERATOR NOT IN VIOLATION.—If the Administrator ap-
39 proves a program or amendment described in subparagraph (A) of
40 this paragraph, the airport operator may not be found to be in vio-
41 lation of a requirement of this subsection or subsection (b) when

1 the airport operator demonstrates that the tenant or an employee,
2 permittee, or invitee of the tenant is responsible for the violation
3 and that the airport operator has complied with all measures in
4 its security program for securing compliance with its security pro-
5 gram by the tenant.

6 (C) MAXIMUM USE OF CHEMICAL AND BIOLOGICAL WEAPON DE-
7TECTION EQUIPMENT.—The Administrator may require airports to
8 maximize the use of technology and equipment that is designed to
9 detect or neutralize potential chemical or biological weapons.

10 (3) PILOT PROGRAMS.—The Administrator shall establish pilot pro-
11 grams in no fewer than 20 airports to test and evaluate new and
12 emerging technology for providing access control and other security
13 protections for closed or secure areas of the airports. The technology
14 may include biometric or other technology that ensures only authorized
15 access to secure areas.

16 (d) AUTHORIZING INDIVIDUALS TO CARRY FIREARMS AND MAKE AR-
17RESTS.—With the approval of the Attorney General and the Secretary of
18 State, the Secretary may authorize an individual who carries out air trans-
19 portation security duties—

20 (1) to carry firearms; and

21 (2) to make arrests without warrant for an offense against the
22 United States committed in the presence of the individual or for a fel-
23 ony under the laws of the United States, if the individual reasonably
24 believes the individual to be arrested has committed or is committing
25 a felony.

26 (e) EXCLUSIVE RESPONSIBILITY OVER PASSENGER SAFETY.—The Ad-
27 ministrator has the exclusive responsibility to direct law enforcement activity
28 related to the safety of passengers on an aircraft involved in an offense
29 under section 46502 of title 49 from the moment all external doors of the
30 aircraft are closed following boarding until those doors are opened to allow
31 passengers to leave the aircraft. When requested by the Administrator,
32 other departments, agencies, and instrumentalities of the Government shall
33 provide assistance necessary to carry out this subsection.

34 (f) GOVERNMENT AND INDUSTRY CONSORTIA.—The Administrator may
35 establish at airports consortia of government and aviation industry rep-
36 resentatives to provide advice on matters related to aviation security and
37 safety. The consortia shall not be considered Federal advisory committees
38 for purposes of the Federal Advisory Committee Act (5 U.S.C. App.).

39 (g) IMPROVEMENT OF SECURED-AREA ACCESS CONTROL.—

40 (1) EMPLOYEE SANCTIONS.—

1 (A) PUBLICATION.—The Administrator shall publish in the
2 Federal Register a list of sanctions for use as guidelines in the
3 discipline of employees for infractions of airport access control re-
4 quirements.

5 (B) DISCIPLINARY APPROACH.—The guidelines shall incorporate
6 a progressive disciplinary approach that relates proposed sanctions
7 to the severity or recurring nature of the infraction and shall in-
8 clude measures such as remedial training, suspension from secu-
9 rity-related duties, suspension from all duties without pay, and
10 termination of employment.

11 (C) USE.—Each airport operator, air carrier, and security
12 screening company shall include the list of sanctions published by
13 the Administrator in its security program. The security program
14 shall include a process for taking prompt disciplinary action
15 against an employee who commits an infraction of airport access
16 control requirements.

17 (2) ACTIONS TO IMPROVE ACCESS CONTROL.—The Administrator
18 shall—

19 (A) work with airport operators and air carriers to implement
20 and strengthen existing controls to eliminate airport access control
21 weaknesses;

22 (B) require airport operators and air carriers to develop and im-
23 plement comprehensive and recurring training programs that
24 teach employees their roles in airport security, the importance of
25 their participation, how their performance will be evaluated, and
26 what action will be taken if they fail to perform;

27 (C) require airport operators and air carriers to develop and im-
28 plement programs that foster and reward compliance with airport
29 access control requirements and discourage and penalize non-
30 compliance in accordance with guidelines issued by the Adminis-
31 trator to measure employee compliance;

32 (D) on an ongoing basis, assess and test for compliance with
33 access control requirements, report annually findings of the assess-
34 ments, and assess the effectiveness of penalties in ensuring compli-
35 ance with security procedures and take other appropriate enforce-
36 ment actions when noncompliance is found;

37 (E) improve and better administer the Administrator's security
38 database to ensure its efficiency, reliability, and usefulness for
39 identification of systemic problems and allocation of resources;

40 (F) improve the execution of the Administrator's quality control
41 program; and

1 (G) work with airport operators to strengthen access control
2 points in secured areas (including air traffic control operations
3 areas, maintenance areas, crew lounges, baggage handling areas,
4 concessions, and catering delivery areas) to ensure the security of
5 passengers and aircraft and consider the deployment of biometric
6 or similar technologies that identify individuals based on unique
7 personal characteristics.

8 (h) IMPROVED AIRPORT PERIMETER ACCESS SECURITY.—

9 (1) DEFINITIONS.—In this subsection:

10 (A) BIOMETRIC IDENTIFIER.—The term “biometric identifier”
11 means a technology that enables the automated identification, or
12 verification of the identity, of an individual based on biometric in-
13 formation.

14 (B) BIOMETRIC IDENTIFIER INFORMATION.—The term “biomet-
15 ric identifier information” means the distinct physical or behav-
16 ioral characteristics of an individual that are used for unique iden-
17 tification, or verification of the identity, of an individual.

18 (C) FAILURE TO ENROLL.—The term “failure to enroll” means
19 the inability of an individual to enroll in a biometric identifier sys-
20 tem due to an insufficiently distinctive biometric sample, the lack
21 of a body part necessary to provide the biometric sample, a system
22 design that makes it difficult to provide consistent biometric iden-
23 tifier information, or other factors.

24 (D) FALSE MATCH.—The term “false match” means the incor-
25 rect matching of one individual’s biometric identifier information
26 to another individual’s biometric identifier information by a bio-
27 metric identifier system.

28 (E) FALSE NON-MATCH.—The term “false non-match” means
29 the rejection of a valid identity by a biometric identifier system.

30 (F) SECURE AREA OF AN AIRPORT.—The term “secure area of
31 an airport” means the sterile area and the Security Identification
32 Display Area of an airport (as the terms are defined in section
33 1540.5 of title 49, Code of Federal Regulations, or a successor
34 regulation to that section).

35 (2) IN GENERAL.—The Administrator, in consultation with the air-
36 port operator and law enforcement authorities, may order the deploy-
37 ment of necessary personnel at a secure area of the airport to counter
38 the risk of criminal violence, the risk of aircraft piracy at the airport,
39 the risk to air carrier aircraft operations at the airport, or to meet na-
40 tional security concerns.

1 (3) CONSIDERATION OF SECURITY OF AIRCRAFT AND GROUND AC-
2 CESS TO SECURE AREAS.—In determining where to deploy the per-
3 sonnel, the Administrator shall consider the physical security needs of
4 air traffic control facilities, parked aircraft, aircraft servicing equip-
5 ment, aircraft supplies (including fuel), automobile parking facilities
6 within airport perimeters or adjacent to secured facilities, and access
7 and transition areas at airports served by other means of ground or
8 water transportation.

9 (4) DEPLOYMENT OF FEDERAL LAW ENFORCEMENT PERSONNEL.—
10 The Administrator may enter into a memorandum of understanding or
11 other agreement with the Attorney General or the head of another ap-
12 propriate Federal law enforcement agency to deploy Federal law en-
13 forcement personnel at an airport in order to meet aviation safety and
14 security concerns.

15 (5) AIRPORT PERIMETER SCREENING.—The Administrator shall—

16 (A) require screening or inspection of all individuals, goods,
17 property, vehicles, and other equipment before entry into a secured
18 area of an airport in the United States described in subsection (c);

19 (B) prescribe specific requirements for the screening and inspec-
20 tion that will ensure at least the same level of protection as will
21 result from screening of passengers and their baggage;

22 (C) establish procedures to ensure the safety and integrity of—

23 (i) all persons providing services with respect to aircraft
24 providing passenger air transportation or intrastate air trans-
25 portation and facilities of those persons at an airport in the
26 United States described in subsection (c);

27 (ii) all supplies, including catering and passenger ameni-
28 ties, placed aboard the aircraft, including the sealing of sup-
29 plies to ensure easy visual detection of tampering; and

30 (iii) all persons providing the supplies and facilities of those
31 persons;

32 (D) require vendors having direct access to the airfield and air-
33 craft to develop security programs; and

34 (E) issue guidance for the use of biometric or other technology
35 that positively verifies the identity of each employee and law en-
36 forcement officer who enters a secure area of an airport.

37 (6) USE OF BIOMETRIC TECHNOLOGY IN AIRPORT ACCESS CONTROL
38 SYSTEMS.—In issuing guidance under paragraph (5)(E), the Adminis-
39 trator in consultation with representatives of the aviation industry, the
40 biometric identifier industry, and the National Institute of Standards
41 and Technology, shall establish, at a minimum—

1 (A) comprehensive technical and operational system require-
2 ments and performance standards for the use of biometric identi-
3 fier technology in airport access control systems (including airport
4 perimeter access control systems) to ensure that the biometric
5 identifier systems are effective, reliable, and secure;

6 (B) a list of products and vendors that meet the requirements
7 and standards set forth in subparagraph (A);

8 (C) procedures for implementing biometric identifier systems—

9 (i) to ensure that individuals do not use an assumed iden-
10 tity to enroll in a biometric identifier system; and

11 (ii) to resolve failures to enroll, false matches, and false
12 nonmatches; and

13 (D) best practices for incorporating biometric identifier tech-
14 nology into airport access control systems in the most effective
15 manner, including a process to best utilize existing airport access
16 control systems, facilities, and equipment, and existing data net-
17 works connecting airports.

18 (7) USE OF BIOMETRIC TECHNOLOGY FOR ARMED LAW ENFORCE-
19 MENT TRAVEL.—

20 (A) IN GENERAL.—The Secretary, in consultation with the At-
21 torney General, shall—

22 (i) implement this section by publication in the Federal
23 Register; and

24 (ii) establish a national registered armed law enforcement
25 program, that shall be federally managed, for law enforce-
26 ment officers needing to be armed when traveling by commer-
27 cial aircraft.

28 (B) PROGRAM REQUIREMENTS.—The program shall—

29 (i) establish a credential or a system that incorporates bio-
30 metric technology and other applicable technologies;

31 (ii) establish a system for law enforcement officers who
32 need to be armed when traveling by commercial aircraft on
33 a regular basis and for those who need to be armed during
34 temporary travel assignments;

35 (iii) comply with other uniform credentialing initiatives, in-
36 cluding the Homeland Security Presidential Directive-12;

37 (iv) apply to all Federal, State, local, tribal, and territorial
38 government law enforcement agencies; and

39 (v) establish a process by which the travel credential or sys-
40 tem may be used to verify the identity, using biometric tech-
41 nology, of a Federal, State, local, tribal, or territorial law en-

1 enforcement officer seeking to carry a weapon on board a com-
2 mercial aircraft, without unnecessarily disclosing to the public
3 that the individual is a law enforcement officer.

4 (C) PROCEDURES.—In establishing the program, the Secretary
5 shall develop procedures—

6 (i) to ensure that a law enforcement officer of a Federal,
7 State, local, tribal, or territorial government flying armed has
8 a specific reason for flying armed and the reason is within
9 the scope of the duties of the officer;

10 (ii) to preserve the anonymity of the armed law enforce-
11 ment officer;

12 (iii) to resolve failures to enroll, false matches, and false
13 nonmatches relating to the use of the law enforcement travel
14 credential or system;

15 (iv) to determine the method of issuance of the biometric
16 credential to law enforcement officers needing to be armed
17 when traveling by commercial aircraft;

18 (v) to invalidate a law enforcement travel credential or sys-
19 tem that is lost, stolen, or no longer authorized for use;

20 (vi) to coordinate the program with the Federal Air Mar-
21 shal Service, including the force multiplier program of the
22 Service; and

23 (vii) to implement a phased approach to launching the pro-
24 gram, addressing the immediate needs of the relevant Federal
25 agent population before expanding the program to other law
26 enforcement populations.

27 (i) AUTHORITY TO ARM FLIGHT DECK CREW WITH LESS-THAN-LETHAL
28 WEAPONS.—

29 (1) IN GENERAL.—If the Administrator, after receiving the rec-
30 ommendations of the National Institute of Justice, determines, with the
31 approval of the Attorney General and the Secretary of State, that it
32 is appropriate and necessary and would effectively serve the public in-
33 terest in avoiding air piracy, the Administrator may authorize members
34 of the flight deck crew on an aircraft providing air transportation or
35 intrastate air transportation to carry a less-than-lethal weapon while
36 the aircraft is engaged in providing the transportation.

37 (2) USAGE.—If the Administrator grants authority under paragraph
38 (1) for flight deck crew members to carry a less-than-lethal weapon
39 while engaged in providing air transportation or intrastate air trans-
40 portation, the Administrator shall—

1 (A) prescribe rules requiring that the crew member be trained
2 in the proper use of the weapon; and

3 (B) prescribe guidelines setting forth the circumstances under
4 which weapons may be used.

5 (3) REQUEST OF AIR CARRIERS TO USE LESS-THAN-LETHAL WEAP-
6 ONS.—If the Administrator receives a request from an air carrier for
7 authorization to allow pilots of the air carrier to carry less-than-lethal
8 weapons, the Administrator shall respond to that request within 90
9 days.

10 (j) SHORT-TERM ASSESSMENT AND DEPLOYMENT OF EMERGING SEC-
11 URITY TECHNOLOGIES AND PROCEDURES.—

12 (1) DEFINITION OF SECURE AREA OF AN AIRPORT.—In this sub-
13 section, the term “secure area of an airport” means the sterile area
14 and the Security Identification Display Area of an airport (as the
15 terms are defined in section 1540.5 of title 49, Code of Federal Regu-
16 lations, or a successor regulation to that section).

17 (2) IN GENERAL.—The Administrator shall recommend to airport
18 operators commercially available measures or procedures to prevent ac-
19 cess to secure airport areas by unauthorized persons. As part of a 6-
20 month assessment, the Administrator shall—

21 (A) review the effectiveness of biometrics systems currently in
22 use at several United States airports, including San Francisco
23 International;

24 (B) review the effectiveness of increased surveillance at access
25 points;

26 (C) review the effectiveness of card- or keypad-based access sys-
27 tems;

28 (D) review the effectiveness of airport emergency exit systems
29 and determine whether those that lead to secure areas of the air-
30 port should be monitored or how breaches can be swiftly re-
31 sponded to; and

32 (E) specifically target the elimination of the “piggy-backing”
33 phenomenon, where another person follows an authorized person
34 through the access point.

35 (3) DEPLOYMENT STRATEGY FOR AVAILABLE TECHNOLOGY; REVIEW
36 OF REDUCTIONS IN UNAUTHORIZED ACCESS.—The 6-month assessment
37 shall include a 12-month deployment strategy for currently available
38 technology at all category X airports, as defined in the Federal Avia-
39 tion Administration approved air carrier security programs required
40 under part 108 of title 14, Code of Federal Regulations. After the as-

1 assessment, the Administrator shall conduct a review of reductions in un-
2 authorized access at these airports.

3 (4) COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM.—

4 (A) IN GENERAL.—The Administrator shall ensure that the
5 Computer-Assisted Passenger Prescreening System, or a successor
6 system—

7 (i) is used to evaluate all passengers before they board an
8 aircraft; and

9 (ii) includes procedures to ensure that individuals selected
10 by the system and their carry-on and checked baggage are
11 adequately screened.

12 (B) MODIFICATIONS.—The Administrator may modify a re-
13 quirement under the Computer-Assisted Passenger Prescreening
14 System for flights that originate and terminate in the same State,
15 if the Administrator determines that—

16 (i) the State has extraordinary air transportation needs or
17 concerns due to its isolation and dependence on air transpor-
18 tation; and

19 (ii) the routine characteristics of passengers, given the na-
20 ture of the market, regularly triggers primary selectee status.

21 (C) ADVANCED AIRLINE PASSENGER PRESCREENING.—

22 (i) TESTING.—The Administrator, or the designee of the
23 Administrator, shall commence testing of an advanced pas-
24 senger prescreening system that will allow the Department to
25 assume the performance of comparing passenger information,
26 as defined by the Administrator, to the automatic selectee
27 and no fly lists, utilizing all appropriate records in the con-
28 solidated and integrated terrorist watchlist maintained by the
29 Federal Government.

30 (ii) ASSUMPTION OF PERFORMANCE.—After completion of
31 testing under clause (i), the Administrator, or the designee of
32 the Administrator, shall begin to assume the performance of
33 the passenger prescreening function of comparing passenger
34 information to the automatic selectee and no fly lists and uti-
35 lize all appropriate records in the consolidated and integrated
36 terrorist watchlist maintained by the Federal Government in
37 performing that function.

38 (iii) DUTIES IN ASSUMING PERFORMANCE.—In assuming
39 performance of the function under clause (ii), the Adminis-
40 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.—The Ad-
36 ministrator, in coordination with the Terrorist Screening Cen-
37 ter, shall include on the No Fly List an individual who was
38 a detainee held at the Naval Station, Guantanamo Bay,
39 Cuba, unless the President certifies in writing to Congress
40 that the detainee poses no threat to the United States, its
41 citizens, or its allies. For purposes of this clause, the term

1 “detainee” means an individual in the custody or under the
2 physical control of the United States as a result of armed
3 conflict.

4 (D) SCREENING OF EMPLOYEES AGAINST WATCHLIST.—The
5 Administrator in coordination with the Secretary of Transpor-
6 tation and the Administrator of the Federal Aviation Administra-
7 tion, shall ensure that individuals are screened against all appro-
8 priate records in the consolidated and integrated terrorist
9 watchlist maintained by the Federal Government before—

10 (i) being certificated by the Federal Aviation Administra-
11 tion;

12 (ii) being granted unescorted access to the secure area of
13 an airport; or

14 (iii) being granted unescorted access to the air operations
15 area (as defined in section 1540.5 of title 49, Code of Federal
16 Regulations, or a successor regulation to that section) of an
17 airport.

18 (E) AIRCRAFT CHARTER CUSTOMER AND LESSEE
19 PRESCREENING.—

20 (i) ESTABLISHMENT.—The Administrator shall establish a
21 process by which operators of aircraft to be used in charter
22 air transportation with a maximum takeoff weight greater
23 than 12,500 pounds and lessors of aircraft with a maximum
24 takeoff weight greater than 12,500 pounds may—

25 (I) request the Department to use the advanced pas-
26 senger prescreening system to compare information
27 about an individual seeking to charter an aircraft with
28 a maximum takeoff weight greater than 12,500 pounds,
29 a passenger proposed to be transported aboard the air-
30 craft, and an individual seeking to lease an aircraft with
31 a maximum takeoff weight greater than 12,500 pounds
32 to the automatic selectee and no fly lists, utilizing all ap-
33 propriate records in the consolidated and integrated ter-
34 rorist watchlist maintained by the Federal Government;
35 and

36 (II) refuse to charter or lease an aircraft with a max-
37 imum takeoff weight greater than 12,500 pounds to or
38 transport aboard the aircraft persons identified on the
39 watch list.

40 (ii) APPLICABILITY.—The requirements of subparagraph
41 (C)(iii) apply to this subparagraph.

1 (iii) DESIGN AND REVIEW OF GUIDELINES, POLICIES, AND
2 OPERATING PROCEDURES.—The Administrator, in consulta-
3 tion with the Terrorist Screening Center, shall design and re-
4 view, as necessary, guidelines, policies, and operating proce-
5 dures for the collection, removal, and updating of data main-
6 tained, or to be maintained, in the no fly and automatic se-
7 lectee lists.

8 (F) APPLICABILITY.—Section 607 of the Vision 100—Century
9 of Aviation Reauthorization Act (Public Law 108–176, 117 Stat.
10 2568) does not apply to the advanced passenger prescreening sys-
11 tem established under subparagraph (C).

12 (G) APPEAL PROCEDURES.—

13 (i) ESTABLISHMENT.—The Administrator shall establish a
14 timely and fair process for individuals identified as a threat
15 under one or more of subparagraphs (C), (D), and (E) to ap-
16 peal to the Transportation Security Administration the deter-
17 mination and correct erroneous information.

18 (ii) MAINTENANCE OF RECORD OF MISIDENTIFIED INDIVID-
19 UALS.—The process shall include the establishment of a
20 method by which the Administrator will be able to maintain
21 a record of air passengers and other individuals who have
22 been misidentified and have corrected erroneous information.
23 To prevent repeated delays of misidentified passengers and
24 other individuals, the Transportation Security Administration
25 record shall contain information determined by the Adminis-
26 trator to authenticate the identity of such a passenger or in-
27 dividual.

28 (k) LIMITATION ON LIABILITY FOR ACTS TO THWART CRIMINAL VIO-
29 LENCE OR AIRCRAFT PIRACY.—An individual is not liable for damages in
30 an action brought in a Federal or State court arising out of the acts of the
31 individual in attempting to thwart an act of criminal violence or piracy on
32 an aircraft if that individual reasonably believed that an act of criminal vio-
33 lence or piracy was occurring or was about to occur.

34 (l) AIR CHARTER PROGRAM.—

35 (1) IN GENERAL.—The Secretary shall implement an aviation secu-
36 rity program for charter air carriers with a maximum certificated take-
37 off weight of more than 12,500 pounds.

38 (2) EXEMPTION FOR ARMED FORCES CHARTERS.—

39 (A) DEFINITION OF ARMED FORCES.—In this paragraph, the
40 term “armed forces” has the meaning given the term in section
41 101(a)(4) of title 10.

1 (B) IN GENERAL.—Paragraph (1) and the other requirements
2 of this chapter do not apply to passengers and property carried
3 by aircraft when employed to provide charter transportation to
4 members of the armed forces.

5 (C) SECURITY PROCEDURES.—The Secretary of Defense, in
6 consultation with the Secretary and the Secretary of Transpor-
7 tation, shall establish security procedures relating to the operation
8 of aircraft when employed to provide charter transportation to
9 members of the armed forces to or from an airport described in
10 subsection (e).

11 (m) SECURITY SCREENING FOR MEMBERS OF THE ARMED FORCES.—

12 (1) IN GENERAL.—The Administrator, in consultation with the De-
13 partment of Defense, shall develop and implement a plan to provide ex-
14 pedited security screening services for a member of the armed forces,
15 and, to the extent possible, an accompanying family member, if the
16 member of the armed forces, while in uniform, presents documentation
17 indicating official orders for air transportation departing from a pri-
18 mary airport (as defined in section 47102 of title 49).

19 (2) PROTOCOLS.—In developing the plan, the Administrator shall
20 consider—

21 (A) leveraging existing security screening models used to reduce
22 passenger wait times;

23 (B) establishing standard guidelines for the screening of mili-
24 tary uniform items, including combat boots; and

25 (C) incorporating new screening protocols into an existing trust-
26 ed passenger program, as established under section 109(a)(3) of
27 the Aviation and Transportation Security Act (Public Law 107–
28 71, 115 Stat. 613), or into the development of a new credential
29 or system that incorporates biometric technology and other appli-
30 cable technologies to verify the identity of individuals traveling in
31 air transportation.

32 (3) RULE OF CONSTRUCTION.—Nothing in this subsection affects the
33 authority of the Administrator to require additional screening of a
34 member of the armed forces if intelligence or law enforcement informa-
35 tion indicates that additional screening is necessary.

36 (4) REPORT.—The Administrator shall submit to the appropriate
37 committees of Congress a report on the implementation of the plan.

38 (n) PASSENGER EXIT POINTS FROM STERILE AREA.—

39 (1) DEFINITION OF STERILE AREA.—In this subsection, the term
40 “sterile area” has the meaning given the term in section 1540.5 of title

1 49, Code of Federal Regulations or any corresponding similar regula-
2 tion or ruling.

3 (2) IN GENERAL.—The Secretary shall ensure that the Transpor-
4 tation Security Administration is responsible for monitoring passenger
5 exit points from the sterile area of airports at which the Transportation
6 Security Administration provided the monitoring as of December 1,
7 2013.

8 **§ 40914. Domestic air transportation system security**

9 (a) ASSESSING THREATS.—The Administrator and the Director of the
10 Federal Bureau of Investigation jointly shall assess current and potential
11 threats to the domestic air transportation system. The assessment shall in-
12 clude consideration of the extent to which there are individuals with the ca-
13 pability and intent to carry out terrorist or related unlawful acts against
14 that system and the ways in which those individuals might carry out those
15 acts. The Administrator and the Director jointly shall decide on and carry
16 out the most effective method for continuous analysis and monitoring of se-
17 curity threats to that system.

18 (b) ASSESSING SECURITY.—In coordination with the Director of the Fed-
19 eral Bureau of Investigation, the Administrator shall carry out periodic
20 threat and vulnerability assessments on security at each airport that is part
21 of the domestic air transportation system. Each assessment shall include
22 consideration of—

23 (1) the adequacy of security procedures related to the handling and
24 transportation of checked baggage and cargo;

25 (2) space requirements for security personnel and equipment;

26 (3) separation of screened and unscreened passengers, baggage, and
27 cargo;

28 (4) separation of the controlled and uncontrolled areas of airport fa-
29 cilities; and

30 (5) coordination of the activities of security personnel of the Trans-
31 portation Security Administration, U.S. Customs and Border Protec-
32 tion, U.S. Immigration and Customs Enforcement, and air carriers,
33 and of other law enforcement personnel.

34 (c) MODAL SECURITY PLAN FOR AVIATION.—In addition to the require-
35 ments set forth in paragraphs (2) through (6) of section 11314(c) of this
36 title, the modal security plan for aviation prepared under section 11314
37 shall—

38 (1) establish a damage mitigation and recovery plan for the aviation
39 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 11314(a) of this title and shall ap-
7 prove 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 Secretary 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 Sec-
18 retary.

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 considers necessary,
4 the Secretary shall assess the effectiveness of the security measures
5 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 considers appropriate.

13 (2) MEANS OF ASSESSMENT.—The Secretary shall conduct an as-
14 sessment under paragraph (1)—

15 (A) in consultation with appropriate aeronautic authorities of
16 the government of a foreign country concerned and each air car-
17 rier serving the foreign airport for which the Secretary is con-
18 ducting the assessment;

19 (B) to establish the extent to which a foreign airport effectively
20 maintains and carries out security measures; and

21 (C) by using a standard that will result in an analysis of the
22 security measures at the airport based at least on the standards
23 and appropriate recommended practices contained in Annex 17 to
24 the Convention on International Civil Aviation in effect on the
25 date of the assessment.

26 (3) REPORT.—Each report to Congress required under section
27 40956(b) of this title shall contain a summary of the assessments con-
28 ducted under this subsection.

29 (b) CONSULTATION.—In carrying out subsection (a), the Secretary shall
30 consult with the Secretary of State—

31 (1) on the terrorist threat that exists in each country; and

32 (2) to establish which foreign airports are not under the de facto
33 control of the government of the foreign country in which they are lo-
34 cated and pose a high risk of introducing danger to international air
35 travel.

36 (c) NOTIFYING FOREIGN AUTHORITIES.—When the Secretary, after con-
37 ducting an assessment under subsection (a), decides that an airport does
38 not maintain and carry out effective security measures, the Secretary, after
39 advising the Secretary of State, shall notify the appropriate authorities of
40 the government of the foreign country of the decision and recommend the

1 steps necessary to bring the security measures in use at the airport up to
2 the standard used by the Secretary in making the assessment.

3 (d) ACTIONS WHEN AIRPORTS NOT MAINTAINING AND CARRYING OUT
4 EFFECTIVE SECURITY MEASURES.—

5 (1) IDENTIFICATION OF AIRPORT.—When the Secretary decides
6 under this section that an airport does not maintain and carry out ef-
7 fective security measures—

8 (A) the Secretary shall—

9 (i) publish the identity of the airport in the Federal Reg-
10 ister;

11 (ii) have the identity of the airport posted and displayed
12 prominently at all United States airports at which scheduled
13 air carrier operations are provided regularly; and

14 (iii) notify the news media of the identity of the airport;

15 (B) each air carrier and foreign air carrier providing transpor-
16 tation between the United States and the airport shall provide
17 written notice of the decision, on or with the ticket, to each pas-
18 senger buying a ticket for transportation between the United
19 States and the airport;

20 (C) notwithstanding section 40105(b) of title 49, the Secretary,
21 after consulting with the appropriate aeronautic authorities of the
22 foreign country concerned and each air carrier serving the airport
23 and with the approval of the Secretary of State, may withhold, re-
24 voke, or prescribe conditions on the operating authority of an air
25 carrier or foreign air carrier that uses that airport to provide for-
26 eign air transportation; and

27 (D) the President may prohibit an air carrier or foreign air car-
28 rier from providing transportation between the United States and
29 any other foreign airport that is served by aircraft flying to or
30 from the airport with respect to which a decision is made under
31 this section.

32 (2) EFFECTIVENESS.—

33 (A) IN GENERAL.—Paragraph (1) becomes effective—

34 (i) 90 days after the government of a foreign country is no-
35 tified under subsection (c) if the Secretary finds that the gov-
36 ernment has not brought the security measures at the airport
37 up to the standard the Secretary used in making an assess-
38 ment under subsection (a); or

39 (ii) immediately on the decision of the Secretary under sub-
40 section (c) if the Secretary decides, after consulting with the
41 Secretary of State, that a condition exists that threatens the

1 safety or security of passengers, aircraft, or crew traveling to
2 or from the airport.

3 (B) STATE DEPARTMENT NOTICE.—The Secretary immediately
4 shall notify the Secretary of State of a decision under subpara-
5 graph (A)(ii) of this paragraph so that the Secretary of State may
6 issue a travel advisory required under section 40918(a) of this
7 title.

8 (3) REPORT TO CONGRESS.—The Secretary promptly shall submit to
9 Congress a report (and classified annex if necessary) on action taken
10 under paragraph (1) or (2), including information on attempts made
11 to obtain the cooperation of the government of a foreign country in
12 meeting the standard the Secretary used in assessing the airport under
13 subsection (a).

14 (4) TERMINATION OF ACTION.—An action required under paragraph
15 (1)(A) and (B) is no longer required only if the Secretary, in consulta-
16 tion with the Secretary of State, decides that effective security meas-
17 ures are maintained and carried out at the airport. The Secretary shall
18 notify Congress when the action is no longer required to be taken.

19 (e) SUSPENSIONS.—Notwithstanding sections 40105(b) and 40106(b) of
20 title 49, the Secretary, with the approval of the Secretary of State and with-
21 out notice or a hearing, shall suspend the right of an air carrier or foreign
22 air carrier to provide foreign air transportation, and the right of a person
23 to operate aircraft in foreign air commerce, to or from a foreign airport
24 when the Secretary decides that—

25 (1) a condition exists that threatens the safety or security of pas-
26 sengers, aircraft, or crew traveling to or from that airport; and

27 (2) the public interest requires an immediate suspension of transpor-
28 tation between the United States and that airport.

29 (f) CONDITION OF CARRIER AUTHORITY.—This section is a condition of
30 authority the Secretary of Transportation grants under part A of subtitle
31 VII of title 49 to an air carrier or foreign air carrier.

32 **§ 40918. Travel advisory and suspension of foreign assist-**
33 **ance**

34 (a) TRAVEL ADVISORIES.—On being notified by the Secretary that the
35 Secretary has decided under section 40917(d)(2)(A)(ii) of this title that a
36 condition exists that threatens the safety or security of passengers, aircraft,
37 or crew traveling to or from a foreign airport that the Secretary has decided
38 under section 40917 does not maintain and carry out effective security
39 measures, the Secretary of State—

40 (1) immediately shall issue a travel advisory for that airport; and

41 (2) shall publicize the advisory widely.

1 (b) SUSPENDING ASSISTANCE.—The President shall suspend assistance
 2 provided under the Foreign Assistance Act of 1961 (22 U.S.C. 2151 et seq.)
 3 or the Arms Export Control Act (22 U.S.C. 2751 et seq.) to a country in
 4 which is located an airport with respect to which section 40917(d)(1) be-
 5 comes effective if the Secretary of State decides the country is a high ter-
 6 rorist threat country. The President may waive this subsection if the Presi-
 7 dent decides, and reports to Congress, that the waiver is required because
 8 of national security interests or a humanitarian emergency.

9 (c) ACTIONS NO LONGER REQUIRED.—An action required under this sec-
 10 tion is no longer required only if the Secretary has made a decision as pro-
 11 vided under section 40917(d)(4) of this title. The Secretary shall notify
 12 Congress when the action is no longer required to be taken.

13 § 40919. Passenger manifests

14 (a) AIR CARRIER REQUIREMENTS.—

15 (1) IN GENERAL.—The Secretary shall require each air carrier to
 16 provide a passenger manifest for a flight to an appropriate representa-
 17 tive of the Secretary of State—

18 (A) not later than 1 hour after that carrier is notified of an
 19 aviation disaster outside the United States involving that flight; or

20 (B) if it is not technologically feasible or reasonable to comply
 21 with clause (A) of this paragraph, then as expeditiously as possi-
 22 ble, but not later than 3 hours after the carrier is so notified.

23 (2) CONTENTS.—The passenger manifest should include the fol-
 24 lowing information:

25 (A) The full name of each passenger.

26 (B) The passport number of each passenger, if required for
 27 travel.

28 (C) The name and telephone number of a contact for each pas-
 29 senger.

30 (3) CONSIDERATION OF REQUIREMENT TO COLLECT INFORMA-
 31 TION.—In carrying out this subsection, the Secretary shall consider the
 32 necessity and feasibility of requiring air carriers to collect passenger
 33 manifest information as a condition for passengers boarding a flight of
 34 the carrier.

35 (b) FOREIGN AIR CARRIER REQUIREMENTS.—The Secretary shall con-
 36 sider imposing a requirement on foreign air carriers comparable to that im-
 37 posed on air carriers under subsection (a)(1) and (2).

38 (c) FLIGHTS IN FOREIGN AIR TRANSPORTATION TO THE UNITED
 39 STATES.—

40 (1) IN GENERAL.—Each air carrier and foreign air carrier operating
 41 a passenger flight in foreign air transportation to the United States

1 shall provide to the Commissioner of U.S. Customs and Border Protec-
2 tion by electronic transmission a passenger and crew manifest con-
3 taining the information specified in paragraph (2). Carriers may use
4 the advanced passenger information system to provide the information.

5 (2) CONTENTS.—A passenger and crew manifest for a flight required
6 under paragraph (1) shall contain the following information:

7 (A) The full name of each passenger and crew member.

8 (B) The date of birth and citizenship of each passenger and
9 crew member.

10 (C) The sex of each passenger and crew member.

11 (D) The passport number and country of issuance of each pas-
12 senger and crew member if required for travel.

13 (E) The United States visa number or resident alien card num-
14 ber of each passenger and crew member, as applicable.

15 (F) Other information the Administrator, in consultation with
16 the Commissioner of U.S. Customs and Border Protection, deter-
17 mines is reasonably necessary to ensure aviation safety.

18 (3) PASSENGER NAME RECORDS.—The carriers shall make passenger
19 name record information available to U. S. Customs and Border Pro-
20 tection on request.

21 (4) TRANSMISSION OF MANIFEST.—Subject to paragraphs (5) and
22 (6), a passenger and crew manifest required for a flight under para-
23 graph (1) shall be transmitted to U. S. Customs and Border Protection
24 in advance of the aircraft landing in the United States in the manner,
25 time, and form U.S. Customs and Border Protection prescribes.

26 (5) TRANSMISSION OF MANIFESTS TO OTHER FEDERAL AGENCIES.—
27 On request, information provided to the Secretary or U. S. Customs
28 and Border Protection under this subsection may be shared with other
29 Federal agencies for the purpose of protecting national security

30 (6) PRESCREENING INTERNATIONAL PASSENGERS.—

31 (A) IN GENERAL.—The Secretary, or the designee of the Sec-
32 retary, shall issue a notice of proposed rulemaking that will allow
33 the Department to compare passenger information for an inter-
34 national flight to or from the United States against the consoli-
35 dated and integrated terrorist watchlist maintained by the Federal
36 Government before departure of the flight.

37 (B) APPEAL PROCEDURES.—

38 (i) ESTABLISHMENT.—The Secretary shall establish a
39 timely and fair process for individuals identified as a threat
40 under subparagraph (A) to appeal to the Department the de-
41 termination and correct erroneous information.

(ii) RECORD OF MISIDENTIFIED INDIVIDUALS.—The process shall include the establishment of a method by which the Secretary will be able to maintain a record of air passengers and other individuals who have been misidentified and have corrected erroneous information. To prevent repeated delays of misidentified passengers and other individuals, the Department record shall contain information determined by the Secretary to authenticate the identity of such a passenger or individual.

§ 40920. Agreements on aircraft sabotage, aircraft hijacking, and airport security

The Secretary of State shall seek multilateral and bilateral agreement on strengthening enforcement measures and standards for compliance related to aircraft sabotage, aircraft hijacking, and airport security.

§ 40921. Intelligence

(a) DEFINITION OF INTELLIGENCE COMMUNITY.—In this section, “intelligence community” means the intelligence and intelligence-related activities of the following units of the United States Government:

- (1) Department of State.
- (2) Department of Defense.
- (3) Department of the Treasury.
- (4) Department of Energy.
- (5) Departments of the Army, Navy, and Air Force.
- (6) Central Intelligence Agency.
- (7) National Security Agency.
- (8) Defense Intelligence Agency.
- (9) Federal Bureau of Investigation.
- (10) Drug Enforcement Administration.

(b) POLICIES AND PROCEDURES ON REPORT AVAILABILITY.—The head of each unit in the intelligence community shall prescribe policies and procedures to ensure that intelligence reports about terrorism are made available, as appropriate, to the heads of other units in the intelligence community, the Secretary, and the Administrator.

(c) UNIT FOR STRATEGIC PLANNING ON TERRORISM.—The heads of the units in the intelligence community shall place greater emphasis on strategic intelligence efforts by establishing a unit for strategic planning on terrorism.

(d) DESIGNATION OF INTELLIGENCE OFFICER.—At the request of the Secretary, the Director of Central Intelligence shall designate at least one intelligence officer of the Central Intelligence Agency to serve in a senior position in the Office of the Secretary.

1 (e) WRITTEN WORKING AGREEMENTS.—The heads of units in the intel-
2 ligence community, the Secretary, and the Administrator shall review and,
3 as appropriate, revise written working agreements between the intelligence
4 community and the Administrator.

5 **§ 40922. Research and development**

6 (a) PROGRAM REQUIREMENT.—

7 (1) IN GENERAL.—The Administrator shall establish and carry out
8 a program to accelerate and expand the research, development, and im-
9 plementation of technologies and procedures to counteract terrorist acts
10 against civil aviation. The program shall provide for developing and
11 having in place new equipment and procedures necessary to meet the
12 technological challenges presented by terrorism. The program shall in-
13 clude research on, and development of, technological improvements and
14 ways to enhance human performance.

15 (2) REQUIRED ACTIONS.—In designing and carrying out the pro-
16 gram established under this subsection, the Administrator shall—

17 (A) consult and coordinate activities with other departments,
18 agencies, and instrumentalities of the United States Government
19 doing similar research;

20 (B) identify departments, agencies, and instrumentalities that
21 would benefit from that research; and

22 (C) seek cost-sharing agreements with those departments, agen-
23 cies, and instrumentalities.

24 (3) ANNUAL REPORTS.—In carrying out the program established
25 under this subsection, the Administrator shall review and consider the
26 annual reports the Secretary submits to Congress on transportation se-
27 curity and intelligence.

28 (4) DESIGNATION OF RESPONSIBLE INDIVIDUAL.—

29 (A) IN GENERAL.—In carrying out the program established
30 under this subsection, the Administrator shall designate an indi-
31 vidual to be responsible for engineering, research, and development
32 with respect to security technology under the program.

33 (B) DECISION-MAKING.—The individual designated under sub-
34 paragraph (A) shall use appropriate systems engineering and risk
35 management models in making decisions regarding the allocation
36 of funds for engineering, research, and development with respect
37 to security technology under the program.

38 (C) ANNUAL REPORT.—The individual designated under sub-
39 paragraph (A) shall, on an annual basis, submit to the Research,
40 Engineering and Development Advisory Committee a report on ac-
41 tivities under this paragraph during the preceding year. Each re-

1 port shall include, for the year covered by the report, information
2 on—

3 (i) progress made in engineering, research, and develop-
4 ment with respect to security technology;

5 (ii) the allocation of funds for engineering, research, and
6 development with respect to security technology; and

7 (iii) engineering, research, and development with respect to
8 technologies drawn from other agencies, including the ration-
9 ale for engineering, research, and development with respect to
10 the technologies.

11 (5) GRANTS.—The Administrator may—

12 (A) make grants to institutions of higher learning and other ap-
13 propriate research facilities with demonstrated ability to carry out
14 research described in paragraph (1), and fix the amounts and
15 terms of the grants; and

16 (B) make cooperative agreements with governmental authorities
17 the Administrator decides are appropriate.

18 (b) REVIEW OF THREATS.—

19 (1) IN GENERAL.—The Administrator periodically shall review
20 threats to civil aviation, with particular focus on—

21 (A) a comprehensive systems analysis (employing vulnerability
22 analysis, threat attribute definition, and technology roadmaps) of
23 the civil aviation system, including—

24 (i) the destruction, commandeering, or diversion of civil air-
25 craft or the use of civil aircraft as a weapon; and

26 (ii) the disruption of civil aviation service, including by
27 cyberattack;

28 (B) explosive material that presents the most significant threat
29 to civil aircraft;

30 (C) the minimum amounts, configurations, and types of explo-
31 sive material that can cause, or would reasonably be expected to
32 cause, catastrophic damage to aircraft in air transportation;

33 (D) the amounts, configurations, and types of explosive material
34 that can be detected reliably by existing, or reasonably anticipated,
35 near-term explosive detection technologies;

36 (E) the potential release of chemical, biological, or similar weap-
37 ons or devices either within an aircraft or within an airport;

38 (F) the feasibility of using various ways to minimize damage
39 caused by explosive material that cannot be detected reliably by
40 existing, or reasonably anticipated, near-term explosive detection
41 technologies;

1 (G) the ability to screen passengers, carry-on baggage, checked
2 baggage, and cargo; and

3 (H) the technologies that might be used in the future to at-
4 tempt to destroy or otherwise threaten commercial aircraft and the
5 way in which those technologies can be countered effectively.

6 (2) PROGRAM FOCUS AND PRIORITIES.—The Administrator shall use
7 the results of the review under this subsection to develop the focus and
8 priorities of the program established under subsection (a).

9 (c) SCIENTIFIC ADVISORY PANEL.—

10 (1) ESTABLISHMENT.—The Administrator shall establish a scientific
11 advisory panel, as a subcommittee of the Research, Engineering, and
12 Development Advisory Committee, to review, comment on, advise the
13 progress of, and recommend modifications in, the program established
14 under subsection (a), including the need for long-range research pro-
15 grams to detect and prevent catastrophic damage to commercial air-
16 craft, commercial aviation facilities, commercial aviation personnel and
17 passengers, and other components of the commercial aviation system
18 by the next generation of terrorist weapons.

19 (2) PANEL MEMBERS.—

20 (A) QUALIFICATIONS.—The advisory panel shall consist of indi-
21 viduals who have scientific and technical expertise in—

22 (i) the development and testing of effective explosive detec-
23 tion systems;

24 (ii) aircraft structure and experimentation to decide on the
25 type and minimum weights of explosives that an effective ex-
26 plosive detection technology must be capable of detecting;

27 (iii) technologies involved in minimizing airframe damage
28 to aircraft from explosives; and

29 (iv) other scientific and technical areas the Administrator
30 considers appropriate.

31 (B) CONSIDERATIONS.—In appointing individuals to the advi-
32 sory panel, the Administrator should consider individuals from
33 academia and the national laboratories, as appropriate.

34 (3) ORGANIZATION AS TEAMS.—The Administrator shall organize the
35 advisory panel into teams capable of undertaking the review of policies
36 and technologies upon request.

37 (4) BIENNIAL REVIEW.—The Administrator shall review the com-
38 position of the advisory panel every 2 years to ensure that the expertise
39 of the individuals on the panel is suited to the current and anticipated
40 duties of the panel.

§ 40923. Explosive detection

(a) DEPLOYMENT AND PURCHASE OF EQUIPMENT.—

(1) IN GENERAL.—A deployment or purchase of explosive detection equipment under section 108.7(b)(8) or 108.20 of title 14, Code of Federal Regulations, or similar regulation is required only if the Administrator certifies that the equipment alone, or as part of an integrated system, can detect under realistic air carrier operating conditions the amounts, configurations, and types of explosive material that would likely be used to cause catastrophic damage to commercial aircraft. The Administrator shall base the certification on the results of tests conducted under protocols developed in consultation with expert scientists outside of the Transportation Security Administration.

(2) FACILITATING DEPLOYMENT.—Until the Administrator determines that equipment certified under paragraph (1) is commercially available and has successfully completed operational testing as provided in paragraph (1), the Administrator shall facilitate the deployment of approved commercially available explosive detection devices the Administrator determines will enhance aviation security significantly. The Administrator shall require that equipment deployed under this paragraph be replaced by equipment certified under paragraph (1) when equipment certified under paragraph (1) becomes commercially available. The Administrator, based on operational considerations at individual airports, may waive the required installation of commercially available equipment under paragraph (1) in the interests of aviation security. The Administrator may permit the requirements of this paragraph to be met at airports by the deployment of dogs or other appropriate animals to supplement equipment for screening passengers, baggage, mail, or cargo for explosives or weapons.

(3) PURCHASES BY ADMINISTRATOR.—This subsection does not prohibit the Administrator from purchasing or deploying explosive detection equipment described in paragraph (1).

(b) GRANTS.—The Administrator may provide grants to continue the Explosive Detection K-9 Team Training Program to detect explosives at airports and on aircraft.

§ 40924. Airport construction guidelines

In consultation with air carriers, airport authorities, and others the Administrator considers appropriate, the Administrator shall develop guidelines for airport design and construction to allow for maximum security enhancement. In developing the guidelines, the Administrator shall consider the results of the assessment carried out under section 40914(a) of this title.

§ 40925. Alaska exemptions

The Administrator may exempt from sections 40911, 40913(a) through (c) and (e), 40916, 40953, and 40954 of this title airports in Alaska served only by air carriers that—

(1) hold certificates issued under section 41102 of title 49;

(2) operate aircraft with certificates for a maximum gross takeoff weight of less than 12,500 pounds; and

(3) board passengers, or load property intended to be carried in an aircraft cabin, that will be screened under section 40911 of this title at another airport in Alaska before the passengers board, or the property is loaded on, an aircraft for a place outside Alaska.

§ 40926. Assessments and evaluations

(a) PERIODIC ASSESSMENTS.—The Administrator shall require each air carrier and airport (including the airport owner or operator in cooperation with the air carriers and vendors serving each airport) that provides for intrastate, interstate, or foreign air transportation to conduct periodic vulnerability assessments of the security systems of that air carrier or airport, respectively. The Transportation Security Administration shall perform periodic audits of the assessments.

(b) INVESTIGATIONS.—The Administrator shall conduct periodic and unannounced inspections of security systems of airports and air carriers to determine the effectiveness and vulnerabilities of the systems. To the extent allowable by law, the Administrator may provide for anonymous tests of those security systems.

§ 40927. Federal air marshals and training of law enforcement personnel

(a) IN GENERAL.—The Administrator under the authority provided by section 40913(d) of this title—

(1) may provide for deployment of Federal air marshals on every passenger flight of air carriers in air transportation or intrastate air transportation;

(2) shall provide for deployment of Federal air marshals on every flight determined by the Secretary to present high security risks;

(3) shall provide for appropriate training, supervision, and equipment of Federal air marshals;

(4) shall require air carriers providing flights described in paragraph (1) to provide seating for a Federal air marshal on the flight without regard to the availability of seats on the flight and at no cost to the United States Government or the marshal;

(5) may require air carriers to provide, on a space-available basis, to an off-duty Federal air marshal a seat on a flight to the airport

1 nearest the marshal's home at no cost to the marshal or the United
2 States Government if the marshal is traveling to that airport after
3 completing his or her security duties;

4 (6) may enter into agreements with Federal, State, and local agen-
5 cies under which appropriately trained law enforcement personnel from
6 the agencies, when traveling on a flight of an air carrier, will carry a
7 firearm and be prepared to assist Federal air marshals;

8 (7) shall establish procedures to ensure that Federal air marshals
9 are made aware of armed or unarmed law enforcement personnel on
10 board an aircraft; and

11 (8) may appoint as a Federal air marshal, regardless of age (if the
12 individual otherwise meets the background and fitness qualifications re-
13 quired for Federal air marshals)—

14 (A) an individual who is a retired law enforcement officer; or

15 (B) an individual who is a retired member of the armed forces.

16 (b) LONG DISTANCE FLIGHTS.—In making the determination under sub-
17 section (a)(2), nonstop, long distance flights, such as those targeted on Sep-
18 tember 11, 2001, should be a priority.

19 (c) CONTINUATION OF INITIATIVES TO PROTECT ANONYMITY OF FED-
20 ERAL AIR MARSHALS.—The Director of the Federal Air Marshal Service
21 shall continue operational initiatives to protect the anonymity of Federal air
22 marshals.

23 (d) TRAINING FOR FEDERAL AND LOCAL LAW ENFORCEMENT PER-
24 SONNEL.—

25 (1) AVAILABILITY OF INFORMATION.—The Director of Immigration
26 and Customs Enforcement and the Director of the Federal Air Marshal
27 Service shall make available, as practicable, appropriate information on
28 in-flight counterterrorism and weapons handling procedures and tactics
29 training to Federal law enforcement officers who fly while in possession
30 of a firearm.

31 (2) IDENTIFICATION OF FRAUDULENT DOCUMENTS.—The Director
32 of Immigration and Customs Enforcement and the Director of the Fed-
33 eral Air Marshal Service, in coordination with the Administrator, shall
34 ensure that Transportation Security Administration screeners and Fed-
35 eral air marshals receive training in identifying fraudulent identifica-
36 tion documents, including fraudulent or expired visas and passports.
37 The training also shall be made available to other Federal law enforce-
38 ment agencies and local law enforcement agencies located in a State
39 that borders Canada or Mexico.

40 (e) TRAINING FOR FOREIGN LAW ENFORCEMENT PERSONNEL.—

1 (1) IN GENERAL.—The Director of Immigration and Customs En-
 2 forcement, after consultation with the Secretary of State, may direct
 3 the Federal Air Marshal Service to provide appropriate air marshal
 4 training to law enforcement personnel of foreign countries.

5 (2) WATCHLIST SCREENING.—The Federal Air Marshal Service may
 6 only provide appropriate air marshal training to law enforcement per-
 7 sonnel of foreign countries after comparing the identifying information
 8 and records of law enforcement personnel of foreign countries against
 9 all appropriate records in the consolidated and integrated terrorist
 10 watchlists maintained by the Federal Government.

11 (3) FEES.—The Director of Immigration and Customs Enforcement
 12 shall establish reasonable fees and charges to pay expenses incurred in
 13 carrying out this subsection. Funds collected under this subsection
 14 shall be credited to the account in the Treasury from which the ex-
 15 penses were incurred and shall be available to the Director of Immigra-
 16 tion and Customs Enforcement for purposes for which amounts in the
 17 account are available.

18 **§ 40928. Crew training**

19 (a) BASIC SECURITY TRAINING.—

20 (1) IN GENERAL.—Each air carrier providing scheduled passenger
 21 air transportation shall carry out a training program for flight and
 22 cabin crew members to prepare the crew members for potential threat
 23 conditions.

24 (2) PROGRAM ELEMENTS.—An air carrier training program under
 25 this subsection shall include, at a minimum, elements that address each
 26 of the following:

27 (A) Recognizing suspicious activities and determining the seri-
 28 ousness of an occurrence.

29 (B) Crew communication and coordination.

30 (C) The proper commands to give passengers and attackers.

31 (D) Appropriate responses to defend oneself.

32 (E) Use of protective devices assigned to crew members (to the
 33 extent devices are required by the Administrator and the Adminis-
 34 trator of the Federal Aviation Administration).

35 (F) Psychology of terrorists to cope with hijacker behavior and
 36 passenger responses.

37 (G) Situational training exercises regarding various threat con-
 38 ditions.

39 (H) Flight deck procedures or aircraft maneuvers to defend the
 40 aircraft and cabin crew responses to the procedures and maneu-
 41 vers.

1 (I) The proper conduct of a cabin search, including explosive de-
2 vice recognition.

3 (J) Other subject matter considered appropriate by the Admin-
4 istrator.

5 (3) APPROVAL.—An air carrier training program under this sub-
6 section shall be subject to approval by the Administrator.

7 (4) MINIMUM STANDARDS.—The Administrator may establish min-
8 imum standards for the training provided under this subsection and for
9 recurrent training.

10 (5) PROGRAMS TO CONTINUE IN EFFECT.—Notwithstanding para-
11 graphs (3) and (4), a training program of an air carrier to prepare
12 flight and cabin crew members for potential threat conditions that was
13 approved by the Administrator of the Federal Aviation Administration
14 or the Administrator before December 12, 2003, may continue in effect
15 until disapproved or ordered modified by the Administrator.

16 (6) MONITORING.—The Administrator, in consultation with the Ad-
17 ministrator of the Federal Aviation Administration, shall monitor air
18 carrier training programs under this subsection and periodically shall
19 review an air carrier's training program to ensure that the program is
20 adequately preparing crew members for potential threat conditions. In
21 determining when an air carrier's training program should be reviewed
22 under this paragraph, the Administrator shall consider complaints from
23 crew members. The Administrator shall ensure that employees respon-
24 sible for monitoring the training programs have the necessary resources
25 and knowledge.

26 (7) UPDATES.—The Administrator, in consultation with the Admin-
27 istrator of the Federal Aviation Administration, shall order air carriers
28 to modify training programs under this subsection to reflect new or dif-
29 ferent security threats.

30 (b) ADVANCED SELF-DEFENSE TRAINING.—

31 (1) IN GENERAL.—The Administrator shall develop and provide a
32 voluntary training program for flight and cabin crew members of air
33 carriers providing scheduled passenger air transportation.

34 (2) PROGRAM ELEMENTS.—The training program under this sub-
35 section shall include both classroom and effective hands-on training in
36 the following elements of self-defense:

37 (A) Deterring a passenger who might present a threat.

38 (B) Advanced control, striking, and restraint techniques.

39 (C) Training to defend oneself against edged or contact weap-
40 ons.

41 (D) Methods to subdue and restrain an attacker.

1 (E) Use of available items aboard the aircraft for self-defense.

2 (F) Appropriate and effective responses to defend oneself, in-
3 cluding the use of force against an attacker.

4 (G) Other elements of training that the Administrator considers
5 appropriate.

6 (3) PARTICIPATION NOT REQUIRED.—A crew member shall not be
7 required to participate in the training program under this subsection.

8 (4) COMPENSATION.—Neither the Federal Government nor an air
9 carrier shall be required to compensate a crew member for partici-
10 pating in the training program under this subsection.

11 (5) FEES.—A crew member is not required to pay a fee for the
12 training program under this subsection.

13 (6) CONSULTATION.—In developing the training program under this
14 subsection, the Administrator shall consult with law enforcement per-
15 sonnel and security experts who have expertise in self-defense training,
16 terrorism experts, representatives of air carriers, the director of self-
17 defense training in the Federal Air Marshal Service, flight attendants,
18 labor organizations representing flight attendants, and educational in-
19 stitutions offering law enforcement training programs.

20 (7) DESIGNATION OF TRANSPORTATION SECURITY ADMINISTRATION
21 OFFICIAL.—The Administrator shall designate an official in the Trans-
22 portation Security Administration to be responsible for implementing
23 the training program under this subsection. The official shall consult
24 with air carriers and labor organizations representing crew members
25 before implementing the program to ensure that it is appropriate for
26 situations that may arise on board an aircraft during a flight.

27 (c) LIMITATION.—Actions by crew members under this section shall be
28 subject to the provisions of section 40913(k) of this title.

29 **§ 40929. Security screening program**

30 (a) IN GENERAL.—An operator of an airport may submit to the Adminis-
31 trator an application to have the screening of passengers and property at
32 the airport under section 40911 of this title be carried out by the screening
33 personnel of a qualified private screening company under a contract entered
34 into with the Administrator.

35 (b) APPROVAL OF APPLICATIONS.—

36 (1) IN GENERAL.—Not later than 120 days after the date of receipt
37 of an application submitted by an airport operator under subsection
38 (a), the Administrator shall approve or deny the application.

39 (2) STANDARDS.—The Administrator shall approve an application
40 submitted by an airport operator under subsection (a) if the Adminis-
41 trator determines that the approval would not compromise security or

1 detrimentally affect the cost-efficiency or the effectiveness of the
2 screening of passengers or property at the airport.

3 (3) REPORTS ON DENIALS OF APPLICATIONS.—

4 (A) IN GENERAL.—If the Administrator denies an application
5 submitted by an airport operator under subsection (a), the Admin-
6 istrator shall provide to the airport operator, not later than 60
7 days following the date of the denial, a written report that sets
8 forth—

9 (i) the findings that served as the basis for the denial;

10 (ii) the results of cost or security analysis conducted in
11 considering the application; and

12 (iii) recommendations on how the airport operator can ad-
13 dress the reasons for the denial.

14 (B) SUBMISSION TO CONGRESS.—The Administrator shall sub-
15 mit to the Committee on Commerce, Science, and Transportation
16 of the Senate and the Committee on Homeland Security of the
17 House of Representatives a copy of a report provided to an airport
18 operator under subparagraph (A).

19 (c) QUALIFIED PRIVATE SCREENING COMPANY.—A private screening
20 company is qualified to provide screening services at an airport under this
21 section if the company will only employ individuals to provide the services
22 who meet all the requirements of this chapter applicable to Federal Govern-
23 ment personnel who perform screening services at airports under this chap-
24 ter and will provide compensation and other benefits to the individuals that
25 are not less than the level of compensation and other benefits provided to
26 the Federal Government personnel in accordance with this chapter.

27 (d) STANDARDS FOR PRIVATE SCREENING COMPANIES.—

28 (1) IN GENERAL.—The Administrator may enter into a contract with
29 a private screening company to provide screening at an airport under
30 this section only if the Administrator determines and certifies to Con-
31 gress that—

32 (A) the level of screening services and protection provided at the
33 airport under the contract will be equal to or greater than the level
34 that would be provided at the airport by Federal Government per-
35 sonnel under this chapter; and

36 (B) the private screening company is owned and controlled by
37 a citizen of the United States, to the extent that the Administrator
38 determines that there are private screening companies owned and
39 controlled by citizens of the United States.

40 (2) WAIVERS.—The Administrator may waive the requirement of
41 paragraph (1)(B) for a company that is a United States subsidiary

1 with a parent company that has implemented a foreign ownership, con-
2 trol, or influence mitigation plan that has been approved by the De-
3 fense Security Service of the Department of Defense prior to the sub-
4 mission of the application. The Administrator has complete discretion
5 to reject any application from a private screening company that re-
6 quires a waiver under this paragraph to provide screening services at
7 an airport.

8 (e) SUPERVISION OF SCREENED PERSONNEL.—The Administrator shall
9 provide Federal Government supervisors to oversee all screening at each air-
10 port at which screening services are provided under this section and provide
11 Federal Government law enforcement officers at the airport pursuant to this
12 chapter.

13 (f) TERMINATION OF CONTRACTS.—The Administrator may terminate a
14 contract entered into with a private screening company to provide screening
15 services at an airport under this section if the Administrator finds that the
16 company has failed repeatedly to comply with a standard, regulation, direc-
17 tive, order, law, or contract applicable to the hiring or training of personnel
18 to provide services or to the provision of screening at the airport.

19 (g) OPERATOR NOT LIABLE.—An operator of an airport is not liable for
20 a claim for damages filed in State or Federal court (including a claim for
21 compensatory, punitive, contributory, or indemnity damages) relating to—

22 (1) the airport operator's decision—

23 (A) to submit an application to the Administrator under sub-
24 section (a) or former section 44919 of title 49; or

25 (B) not to submit an application; and

26 (2) an act of negligence, gross negligence, or intentional wrongdoing
27 by—

28 (A) a qualified private screening company or its employees in
29 a case in which the qualified private screening company is acting
30 under a contract entered into with the Secretary or the Secretary's
31 designee; or

32 (B) employees of the Federal Government providing passenger
33 and property security screening services at the airport.

34 (h) RECOMMENDATIONS OF AIRPORT OPERATOR.—As part of any sub-
35 mission of an application for a private screening company to provide screen-
36 ing services at an airport, the airport operator shall provide to the Adminis-
37 trator a recommendation as to which company would best serve the security
38 screening and passenger needs of the airport, along with a statement ex-
39 plaining the basis of the operator's recommendation.

40 (i) OPERATOR LIABILITY.—Nothing in this section shall relieve an airport
41 operator from liability for its own acts or omissions related to its security

1 responsibilities. Except as may be provided by subchapter IV of chapter 105
2 of this title, nothing in this section shall relieve a qualified private screening
3 company or its employees from liability related to its own acts of negligence,
4 gross negligence, or intentional wrongdoing.

5 **§ 40930. Federal flight deck officer program**

6 (a) DEFINITIONS.—In this section:

7 (1) AIR TRANSPORTATION.—The term “air transportation” includes
8 all-cargo air transportation.

9 (2) PILOT.—The term “pilot” means an individual who has final au-
10 thority and responsibility for the operation and safety of the flight or
11 another flight deck crew member.

12 (b) EXEMPTION.—This section does not apply to air carriers operating
13 under part 135 of title 14, Code of Federal Regulations, and to pilots em-
14 ployed by the carriers to the extent that the carriers and pilots are covered
15 by section 135.119 of title 14 or a successor to that section.

16 (c) ESTABLISHMENT.—The Administrator shall establish a program to
17 deputize volunteer pilots of air carriers providing air transportation or intra-
18 state air transportation as Federal law enforcement officers to defend the
19 flight decks of aircraft of air carriers against acts of criminal violence or
20 air piracy. The officers shall be known as “Federal flight deck officers”.

21 (d) PROCEDURAL REQUIREMENTS.—

22 (1) IN GENERAL.—The Administrator shall establish procedural re-
23 quirements to carry out the program under this section.

24 (2) COMMENCEMENT OF PROGRAM.—The Administrator shall under-
25 take the process of training and deputizing pilots who are qualified to
26 be Federal flight deck officers as Federal flight deck officers under the
27 program.

28 (3) ISSUES TO BE ADDRESSED.—The procedural requirements estab-
29 lished under paragraph (1) shall address the following issues:

30 (A) The type of firearm to be used by a Federal flight deck offi-
31 cer.

32 (B) The type of ammunition to be used by a Federal flight deck
33 officer.

34 (C) The standards and training needed to qualify and requalify
35 as a Federal flight deck officer.

36 (D) The placement of the firearm of a Federal flight deck offi-
37 cer on board the aircraft to ensure both its security and its ease
38 of retrieval in an emergency.

39 (E) An analysis of the risk of catastrophic failure of an aircraft
40 as a result of the discharge (including an accidental discharge) of

1 a firearm to be used in the program into the avionics, electrical
2 systems, or other sensitive areas of the aircraft.

3 (F) The division of responsibility between pilots in the event of
4 an act of criminal violence or air piracy if only one pilot is a Fed-
5 eral flight deck officer and if both pilots are Federal flight deck
6 officers.

7 (G) Procedures for ensuring that the firearm of a Federal flight
8 deck officer does not leave the cockpit if there is a disturbance in
9 the passenger cabin of the aircraft or if the pilot leaves the cockpit
10 for personal reasons.

11 (H) Interaction between a Federal flight deck officer and a Fed-
12 eral air marshal on board the aircraft.

13 (I) The process for selection of pilots to participate in the pro-
14 gram based on their fitness to participate in the program, includ-
15 ing whether an additional background check should be required be-
16 yond that required by section 40954(a)(1) of this title.

17 (J) Storage and transportation of firearms between flights, in-
18 cluding international flights, to ensure the security of the firearms,
19 focusing particularly on whether security would be enhanced by re-
20 quiring storage of the firearm at the airport when the pilot leaves
21 the airport to remain overnight away from the pilot's base airport.

22 (K) Methods for ensuring that security personnel will be able
23 to identify whether a pilot may carry a firearm under the pro-
24 gram.

25 (L) Methods for ensuring that pilots (including Federal flight
26 deck officers) will be able to identify whether a passenger is a law
27 enforcement officer who may carry a firearm aboard the aircraft.

28 (M) Other issues that the Administrator considers necessary.

29 (4) PREFERENCE.—In selecting pilots to participate in the program,
30 the Administrator shall give preference to pilots who are former mili-
31 tary or law enforcement personnel.

32 (5) CLASSIFIED INFORMATION.—Notwithstanding section 552 of title
33 5 but subject to section 40119 of title 49, information developed under
34 paragraph (3)(E) shall not be disclosed.

35 (6) NOTICE TO CONGRESS.—The Administrator shall provide notice
36 to the Committee on Transportation and Infrastructure of the House
37 of Representatives and the Committee on Commerce, Science, and
38 Transportation of the Senate after completing the analysis required by
39 paragraph (3)(E).

40 (7) MINIMIZATION OF RISK.—If the Administrator determines as a
41 result of the analysis under paragraph (3)(E) that there is a significant

1 risk of the catastrophic failure of an aircraft as a result of the dis-
2 charge of a firearm, the Administrator shall take necessary actions to
3 minimize that risk.

4 (8) REVIEW STANDARD.—The Administrator’s decisions regarding
5 the methods for implementing each of the procedural requirements
6 specified in paragraph (3) shall be subject to review only for abuse of
7 discretion.

8 (e) TRAINING, SUPERVISION, AND EQUIPMENT.—

9 (1) IN GENERAL.—The Administrator shall only be obligated to pro-
10 vide the training, supervision, and equipment necessary for a pilot to
11 be a Federal flight deck officer under this section at no expense to the
12 pilot or the air carrier employing the pilot.

13 (2) TRAINING.—

14 (A) IN GENERAL.—The Administrator shall base the require-
15 ments for the training of Federal flight deck officers under sub-
16 section (d) on the training standards applicable to Federal air
17 marshals, except that the Administrator shall take into account
18 the differing roles and responsibilities of Federal flight deck offi-
19 cers and Federal air marshals.

20 (B) ELEMENTS.—The training of a Federal flight deck officer
21 shall include, at a minimum—

22 (i) training to ensure that the officer achieves the level of
23 proficiency with a firearm required under subparagraph
24 (C)(i);

25 (ii) training to ensure that the officer maintains exclusive
26 control over the officer’s firearm at all times, including train-
27 ing in defensive maneuvers; and

28 (iii) training to assist the officer in determining when it is
29 appropriate to use the officer’s firearm and when it is appro-
30 priate to use less than lethal force.

31 (C) TRAINING IN USE OF FIREARMS.—

32 (i) LEVEL OF PROFICIENCY.—To be deputized as a Federal
33 flight deck officer, a pilot must achieve a level of proficiency
34 with a firearm that is required by the Administrator. The
35 level shall be comparable to the level of proficiency required
36 of Federal air marshals.

37 (ii) TRAINING BY ADMINISTRATOR OR FIREARMS TRAINING
38 FACILITY.—The training of a Federal flight deck officer in
39 the use of a firearm may be conducted by the Administrator
40 or by a firearms training facility approved by the Adminis-
41 trator.

1 (iii) REQUALIFICATION.—The Administrator shall require a
2 Federal flight deck officer to requalify to carry a firearm
3 under the program. The requalification shall occur at an in-
4 terval required by the Administrator.

5 (f) DEPUTIZATION.—

6 (1) IN GENERAL.—The Administrator may deputize, as a Federal
7 flight deck officer under this section, a pilot who submits to the Admin-
8 istrator a request to be such an officer and who the Administrator de-
9 termines is qualified to be such an officer.

10 (2) QUALIFICATION.—A pilot is qualified to be a Federal flight deck
11 officer under this section if—

12 (A) the pilot is employed by an air carrier;

13 (B) the Administrator determines that the pilot meets the
14 standards established by the Administrator for being a Federal
15 flight deck officer; and

16 (C) the Administrator determines that the pilot has completed
17 the training required by the Administrator.

18 (3) DEPUTIZATION BY OTHER FEDERAL AGENCIES.—The Adminis-
19 trator may request another Federal agency to deputize, as Federal
20 flight deck officers under this section, pilots that the Administrator de-
21 termines are qualified to be Federal flight deck officers.

22 (4) REVOCATION.—The Administrator may revoke the deputization
23 of a pilot as a Federal flight deck officer if the Administrator finds
24 that the pilot is no longer qualified to be a Federal flight deck officer.

25 (g) COMPENSATION.—Pilots participating in the program under this sec-
26 tion shall not be eligible for compensation from the Federal Government for
27 services provided as a Federal flight deck officer. The Federal Government
28 and air carriers shall not be obligated to compensate a pilot for partici-
29 pating in the program or for the pilot's training or qualification and requali-
30 fication to carry firearms under the program.

31 (h) AUTHORITY TO CARRY FIREARMS.—

32 (1) IN GENERAL.—The Administrator shall authorize a Federal
33 flight deck officer to carry a firearm while engaged in providing air
34 transportation or intrastate air transportation. Notwithstanding sub-
35 section (e)(1), the officer may purchase a firearm and carry that fire-
36 arm aboard an aircraft of which the officer is the pilot under this sec-
37 tion if the firearm is of a type that may be used under the program.

38 (2) PREEMPTION.—Notwithstanding any other provision of Federal
39 or State law, a Federal flight deck officer, whenever necessary to par-
40 ticipate in the program, may carry a firearm in a State and from one
41 State to another State.

1 (3) CARRYING FIREARMS OUTSIDE UNITED STATES.—In consultation
2 with the Secretary of State, the Administrator may take necessary ac-
3 tion to ensure that a Federal flight deck officer may carry a firearm
4 in a foreign country whenever necessary to participate in the program.

5 (i) AUTHORITY TO USE FORCE.—Notwithstanding section 40913(d) of
6 this title, the Administrator shall prescribe the standards and circumstances
7 under which a Federal flight deck officer may use, while the program under
8 this section is in effect, force (including lethal force) against an individual
9 in the defense of the flight deck of an aircraft in air transportation or intra-
10 state air transportation.

11 (j) LIMITATION ON LIABILITY.—

12 (1) AIR CARRIERS.—An air carrier is not liable for damages in an
13 action brought in a Federal or State court arising out of a Federal
14 flight deck officer's use of or failure to use a firearm.

15 (2) FEDERAL FLIGHT DECK OFFICERS.—A Federal flight deck offi-
16 cer is not liable for damages in an action brought in a Federal or State
17 court arising out of the acts or omissions of the officer in defending
18 the flight deck of an aircraft against acts of criminal violence or air
19 piracy unless the officer is guilty of gross negligence or willful mis-
20 conduct.

21 (3) FEDERAL GOVERNMENT.—For purposes of an action against the
22 United States with respect to an act or omission of a Federal flight
23 deck officer in defending the flight deck of an aircraft, the officer shall
24 be treated as an employee of the Federal Government under chapter
25 171 of title 28, relating to tort claims procedure.

26 (k) PROCEDURES FOLLOWING ACCIDENTAL DISCHARGES.—If an acci-
27 dental discharge of a firearm under the pilot program results in the injury
28 or death of a passenger or crew member on an aircraft, the Administrator—

29 (1) shall revoke the deputization of the Federal flight deck officer
30 responsible for that firearm if the Administrator determines that the
31 discharge was attributable to the negligence of the officer; and

32 (2) if the Administrator determines that a shortcoming in standards,
33 training, or procedures was responsible for the accidental discharge,
34 may temporarily suspend the program until the shortcoming is cor-
35 rected.

36 (l) LIMITATION ON AUTHORITY OF AIR CARRIERS.—An air carrier may
37 not—

38 (1) prohibit a pilot employed by the air carrier from becoming a Fed-
39 eral flight deck officer under this section;

40 (2) threaten a retaliatory action against a pilot employed by the air
41 carrier for becoming a Federal flight deck officer under this section;

1 (3) prohibit a Federal flight deck officer from piloting an aircraft op-
 2 erated by the air carrier; or

3 (4) terminate the employment of a Federal flight deck officer, solely
 4 on the basis of his or her volunteering for or participating in the pro-
 5 gram under this section.

6 **§ 40931. Deputation of State and local law enforcement offi-**
 7 **cers**

8 (a) DEPUTATION AUTHORITY.—The Administrator may deputize a State
 9 or local law enforcement officer to carry out Federal airport security duties
 10 under this chapter.

11 (b) FULFILLMENT OF REQUIREMENTS.—A State or local law enforcement
 12 officer who is deputized under this section shall be treated as a Federal law
 13 enforcement officer for purposes of meeting the requirements of this chapter
 14 and other provisions of law to provide Federal law enforcement officers to
 15 carry out Federal airport security duties.

16 (c) AGREEMENTS.—To deputize a State or local law enforcement officer
 17 under this section, the Administrator shall enter into a voluntary agreement
 18 with the appropriate State or local law enforcement agency that employs the
 19 State or local law enforcement officer.

20 (d) REIMBURSEMENT.—

21 (1) IN GENERAL.—The Administrator shall reimburse a State or
 22 local law enforcement agency for all reasonable, allowable, and allocable
 23 costs incurred by the State or local law enforcement agency with re-
 24 spect to a law enforcement officer deputized under this section.

25 (2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to
 26 be appropriated such sums as may be necessary to carry out this sub-
 27 section.

28 (e) FEDERAL TORT CLAIMS ACT.—A State or local law enforcement offi-
 29 cer who is deputized under this section shall be treated as an “employee
 30 of the Government” for purposes of sections 1346(b) and 2401(b) and chap-
 31 ter 171 of title 28 while carrying out Federal airport security duties in the
 32 course and scope of the officer’s employment, subject to Federal supervision
 33 and control, and under the terms of the deputation.

34 (f) STATIONING OF OFFICERS.—The Administrator may allow law en-
 35 forcement personnel to be stationed other than at the airport security
 36 screening location if that would be preferable for law enforcement purposes
 37 and if the personnel would still be able to provide a prompt response to
 38 problems occurring at the screening location.

39 **§ 40932. Airport security improvement projects**

40 (a) DEFINITION OF SPONSOR.—In this section, the term “sponsor” has
 41 the meaning given the term in section 47102 of title 49.

1 (b) GRANT AUTHORITY.—Subject to the requirements of this section, the
2 Administrator shall make grants to airport sponsors—

3 (1) for projects to replace baggage conveyer systems related to avia-
4 tion security;

5 (2) for projects to reconfigure terminal baggage areas as needed to
6 install explosive detection systems;

7 (3) for projects to enable the Administrator to deploy explosive detec-
8 tion systems behind the ticket counter, in the baggage sorting area, or
9 in line with the baggage handling system; and

10 (4) for other airport security capital improvement projects.

11 (c) APPLICATIONS.—A sponsor seeking a grant under this section shall
12 submit to the Administrator an application in the form, and containing the
13 information, the Administrator prescribes.

14 (d) APPROVAL.—The Administrator, after consultation with the Secretary
15 of Transportation, may approve an application of a sponsor for a grant
16 under this section only if the Administrator determines that the project will
17 improve security at an airport or improve the efficiency of the airport with-
18 out lessening security.

19 (e) LETTERS OF INTENT.—

20 (1) ISSUANCE.—The Administrator shall issue a letter of intent to
21 a sponsor committing to obligate from future budget authority an
22 amount, not more than the Federal Government's share of the project's
23 cost, for an airport security improvement project (including interest
24 costs and costs of formulating the project).

25 (2) SCHEDULE.—A letter of intent under this subsection shall estab-
26 lish a schedule under which the Administrator will reimburse the spon-
27 sor for the Government's share of the project's costs, as amounts be-
28 come available, if the sponsor, after the Administrator issues the letter,
29 carries out the project without receiving amounts under this section.

30 (3) NOTICE TO ADMINISTRATOR.—A sponsor that has been issued a
31 letter of intent under this subsection shall notify the Administrator of
32 the sponsor's intent to carry out a project before the project begins.

33 (4) NOTICE TO CONGRESS.—The Administrator shall transmit to the
34 Committees on Appropriations and Transportation and Infrastructure
35 of the House of Representatives and the Committees on Appropriations
36 and Commerce, Science and Transportation of the Senate a written no-
37 tification at least 3 days before the issuance of a letter of intent under
38 this section.

39 (5) LIMITATIONS.—A letter of intent issued under this subsection is
40 not an obligation of the Government under section 1501 of title 31,
41 and the letter is not deemed to be an administrative commitment for

1 financing. An obligation or administrative commitment may be made
2 only as amounts are provided in authorization and appropriations laws.

3 (6) STATUTORY CONSTRUCTION.—Nothing in this subsection shall be
4 construed to prohibit the obligation of amounts pursuant to a letter of
5 intent under this subsection in the same fiscal year as the letter of in-
6 tent is issued.

7 (f) FEDERAL SHARE.—The Government's share of the cost of a project
8 under this section shall be 90 percent for a project at a medium or large
9 hub airport and 95 percent for a project at any other airport.

10 (g) APPLICABILITY OF CERTAIN REQUIREMENTS.—The requirements
11 that apply to grants and letters of intent issued under chapter 471 of title
12 49 (other than section 47102(3)) shall apply to grants and letters of intent
13 issued under this section.

14 (h) AVIATION SECURITY CAPITAL FUND.—

15 (1) IN GENERAL.—There is established in the Department the Avia-
16 tion Security Capital Fund. The first \$250,000,000 from fees received
17 under section 40958(a) of this title in each of fiscal years 2004
18 through 2028 is available to be deposited in the Fund. The Adminis-
19 trator shall impose the fee authorized by section 40958(a) so as to col-
20 lect at least \$250,000,000 in each of the fiscal years for deposit into
21 the Fund. Amounts in the Fund are available to the Administrator to
22 make grants under this section.

23 (2) ALLOCATION.—Of the amount made available under paragraph
24 (1) for a fiscal year, not less than \$200,000,000 shall be allocated to
25 fulfill letters of intent issued under subsection (d).

26 (3) DISCRETIONARY GRANTS.—Of the amount made available under
27 paragraph (1) for a fiscal year, up to \$50,000,000 shall be used to
28 make discretionary grants, including other transaction agreements for
29 airport security improvement projects, with priority given to small hub
30 airports and nonhub airports.

31 (i) LEVERAGED FUNDING.—For purposes of this section, a grant under
32 subsection (b) to an airport sponsor to service an obligation issued by or
33 on behalf of that sponsor to fund a project described in subsection (b) is
34 considered to be a grant for that project.

35 **§ 40933. Repair station security**

36 (a) SECURITY REVIEW AND AUDIT.—To ensure the security of mainte-
37 nance and repair work conducted on air carrier aircraft and components at
38 foreign repair stations, the Administrator, in consultation with the Adminis-
39 trator of the Federal Aviation Administration, shall complete a security re-
40 view and audit of foreign repair stations that are certified by the Adminis-
41 trator of the Federal Aviation Administration under part 145 of title 14,

1 Code of Federal Regulations, and that work on air carrier aircraft and com-
2 ponents. The review shall be completed no later than 6 months after the
3 date on which the Administrator issues regulations under subsection (f).

4 (b) ADDRESSING SECURITY CONCERNS.—The Administrator shall require
5 a foreign repair station to address the security issues and vulnerabilities
6 identified in a security audit conducted under subsection (a) within 90 days
7 of providing notice to the repair station of the security issues and
8 vulnerabilities so identified and shall notify the Administrator of the Federal
9 Aviation Administration that a deficiency was identified in the security
10 audit.

11 (c) SUSPENSIONS AND REVOCATIONS OF CERTIFICATES.—

12 (1) FAILURE TO CARRY OUT EFFECTIVE SECURITY MEASURES.—If,
13 after the 90th day on which a notice is provided to a foreign repair
14 station under subsection (b), the Administrator determines that the
15 foreign repair station does not maintain and carry out effective security
16 measures, the Administrator shall notify the Administrator of the Fed-
17 eral Aviation Administration of the determination. On receipt of the de-
18 termination, the Administrator of the Federal Aviation Administration
19 shall suspend the certification of the repair station until the Adminis-
20 trator determines that the repair station maintains and carries out ef-
21 fective security measures and transmits the determination to the Ad-
22 ministrator of the Federal Aviation Administration.

23 (2) IMMEDIATE SECURITY RISK.—If the Administrator determines
24 that a foreign repair station poses an immediate security risk, the Ad-
25 ministrator shall notify the Administrator of the Federal Aviation Ad-
26 ministration of the determination. On receipt of the determination, the
27 Administrator of the Federal Aviation Administration shall revoke the
28 certification of the repair station.

29 (3) PROCEDURES FOR APPEALS.—The Administrator, in consultation
30 with the Administrator of the Federal Aviation Administration, shall
31 establish procedures for appealing a revocation of a certificate under
32 this subsection.

33 (d) FAILURE TO MEET AUDIT DEADLINE.—If the security audits re-
34 quired by subsection (a) are not completed on or before the date that is
35 6 months after the date on which the Administrator issues regulations
36 under subsection (f), the Administrator of the Federal Aviation Administra-
37 tion shall be barred from certifying a foreign repair station (other than a
38 station that was previously certified, or is in the process of certification, by
39 the Administrator of the Federal Aviation Administration under part A of
40 subtitle VII of title 49) until the audits are completed for existing stations.

1 (e) PRIORITY FOR AUDITS.—In conducting the audits described in sub-
 2 section (a), the Administrator and the Administrator of the Federal Avia-
 3 tion Administration shall give priority to foreign repair stations located in
 4 countries identified by the Government as posing the most significant secu-
 5 rity risks.

6 (f) REGULATIONS.—The Administrator, in consultation with the Adminis-
 7 trator of the Federal Aviation Administration, shall issue final regulations
 8 to ensure the security of foreign and domestic aircraft repair stations.

9 **§ 40934. Deployment and use of detection equipment at air-**
 10 **port screening checkpoints**

11 (a) WEAPONS AND EXPLOSIVES.—The Secretary shall give a high priority
 12 to developing, testing, improving, and deploying, at airport screening check-
 13 points, equipment that detects nonmetallic, chemical, biological, and radio-
 14 logical weapons, and explosives, in all forms, on individuals and in their per-
 15 sonal property. The Secretary shall ensure that the equipment alone, or as
 16 part of an integrated system, can detect under realistic operating conditions
 17 the types of weapons and explosives that terrorists would likely try to smug-
 18 gle aboard an air carrier aircraft.

19 (b) STRATEGIC PLAN FOR DEPLOYMENT AND USE OF EXPLOSIVE DE-
 20TECTION EQUIPMENT AT AIRPORT SCREENING CHECKPOINTS.—

21 (1) IN GENERAL.—The Administrator shall submit to the appro-
 22 priate congressional committees a strategic plan to promote the optimal
 23 utilization and deployment of explosive detection equipment at airports
 24 to screen individuals and their personal property. Such equipment in-
 25 cludes walk-through explosive detection portals, document scanners,
 26 shoe scanners, and backscatter x-ray scanners. The plan may be sub-
 27 mitted in a classified format.

28 (2) CONTENT.—The strategic plan shall include, at minimum—

29 (A) a description of current efforts to detect explosives in all
 30 forms on individuals and in their personal property;

31 (B) a description of the operational applications of explosive de-
 32 tection equipment at airport screening checkpoints;

33 (C) a deployment schedule and a description of the quantities
 34 of equipment needed to implement the plan;

35 (D) a description of funding needs to implement the plan, in-
 36 cluding a financing plan that provides for leveraging of non-Fed-
 37 eral funding;

38 (E) a description of the measures taken and anticipated to be
 39 taken in carrying out subsection (d); and

40 (F) a description of any recommended legislative actions.

1 (c) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be ap-
2 propriated to the Secretary for the use of the Transportation Security Ad-
3 ministration \$250,000,000, in addition to amounts otherwise authorized by
4 law, for research, development, and installation of detection systems and
5 other devices for the detection of biological, chemical, radiological, and ex-
6 plosive materials.

7 (d) INTERIM ACTION.—Until measures are implemented that enable the
8 screening of all passengers for explosives, the Administrator shall provide,
9 by means the Administrator considers appropriate, explosives detection
10 screening for all passengers identified for additional screening and their per-
11 sonal property that will be carried aboard a passenger aircraft operated by
12 an air carrier or foreign air carrier in air transportation or intrastate air
13 transportation.

14 **§ 40935. Appeal and redress process for passengers wrongly**
15 **delayed or prohibited from boarding a flight**

16 (a) IN GENERAL.—The Secretary shall establish a timely and fair process
17 for individuals who believe they have been delayed or prohibited from board-
18 ing a commercial aircraft because they were wrongly identified as a threat
19 under the regimes utilized by the Transportation Security Administration,
20 U.S. Customs and Border Protection, or another office or component of the
21 Department.

22 (b) OFFICE OF APPEALS AND REDRESS.—

23 (1) ESTABLISHMENT.—The Secretary shall establish in the Depart-
24 ment an Office of Appeals and Redress to implement, coordinate, and
25 execute the process established by the Secretary under subsection (a).
26 The Office shall include representatives from the Transportation Secu-
27 rity Administration, U.S. Customs and Border Protection, and other
28 offices and components of the Department that the Secretary deter-
29 mines appropriate.

30 (2) RECORDS.—The process established by the Secretary under sub-
31 section (a) shall include the establishment of a method by which the
32 Office, under the direction of the Secretary, will be able to maintain
33 a record of air carrier passengers and other individuals who have been
34 misidentified and have corrected erroneous information.

35 (3) INFORMATION.—To prevent repeated delays of a misidentified
36 passenger or other individual, the Office of Appeals and Redress
37 shall—

38 (A) ensure that the records maintained under this subsection
39 contain information determined by the Secretary to authenticate
40 the identity of the passenger or individual;

1 (B) furnish to the Transportation Security Administration, U.S.
2 Customs and Border Protection, or another appropriate office or
3 component of the Department, on request, information necessary
4 to allow the office or component to assist air carriers in improving
5 their administration of the advanced passenger prescreening sys-
6 tem and reduce the number of false positives; and

7 (C) require that air carriers and foreign air carriers take action
8 to identify passengers determined, under the process established
9 under subsection (a), to have been wrongly identified.

10 (4) HANDLING OF PERSONALLY IDENTIFIABLE INFORMATION.—The
11 Secretary, in conjunction with the Chief Privacy Officer of the Depart-
12 ment, shall—

13 (A) require that Federal employees of the Department handling
14 personally identifiable information of passengers (in this para-
15 graph referred to as “PII”) complete mandatory privacy and secu-
16 rity training prior to being authorized to handle PII;

17 (B) ensure that the records maintained under this subsection
18 are secured by encryption, one-way hashing, other data
19 anonymization techniques, or other, equivalent security technical
20 protections the Secretary determines necessary;

21 (C) limit the information collected from misidentified passengers
22 or other individuals to the minimum amount necessary to resolve
23 a redress request;

24 (D) require that the data generated under this subsection shall
25 be shared or transferred via a secure data network, that has been
26 audited to ensure that the anti-hacking and other security related
27 software functions properly and is updated as necessary;

28 (E) ensure that an employee of the Department receiving the
29 data contained in the records handles the information under sec-
30 tion 552a of title 5 and the Federal Information Security Manage-
31 ment Act of 2002 (Public Law 107–296, 116 Stat. 2259);

32 (F) only retain the data for as long as needed to assist the indi-
33 vidual traveler in the redress process; and

34 (G) conduct and publish a privacy impact assessment of the
35 process described within this subsection and transmit the assess-
36 ment to the Committee on Homeland Security of the House of
37 Representatives, the Committee on Commerce, Science, and
38 Transportation of the Senate, and the Committee on Homeland
39 Security and Governmental Affairs of the Senate.

40 (5) INITIATION OF REDRESS PROCESS AT AIRPORTS.—The Office of
41 Appeals and Redress shall establish at each airport at which the De-

1 partment has a significant presence a process to provide information
2 to air carrier passengers to begin the redress process established under
3 subsection (a).

4 **§ 40936. Expedited screening for severely injured or dis-**
5 **abled members of the armed forces and severely**
6 **injured or disabled veterans**

7 (a) PASSENGER SCREENING.—The Administrator, in consultation with
8 the Secretary of Defense, the Secretary of Veterans Affairs, and organiza-
9 tions identified by the Secretaries of Defense and Veterans Affairs that ad-
10 vocate on behalf of severely injured or disabled members of the armed forces
11 and severely injured or disabled veterans, shall develop and implement a
12 process to support and facilitate the ease of travel and to the extent possible
13 provide expedited passenger screening services through passenger screening
14 for severely injured or disabled members of the armed forces and severely
15 injured or disabled veterans. The process shall be designed to offer the indi-
16 vidual private screening to the maximum extent practicable.

17 (b) OPERATIONS CENTER.—As part of the process under subsection (a),
18 the Administrator shall maintain an operations center to provide support
19 and facilitate the movement of severely injured or disabled members of the
20 armed forces and severely injured or disabled veterans through passenger
21 screening prior to boarding a passenger aircraft operated by an air carrier
22 or foreign air carrier in air transportation or intrastate air transportation.

23 (c) PROTOCOLS.—The Administrator shall—

24 (1) establish and publish protocols, in consultation with the Sec-
25 retary of Defense, the Secretary of Veterans Affairs, and the organiza-
26 tions identified under subsection (a), under which a severely injured or
27 disabled member of the armed forces or severely injured or disabled
28 veteran, or the family member or other representative of the member
29 or veteran, may contact the operations center maintained under sub-
30 section (b) and request the expedited passenger screening services de-
31 scribed in subsection (a) for that member or veteran; and

32 (2) on receipt of a request under paragraph (1), require the oper-
33 ations center to notify the appropriate Federal Security Director of the
34 request for expedited passenger screening services, as described in sub-
35 section (a), for that member or veteran.

36 (d) TRAINING.—The Administrator shall integrate training on the proto-
37 cols established under subsection (c) into the training provided to all em-
38 ployees who will regularly provide the passenger screening services described
39 in subsection (a).

40 (e) RULE OF CONSTRUCTION.—Nothing in this section shall affect the
41 authority of the Administrator to require additional screening of a severely

1 injured or disabled member of the armed forces, a severely injured or dis-
 2 abled veteran, or their accompanying family members or nonmedical attend-
 3 ants, if intelligence, law enforcement, or other information indicates that ad-
 4 ditional screening is necessary.

5 (f) REPORT.—The Administrator, not later than August 9 of each year,
 6 shall submit to Congress a report on the implementation of this section.
 7 Each report shall include each of the following:

8 (1) Information on the training provided under subsection (d).

9 (2) Information on the consultations between the Administrator and
 10 the organizations identified under subsection (a).

11 (3) The number of people who accessed the operations center during
 12 the period covered by the report.

13 (4) Other information the Administrator determines is appropriate.

14 **§ 40937. Honor Flight program**

15 The Administrator shall establish, in collaboration with the Honor Flight
 16 Network or other not-for-profit organization that honors veterans, a process
 17 for providing expedited and dignified passenger screening services for vet-
 18 erans traveling on an Honor Flight Network private charter, or another not-
 19 for-profit organization that honors veterans, to visit war memorials built
 20 and dedicated to honor the service of those veterans.

21 **Subchapter III—Administration and** 22 **Personnel**

23 **§ 40951. Federal Security Managers**

24 (a) ESTABLISHMENT, DESIGNATION, AND STATIONING.—The Adminis-
 25 trator shall establish the position of Federal Security Manager at each air-
 26 port in the United States described in section 40913(e) of this title. The
 27 Administrator shall designate individuals as Managers for, and station those
 28 Managers at, those airports.

29 (b) DUTIES AND POWERS.—The Federal Security Manager at each air-
 30 port shall—

31 (1) oversee the screening of passengers and property at the airport;

32 and

33 (2) carry out other duties prescribed by the Administrator.

34 **§ 40952. Foreign Security Liaison Officers**

35 (a) ESTABLISHMENT, DESIGNATION, AND STATIONING.—The Adminis-
 36 trator shall establish the position of Foreign Security Liaison Officer for
 37 each airport outside the United States at which the Administrator decides
 38 an Officer is necessary for air transportation security. In coordination with
 39 the Secretary of State, the Administrator shall designate an Officer for each
 40 of those airports. In coordination with the Secretary of State, the Adminis-
 41 trator shall designate an Officer for each of those airports where extraor-

1 dinary security measures are in place. The Secretary of State shall give high
2 priority to stationing those Officers.

3 (b) DUTIES AND POWERS.—Each Federal Security Liaison Officer re-
4 ports directly to the Administrator. The Officer at each airport shall—

5 (1) serve as the liaison of the Administrator to foreign security au-
6 thorities (including governments of foreign countries and foreign air-
7 port authorities) in carrying out United States Government security re-
8 quirements at that airport; and

9 (2) to the extent practicable, carry out duties and powers referred
10 to in section 40951(b) of this title.

11 (c) COORDINATION OF ACTIVITIES.—The activities of each Foreign Secu-
12 rity Liaison Officer shall be coordinated with the chief of the diplomatic
13 mission of the United States to which the Officer is assigned. Activities of
14 an Officer under this section shall be consistent with the duties and powers
15 of the Secretary of State and the chief of mission to a foreign country under
16 section 103 of the Omnibus Diplomatic Security and Antiterrorism Act of
17 1986 (22 U.S.C. 4802) and section 207 of the Foreign Service Act of 1980
18 (22 U.S.C. 3927).

19 **§ 40953. Employment standards and training**

20 (a) EMPLOYMENT STANDARDS.—The Administrator shall prescribe stand-
21 ards for the employment and continued employment of, and contracting for,
22 air carrier personnel and, as appropriate, airport security personnel. The
23 standards shall include—

24 (1) minimum training requirements for new employees;

25 (2) retraining requirements;

26 (3) minimum staffing levels;

27 (4) minimum language skills; and

28 (5) minimum education levels for employees, when appropriate.

29 (b) REVIEW AND RECOMMENDATIONS.—In coordination with air carriers,
30 airport operators, and other interested persons, the Administrator shall re-
31 view issues related to human performance in the aviation security system
32 to maximize that performance. When the review is completed, the Adminis-
33 trator shall recommend guidelines and prescribe appropriate changes in ex-
34 isting procedures to improve that performance.

35 (c) SECURITY PROGRAM TRAINING, STANDARDS, AND QUALIFICA-
36 TIONS.—

37 (1) IN GENERAL.—The Administrator—

38 (A) may train individuals employed to carry out a security pro-
39 gram under section 40913(c) of this title; and

40 (B) shall prescribe uniform training standards and uniform
41 minimum qualifications for individuals eligible for that training.

1 (2) REIMBURSEMENTS.—The Administrator may authorize reim-
2 bursement for travel, transportation, and subsistence expenses for secu-
3 rity training of non-United States Government domestic and foreign in-
4 dividuals whose services will contribute significantly to carrying out
5 civil aviation security programs. To the extent practicable, air travel re-
6 imbursed under this paragraph shall be on air carriers.

7 (d) EDUCATION AND TRAINING STANDARDS FOR SECURITY COORDINA-
8 TORS, SUPERVISORY PERSONNEL, AND PILOTS.—

9 (1) IN GENERAL.—The Administrator shall prescribe standards for
10 educating and training—

- 11 (A) ground security coordinators;
12 (B) security supervisory personnel; and
13 (C) airline pilots as in-flight security coordinators.

14 (2) ELEMENTS.—The standards shall include initial training, re-
15 training, and continuing education requirements and methods. The re-
16 quirements and methods shall be used annually to measure the per-
17 formance of ground security coordinators and security supervisory per-
18 sonnel.

19 (e) SECURITY SCREENERERS.—

20 (1) TRAINING PROGRAM.—The Administrator shall establish a pro-
21 gram for the hiring and training of security screening personnel.

22 (2) HIRING.—

23 (A) QUALIFICATIONS.—The Administrator shall establish quali-
24 fication standards for individuals to be hired by the United States
25 as security screening personnel. The standards shall require, at a
26 minimum, an individual—

27 (i) to have a satisfactory or better score on a Federal secu-
28 rity screening personnel selection examination;

29 (ii) to be a citizen of the United States or a national of
30 the United States, as defined in section 101(a) of the Immi-
31 gration and Nationality Act (8 U.S.C. 1101(a));

32 (iii) to meet, at a minimum, the requirements set forth in
33 subsection (f);

34 (iv) to meet other qualifications the Administrator may es-
35 tablish; and

36 (v) to have the ability to demonstrate daily a fitness for
37 duty without an impairment due to illegal drugs, sleep depri-
38 vation, medication, or alcohol.

39 (B) BACKGROUND CHECKS.—The Administrator shall require
40 that an individual to be hired as a security screener undergo an

1 employment investigation (including a criminal history record
2 check) under section 40954(a)(1) of this title.

3 (C) DISQUALIFICATION OF INDIVIDUALS WHO PRESENT NA-
4 TIONAL SECURITY RISKS.—The Administrator, in consultation
5 with the heads of other appropriate Federal agencies, shall estab-
6 lish procedures, in addition to any background check conducted
7 under section 40954, to ensure that an individual who presents a
8 threat to national security is not employed as a security screener.

9 (3) EXAMINATION.—The Administrator shall develop a security
10 screening personnel examination for use in determining the qualifica-
11 tion of individuals seeking employment as security screening personnel.

12 (4) REVIEW OF STANDARDS, RULES, AND REGULATIONS.—The Ad-
13 ministrator shall review, and revise as necessary, a standard, rule, or
14 regulation governing the employment of individuals as security screen-
15 ing personnel.

16 (f) EMPLOYMENT STANDARDS FOR SCREENING PERSONNEL.—

17 (1) SCREENER REQUIREMENTS.—An individual may not be deployed
18 as a security screener unless that individual meets the following re-
19 quirements:

20 (A) EDUCATION OR EXPERIENCE.—The individual possesses a
21 high school diploma, a general equivalency diploma, or experience
22 that the Administrator has determined to be sufficient for the in-
23 dividual to perform the duties of the position.

24 (B) BASIC APTITUDES AND PHYSICAL ABILITIES.—The indi-
25 vidual possesses basic aptitudes and physical abilities, including
26 color perception, visual and aural acuity, physical coordination,
27 and motor skills, to the following standards:

28 (i) Screeners operating screening equipment are able to dis-
29 tinguish on the screening equipment monitor the appropriate
30 imaging standard specified by the Administrator.

31 (ii) Screeners operating screening equipment are able to
32 distinguish each color displayed on every type of screening
33 equipment and explain what each color signifies.

34 (iii) Screeners are able to hear and respond to the spoken
35 voice and to audible alarms generated by screening equipment
36 in an active checkpoint environment.

37 (iv) Screeners performing physical searches or other related
38 operations are able to efficiently and thoroughly manipulate
39 and handle the baggage, containers, and other objects subject
40 to security processing.

1 (v) Screeners performing pat-downs or hand-held metal de-
2 tector searches of individuals have sufficient dexterity and ca-
3 pability to thoroughly conduct those procedures over an indi-
4 vidual's entire body.

5 (C) READ, WRITE, AND SPEAK ENGLISH.—The individual is able
6 to read, speak, and write English well enough to—

7 (i) carry out written and oral instructions regarding the
8 proper performance of screening duties;

9 (ii) read English language identification media, credentials,
10 airline tickets, and labels on items normally encountered in
11 the screening process;

12 (iii) provide direction to and understand and answer ques-
13 tions from English-speaking individuals undergoing screening;
14 and

15 (iv) write incident reports and statements and log entries
16 into security records in the English language.

17 (D) TRAINING.—The individual has satisfactorily completed all
18 initial, recurrent, and appropriate specialized training required by
19 the security program, except as provided in paragraph (3).

20 (2) VETERANS PREFERENCE.—The Administrator shall provide a
21 preference for the hiring of an individual as a security screener if the
22 individual is a member or former member of the armed forces and if
23 the individual is entitled, under statute, to retired, retirement, or re-
24 tainer pay on account of service as a member of the armed forces.

25 (3) EXCEPTIONS.—An individual who has not completed the training
26 required by this section may be deployed during the on-the-job portion
27 of training to perform functions if that individual—

28 (A) is closely supervised; and

29 (B) does not make independent judgments as to whether indi-
30 viduals or property may enter a sterile area or aircraft without
31 further inspection.

32 (4) REMEDIAL TRAINING.—No individual employed as a security
33 screener may perform a screening function after that individual has
34 failed an operational test related to that function until that individual
35 has successfully completed the remedial training specified in the secu-
36 rity program.

37 (5) ANNUAL PROFICIENCY REVIEW.—The Administrator shall pro-
38 vide that an annual evaluation of each individual assigned screening
39 duties is conducted and documented. An individual employed as a secu-
40 rity screener may not continue to be employed in that capacity unless
41 the evaluation demonstrates that the individual—

1 (A) continues to meet all qualifications and standards required
2 to perform a screening function;

3 (B) has a satisfactory record of performance and attention to
4 duty based on the standards and requirements in the security pro-
5 gram; and

6 (C) demonstrates the current knowledge and skills necessary to
7 courteously, vigilantly, and effectively perform screening functions.

8 (6) OPERATIONAL TESTING.—In addition to the annual proficiency
9 review conducted under paragraph (5), the Administrator shall provide
10 for the operational testing of personnel.

11 (g) TRAINING.—

12 (1) USE OF OTHER AGENCIES.—The Administrator may enter into
13 a memorandum of understanding or other arrangement with another
14 Federal agency or department with appropriate law enforcement re-
15 sponsibilities, to provide personnel, resources, or other forms of assist-
16 ance in the training of security screening personnel.

17 (2) TRAINING PLAN.—The Administrator shall develop a plan for the
18 training of security screening personnel. The plan shall require, at a
19 minimum, that a security screener—

20 (A) has completed 40 hours of classroom instruction or success-
21 fully completed a program that the Administrator determines will
22 train individuals to a level of proficiency equivalent to the level
23 that would be achieved by the classroom instruction;

24 (B) has completed 60 hours of on-the-job instructions; and

25 (C) has successfully completed an on-the-job training examina-
26 tion prescribed by the Administrator.

27 (3) EQUIPMENT-SPECIFIC TRAINING.—An individual employed as a
28 security screener may not use a security screening device or equipment
29 in the scope of that individual's employment unless the individual has
30 been trained on that device or equipment and has successfully com-
31 pleted a test on the use of the device or equipment.

32 (h) TECHNOLOGICAL TRAINING.—

33 (1) DEFINITION OF DUAL-USE ITEM.—In this subsection, the term
34 “dual-use item” means an item that may seem harmless but that may
35 be used as a weapon.

36 (2) IN GENERAL.—The Administrator shall require training to en-
37 sure that screeners are proficient in using the most up-to-date new
38 technology and to ensure their proficiency in recognizing new threats
39 and weapons.

1 (3) PERIODIC ASSESSMENTS.—The Administrator shall make peri-
 2 odic assessments to determine if there are dual-use items and inform
 3 security screening personnel of the existence of the items.

4 (4) CURRENT LISTS OF DUAL-USE ITEMS.—Current lists of dual-use
 5 items shall be part of the ongoing training for screeners.

6 (i) LIMITATION ON RIGHT TO STRIKE.—An individual who screens pas-
 7 sengers or property, or both, at an airport under this section may not par-
 8 ticipate in a strike, or assert the right to strike, against the person (includ-
 9 ing a governmental entity) employing the individual to perform the screen-
 10 ing.

11 (j) UNIFORMS.—The Administrator shall require an individual who
 12 screens passengers and property under section 40911 of this title to be at-
 13 tired while on duty in a uniform approved by the Administrator.

14 (k) ACCESSIBILITY OF COMPUTER-BASED TRAINING FACILITIES.—The
 15 Administrator shall work with air carriers and airports to ensure that com-
 16 puter-based training facilities intended for use by security screeners at an
 17 airport regularly serving an air carrier holding a certificate issued by the
 18 Secretary of Transportation are conveniently located for that airport and
 19 easily accessible.

20 (l) SCREENER PERSONNEL.—

21 (1) IMPROVING JOB PERFORMANCE.—The Administrator shall take
 22 such actions as may be necessary to improve the job performance of
 23 airport screening personnel.

24 (2) AUTHORITY OF ADMINISTRATOR.—

25 (A) IN GENERAL.—Except as provided in subparagraph (B), the
 26 Administrator may employ, appoint, discipline, terminate, and fix
 27 the compensation, terms, and conditions of employment of Federal
 28 service for the number of individuals the Administrator determines
 29 to be necessary to carry out the screening functions of the Admin-
 30 istrator under section 40911 of this title. The Administrator shall
 31 establish levels of compensation and other benefits for the individ-
 32 uals employed.

33 (B) UNIFORMED SERVICES EMPLOYMENT AND REEMPLOYMENT
 34 RIGHTS.—In carrying out the functions authorized under subpara-
 35 graph (A), the Administrator is subject to the provisions set forth
 36 in chapter 43 of title 38.

37 **§ 40954. Employment investigations and restrictions**

38 (a) EMPLOYMENT INVESTIGATION REQUIREMENT.—

39 (1) IN GENERAL.—

40 (A) EMPLOYEE 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, shall be conducted of each individual employed in, or apply-
5 ing for, a position as a security screener under section 40953(e)
6 of this title or a position in which the individual has unescorted
7 access, or may permit other individuals to have unescorted access,
8 to—

9 (i) aircraft of an air carrier or foreign air carrier; or

10 (ii) a secured area of an airport in the United States the
11 Administrator designates that serves an air carrier or foreign
12 air carrier.

13 (B) FURTHER COVERAGE.—The Administrator shall require by
14 regulation that an employment investigation (including a criminal
15 history record check and a review of available law enforcement
16 data bases and records of other governmental and international
17 agencies, to the extent determined practicable by the Adminis-
18 trator) be conducted for—

19 (i) individuals who are responsible for screening passengers
20 or property under section 40911 of this title;

21 (ii) supervisors of the individuals described in clause (i);

22 (iii) individuals who regularly have escorted access to air-
23 craft of an air carrier or foreign air carrier or a secured area
24 of an airport in the United States the Administrator des-
25 ignates that serves an air carrier or foreign air carrier; and

26 (iv) other individuals who exercise security functions associ-
27 ated with baggage or cargo that the Administrator determines
28 is necessary to ensure air transportation security.

29 (C) EXEMPTION.—An employment investigation, including a
30 criminal history record check, is not required under this subsection
31 for an individual who is exempted under section 107.31(m)(1) or
32 (2) of title 14, Code of Federal Regulations, as in effect on No-
33 vember 22, 2000. The Administrator shall work with the Inter-
34 national Civil Aviation Organization and with appropriate authori-
35 ties of foreign countries to ensure that individuals exempted under
36 this subparagraph do not pose a threat to aviation or national se-
37 curity.

38 (2) EMPLOYER ROLE.—An air carrier, foreign air carrier, airport op-
39 erator, or government that employs, or authorizes or makes a contract
40 for the services of, an individual in a position described in paragraph

1 (1) shall ensure that the investigation the Administrator requires is
2 conducted.

3 (3) PERIODIC AUDITS.—The Administrator shall provide for the peri-
4 odic audit of the effectiveness of criminal history record checks con-
5 ducted under paragraph (1).

6 (b) PROHIBITED EMPLOYMENT.—

7 (1) IN GENERAL.—Except as provided in paragraph (3), an air car-
8 rier, foreign air carrier, airport operator, or government may not em-
9 ploy, or authorize or make a contract for the services of, an individual
10 in a position described in subsection (a)(1) if—

11 (A) the investigation of the individual required under this sec-
12 tion has not been conducted; or

13 (B) the results of that investigation establish that, in the 10-
14 year period ending on the date of the investigation, the individual
15 was convicted (or found not guilty by reason of insanity) of—

16 (i) a crime referred to in section 32 or 2744 or chapter 127
17 of title 18 or section 46306, 46308, 46312, or 46315 of title
18 49;

19 (ii) murder;

20 (iii) assault with intent to murder;

21 (iv) espionage;

22 (v) sedition;

23 (vi) treason;

24 (vii) rape;

25 (viii) kidnapping;

26 (ix) unlawful possession, sale, distribution, or manufacture
27 of an explosive or weapon;

28 (x) extortion;

29 (xi) armed or felony unarmed robbery;

30 (xii) distribution of, or intent to distribute, a controlled
31 substance;

32 (xiii) a felony involving a threat;

33 (xiv) a felony involving—

34 (I) willful destruction of property;

35 (II) importation or manufacture of a controlled sub-
36 stance;

37 (III) burglary;

38 (IV) theft;

39 (V) dishonesty, fraud, or misrepresentation;

40 (VI) possession or distribution of stolen property;

41 (VII) aggravated assault;

1 (VIII) bribery; and

2 (IX) illegal possession of a controlled substance pun-
3 ishable by a maximum term of imprisonment of more
4 than 1 year, or another crime classified as a felony that
5 the Administrator determines indicates a propensity for
6 placing contraband aboard an aircraft in return for
7 money; or

8 (xv) conspiracy to commit any of the acts referred to in
9 clauses (i) through (xiv).

10 (2) OTHER FACTORS.—The Administrator may specify other factors
11 that are sufficient to prohibit the employment of an individual in a po-
12 sition described in subsection (a)(1).

13 (3) ALTERNATE SECURITY ARRANGEMENTS.—An air carrier, foreign
14 air carrier, airport operator, or government may employ, or authorize
15 or contract for the services of, an individual in a position described in
16 subsection (a)(1) without carrying out the investigation required under
17 this section, if the Administrator approves a plan to employ the indi-
18 vidual that provides alternate security arrangements.

19 (c) FINGERPRINTING AND RECORD CHECK INFORMATION.—

20 (1) IN GENERAL.—If the Administrator requires an identification
21 and criminal history record check, to be conducted by the Attorney
22 General, as part of an investigation under this section, the Adminis-
23 trator shall designate an individual to obtain fingerprints and submit
24 those fingerprints to the Attorney General. The Attorney General may
25 make the results of a check available to an individual the Administrator
26 designates. Before designating an individual to obtain and submit fin-
27 gerprints or receive results of a check, the Administrator shall consult
28 with the Attorney General. All Federal agencies shall cooperate with
29 the Administrator and the Administrator's designee in the process of
30 collecting and submitting fingerprints.

31 (2) REGULATIONS.—The Administrator shall prescribe regulations
32 on—

33 (A) procedures for taking fingerprints; and

34 (B) requirements for using information received from the Attor-
35 ney General under paragraph (1)—

36 (i) to limit the dissemination of the information; and

37 (ii) to ensure that the information is used only to carry out
38 this section.

39 (3) ACCESS TO INVESTIGATION.—If an identification and criminal
40 history record check is conducted as part of an investigation of an indi-
41 vidual under this section, the individual—

1 (A) shall receive a copy of a record received from the Attorney
2 General; and

3 (B) may complete and correct the information contained in the
4 check before a final employment decision is made based on the
5 check.

6 (d) FEES AND CHARGES.—The Administrator and the Attorney General
7 shall establish reasonable fees and charges to pay expenses incurred in car-
8 rying out this section. The employer of the individual being investigated
9 shall pay the costs of a record check of the individual. Money collected
10 under this section shall be credited to the account in the Treasury from
11 which the expenses were incurred and are available to the Administrator
12 and the Attorney General for those expenses.

13 (e) WHEN INVESTIGATION OR RECORD CHECK NOT REQUIRED.—This
14 section does not require an investigation or record check when the investiga-
15 tion or record check is prohibited by a law of a foreign country.

16 **§ 40955. Prohibition on transferring duties and powers**

17 Except as specifically provided by law, the Administrator may not trans-
18 fer a duty or power under section 40913(a), (b), (c), or (e), 40916,
19 40922(a) through (c), 40953(a) through (k), 40954, or 40956(b)(2) of this
20 title.

21 **§ 40956. Reports**

22 (a) TRANSPORTATION SECURITY.—Not later than March 31 of each year,
23 the Secretary shall submit to Congress a report on transportation security
24 with recommendations the Secretary considers appropriate. The report shall
25 be prepared in conjunction with the biennial report the Administrator sub-
26 mits under subsection (b) in each year the Administrator submits the bien-
27 nial report, but may not duplicate the information submitted under sub-
28 section (b) or section 40917(a)(3) of this title. The Secretary may submit
29 the report in classified and unclassified parts. The report shall include—

30 (1) an assessment of trends and developments in terrorist activities,
31 methods, and other threats to transportation;

32 (2) an evaluation of deployment of explosive detection devices;

33 (3) recommendations for research, engineering, and development ac-
34 tivities related to transportation security, except research engineering
35 and development activities related to aviation security to the extent
36 those activities are covered by the national aviation research plan re-
37 quired under section 44501(e) of title 49;

38 (4) identification and evaluation of cooperative efforts with other de-
39 partments, agencies, and instrumentalities of the United States Gov-
40 ernment;

1 (5) an evaluation of cooperation with foreign transportation and se-
2 curity authorities;

3 (6) the status of the extent to which the recommendations of the
4 President's Commission on Aviation Security and Terrorism have been
5 carried out and the reasons for delay in carrying out those rec-
6 ommendations;

7 (7) an assessment of financial and staffing requirements, and attain-
8 ment of existing staffing goals, for carrying out duties and powers of
9 the Administrator relating to security; and

10 (8) appropriate legislative and regulatory recommendations.

11 (b) SCREENING AND FOREIGN AIR CARRIER AND AIRPORT SECURITY.—
12 The Administrator shall submit biennially to Congress a report on the effec-
13 tiveness of procedures under section 40911 of this title that includes—

14 (1) a summary of the assessments conducted under section
15 40917(a)(1) and (2) of this title; and

16 (2) an assessment of the steps being taken, and the progress being
17 made, in ensuring compliance with section 40916 of this title for each
18 foreign air carrier security program at airports outside the United
19 States—

20 (A) at which the Administrator decides that Foreign Security
21 Liaison Officers are necessary for air transportation security; and

22 (B) for which extraordinary security measures are in place.

23 **§ 40957. Training to operate certain aircraft**

24 (a) WAITING PERIOD.—

25 (1) DEFINITION OF TRAINING.—In this subsection, the term “train-
26 ing”—

27 (A) means training received from an instructor in an aircraft
28 or aircraft simulator; but

29 (B) does not include recurrent training, ground training, or
30 demonstration flights for marketing purposes.

31 (2) REQUIREMENTS.—A person operating as a flight instructor, pilot
32 school, or aviation training center or subject to regulation under part
33 A of subtitle VII of title 49 may provide training in the operation of
34 an aircraft having a maximum certificated takeoff weight of more than
35 12,500 pounds to an alien (as defined in section 101(a) of the Immig-
36 ration and Nationality Act (8 U.S.C. 1101(a))) or to another indi-
37 vidual specified by the Secretary only if—

38 (A) that person has first notified the Secretary that the alien
39 or individual has requested training and submitted to the Sec-
40 retary, in the form the Secretary prescribes, the following informa-
41 tion about the alien or individual:

1 (i) Full name, including aliases used by the applicant or
2 variations in spelling of the applicant's name.

3 (ii) Passport and visa information.

4 (iii) Country of citizenship.

5 (iv) Date of birth.

6 (v) Dates of training.

7 (vi) Fingerprints collected by, or under the supervision of,
8 a Federal, State, or local law enforcement agency or by an-
9 other entity approved by the Federal Bureau of Investigation
10 or the Secretary, including fingerprints taken by United
11 States Government personnel at a United States embassy or
12 consulate; and

13 (B) the Secretary has not directed, within 30 days after being
14 notified under subparagraph (A), that person not to provide the
15 requested training because the Secretary has determined that the
16 individual presents a risk to aviation or national security.

17 (b) INTERRUPTION OF TRAINING.—If the Secretary, more than 30 days
18 after receiving notification under subsection (a) from a person providing
19 training described in subsection (a), determines that the individual presents
20 a risk to aviation or national security, the Secretary shall immediately notify
21 the person providing the training of the determination, and that person
22 shall immediately terminate the training.

23 (c) NOTIFICATION.—A person operating as a flight instructor, pilot
24 school, or aviation training center or subject to regulation under part A of
25 subtitle VII of title 49 may provide training in the operation of an aircraft
26 having a maximum certificated takeoff weight of 12,500 pounds or less to
27 an alien (as defined in section 101(a) of the Immigration and Nationality
28 Act (8 U.S.C. 1101(a)) or to another individual specified by the Secretary
29 only if that person has notified the Secretary that the individual has re-
30 quested the training and furnished the Secretary with that individual's iden-
31 tification in the form the Secretary requires.

32 (d) EXPEDITED PROCESSING.—The Secretary shall establish a process to
33 ensure that the waiting period under subsection (a) shall not exceed 5 days
34 for an alien (as defined in section 101(a) of the Immigration and Nation-
35 ality Act (8 U.S.C. 1101(a))) who—

36 (1) holds an airman's certification of a foreign country that is recog-
37 nized by an agency of the United States, including a military agency,
38 that permits an individual to operate a multi-engine aircraft that has
39 a certificated takeoff weight of more than 12,500 pounds;

40 (2) is employed by a foreign air carrier that is certified under part
41 129 of title 14, Code of Federal Regulations, and that has a security

1 program approved under part 1546 of title 49, Code of Federal Regula-
2 tions;

3 (3) is an individual that has unescorted access to a secured area of
4 an airport designated under section 40954(a)(1)(A)(ii) of this title; or

5 (4) is an individual that is part of a class of individuals that the Sec-
6 retary has determined that providing aviation training to presents mini-
7 mal risk to aviation or national security because of the aviation train-
8 ing already possessed by the class of individuals.

9 (e) NONAPPLICABILITY TO CERTAIN FOREIGN MILITARY PILOTS.—The
10 procedures and processes required by subsections (a) through (d) do not
11 apply to a foreign military pilot endorsed by the Department of Defense for
12 flight training in the United States and seeking training described in sub-
13 section (a)(1) in the United States.

14 (f) FEE.—

15 (1) IN GENERAL.—The Secretary may assess a fee for an investiga-
16 tion under this section. The Secretary may adjust the maximum
17 amount of the fee to reflect the costs of an investigation.

18 (2) OFFSET.—Notwithstanding section 3302 of title 31, a fee col-
19 lected under this section—

20 (A) shall be credited to the account in the Treasury from which
21 the expenses were incurred and shall be available to the Secretary
22 for those expenses; and

23 (B) remains available until expended.

24 (g) INTERAGENCY COOPERATION.—The Attorney General, the Director of
25 National Intelligence, and the Administrator of the Federal Aviation Admin-
26 istration shall cooperate with the Secretary in implementing this section.

27 (h) SECURITY AWARENESS TRAINING FOR EMPLOYEES.—The Secretary
28 shall require flight schools to conduct a security awareness program for
29 flight school employees to increase their awareness of suspicious cir-
30 cumstances and activities of individuals enrolling in or attending flight
31 school.

32 **§ 40958. Security service fee**

33 (a) GENERAL AUTHORITY.—

34 (1) PASSENGER FEES.—The Administrator shall impose a uniform
35 fee, on passengers of air carriers and foreign air carriers in air trans-
36 portation and intrastate air transportation originating at airports in
37 the United States, to pay for the following costs of providing civil avia-
38 tion security services:

39 (A) Salary, benefits, overtime, retirement and other costs of
40 screening personnel, their supervisors and managers, Federal law
41 enforcement personnel, and State and local law enforcement offi-

1 cers deputized under section 40931 of this title, who are deployed
2 at airport security screening locations under section 40911 of this
3 title.

4 (B) The costs of training personnel described in subparagraph
5 (A), and the acquisition, operation, and maintenance of equipment
6 used by the personnel.

7 (C) The costs of performing background investigations of per-
8 sonnel described in subparagraphs (A), (D), (F), and (G).

9 (D) The costs of the Federal air marshals program.

10 (E) The costs of performing civil aviation security research and
11 development under this title.

12 (F) The costs of Federal Security Managers under section
13 40913 of this title.

14 (G) The costs of deploying Federal law enforcement personnel
15 under section 40913(h) of this title.

16 (H) The costs of security-related capital improvements at air-
17 ports.

18 (I) The costs of training pilots and flight attendants under sec-
19 tions 40928 and 40930 of this title.

20 (2) DETERMINATION OF COSTS.—The amount of costs listed in para-
21 graph (1) shall be determined by the Administrator and are not subject
22 to judicial review

23 (b) SCHEDULE OF FEES.—In imposing fees under subsection (a), the Ad-
24 ministrator shall ensure that the fees are reasonably related to the Trans-
25 portation Security Administration’s costs of providing services rendered.

26 (c) LIMITATION ON FEE.—

27 (1) DEFINITION OF ROUND TRIP.—In this subsection, “round trip”
28 means a trip on an air travel itinerary that terminates or has a stop-
29 over at the origin point (or co-terminal).

30 (2) LIMITATION.—The fee imposed under subsection (a) is \$5.60 per
31 one-way trip in air transportation or intrastate air transportation that
32 originates at an airport in the United States, except the fee imposed
33 per round trip shall not exceed \$11.20.

34 (d) IMPOSITION OF FEE.—

35 (1) IN GENERAL.—Notwithstanding section 9701 of title 31 and the
36 procedural requirements of section 553 of title 5, the Administrator
37 shall impose the fee under subsection (a) through the publication of no-
38 tice of the fee in the Federal Register and begin collection of the fee
39 as soon as possible.

40 (2) SPECIAL RULES FOR PASSENGER FEES.—A fee imposed under
41 subsection (a) through the procedures under paragraph (1) shall apply

1 only to tickets sold after the date on which the fee is imposed. If a
2 fee imposed under subsection (a) through the procedures under para-
3 graph (1) on transportation of a passenger of a carrier described in
4 subsection (a) is not collected from the passenger, the amount of the
5 fee shall be paid by the carrier.

6 (3) SUBSEQUENT MODIFICATION OF FEE.—After imposing a fee
7 under paragraph (1), the Administrator may modify, from time to time
8 through publication of notice in the Federal Register, the imposition
9 or collection of the fee, or both.

10 (4) LIMITATION ON COLLECTION.—A fee may be collected under this
11 section, other than subsection (i), only to the extent that the expendi-
12 ture of the fee to pay the costs of activities and services for which the
13 fee is imposed is provided for in advance in an appropriations Act or
14 in section 40932 of this title.

15 (e) ADMINISTRATION OF FEES.—

16 (1) FEES PAYABLE TO ADMINISTRATOR.—All fees imposed and
17 amounts collected under this section are payable to the Administrator.

18 (2) FEES COLLECTED BY AIR CARRIER.—A fee imposed under sub-
19 section (a)(1) shall be collected by the air carrier or foreign air carrier
20 that sells a ticket for transportation described in subsection (a).

21 (3) DUE DATE FOR REMITTANCE.—A fee collected under this section
22 shall be remitted on the last day of each calendar month by the carrier
23 collecting the fee. The amount to be remitted shall be for the calendar
24 month preceding the calendar month in which the remittance is made.

25 (4) INFORMATION.—The Administrator may require the provision of
26 information the Administrator decides is necessary to verify that fees
27 have been collected and remitted at the proper times and in the proper
28 amounts.

29 (5) FEE NOT SUBJECT TO TAX.—For purposes of section 4261 of
30 the Internal Revenue Code of 1986 (26 U.S.C. 4261), a fee imposed
31 under this section is not considered to be part of the amount paid for
32 taxable transportation.

33 (6) COST OF COLLECTING FEE.—No portion of the fee collected
34 under this section may be retained by the air carrier or foreign air car-
35 rier for the costs of collecting, handling, or remitting the fee, except
36 for interest accruing to the carrier after collection and before remit-
37 tance.

38 (f) RECEIPTS CREDITED AS OFFSETTING COLLECTIONS.—Notwith-
39 standing section 3302 of title 31, a fee collected under this section—

40 (1) shall be credited as offsetting collections to the account that fi-
41 nances the activities and services for which the fee is imposed;

1 (2) shall be available for expenditure only to pay the costs of activi-
2 ties and services for which the fee is imposed; and

3 (3) remains available until expended.

4 (g) REFUNDS.—The Administrator may refund a fee paid by mistake or
5 an amount paid in excess of that required.

6 (h) EXEMPTIONS.—The Administrator may exempt from the passenger
7 fee imposed under subsection (a) a passenger enplaning at an airport in the
8 United States that does not receive screening services under section 40911
9 of this title for that segment of the trip for which the passenger does not
10 receive screening.

11 (i) DEPOSIT OF RECEIPTS.—

12 (1) IN GENERAL.—Out of fees received in a fiscal year under sub-
13 section (a), after amounts are made available in the fiscal year under
14 section 40932(h), the next funds derived from the fees in the fiscal
15 year, in the amount specified for the fiscal year in paragraph (4), shall
16 be credited as offsetting receipts and deposited in the general fund of
17 the Treasury.

18 (2) FEE LEVELS.—The Secretary shall impose the fee authorized by
19 subsection (a) so as to collect in a fiscal year at least the amount speci-
20 fied in paragraph (4) for the fiscal year for making deposits under
21 paragraph (1).

22 (3) RELATIONSHIP TO OTHER PROVISIONS.—Subsections (b) and (f)
23 do not apply to amounts to be used for making deposits under this sub-
24 section.

25 (4) FISCAL YEAR AMOUNTS.—For purposes of paragraphs (1) and
26 (2), the fiscal year amounts are as follows:

27 (A) \$1,280,000,000 for fiscal year 2017.

28 (B) \$1,320,000,000 for fiscal year 2018.

29 (C) \$1,360,000,000 for fiscal year 2019.

30 (D) \$1,400,000,000 for fiscal year 2020.

31 (E) \$1,440,000,000 for fiscal year 2021.

32 (F) \$1,480,000,000 for fiscal year 2022.

33 (G) \$1,520,000,000 for fiscal year 2023.

34 (H) \$1,560,000,000 for fiscal year 2024.

35 (I) \$1,600,000,000 for fiscal year 2025.

36 **§ 40959. Immunity for reporting suspicious activities**

37 (a) IN GENERAL.—An air carrier or foreign air carrier or an employee
38 of an air carrier or foreign air carrier who makes a voluntary disclosure of
39 a suspicious transaction relevant to a possible violation of law or regulation,
40 relating to air piracy, a threat to aircraft or passenger safety, or terrorism,
41 as defined in section 3077 of title 18, to an employee or agent of the De-

1 partment, the Department of Justice, a Federal, State, or local law enforce-
 2 ment officer, or an airport or airline security officer shall not be civilly liable
 3 to any person under a law or regulation of the United States, or a constitu-
 4 tion, law, or regulation of a State or political subdivision of a State, for the
 5 disclosure.

6 (b) APPLICATION.—Subsection (a) does not apply to—

7 (1) a disclosure made with actual knowledge that the disclosure was
 8 false, inaccurate, or misleading; or

9 (2) a disclosure made with reckless disregard as to the truth or fal-
 10 sity of that disclosure.

11 **§ 40960. Performance goals and objectives**

12 (a) LONG-TERM RESULTS-BASED MANAGEMENT.—Each year, consistent
 13 with the requirements of the Government Performance and Results Act of
 14 1993 (in this section referred to as “GPRA”) (Public Law 103–62, 107
 15 Stat. 285), the Secretary and the Administrator shall agree on a perform-
 16 ance plan for the succeeding 5 years that establishes measurable goals and
 17 objectives for aviation security. The plan shall identify action steps nec-
 18 essary to achieve the goals.

19 (b) CLARIFICATION OF RESPONSIBILITIES.—In addition to meeting the
 20 requirements of GPRA, the performance plan should clarify the responsibil-
 21 ities of the Secretary, the Administrator, and any other agency or organiza-
 22 tion that may have a role in ensuring the safety and security of the civil
 23 air transportation system.

24 (c) ANNUAL PERFORMANCE REPORT.—Each year, consistent with the re-
 25 quirements of GPRA, the Administrator shall prepare and submit to Con-
 26 gress an annual report, including an evaluation of the extent to which goals
 27 and objectives were met. The report shall include the results achieved during
 28 the year relative to the goals established in the performance plan.

29 **§ 40961. Aviation Security Advisory Committee**

30 (a) DEFINITIONS.—In this section:

31 (1) ADVISORY COMMITTEE.—The term “Advisory Committee” means
 32 the aviation security advisory committee established under subsection

33 (b).

34 (2) PERIMETER SECURITY.—The term “perimeter security”—

35 (A) means procedures or systems to monitor, secure, and pre-
 36 vent unauthorized access to an airport, including its airfield and
 37 terminal; and

38 (B) includes the fence area surrounding an airport, access
 39 gates, and access controls.

40 (b) ESTABLISHMENT.—The Administrator shall establish in the Trans-
 41 portation Security Administration an aviation security advisory committee.

1 (e) DUTIES.—

2 (1) IN GENERAL.—The Administrator shall consult the Advisory
3 Committee, as appropriate, on aviation security matters, including on
4 the development, refinement, and implementation of policies, programs,
5 rulemaking, and security directives pertaining to aviation security,
6 while adhering to sensitive security guidelines.

7 (2) RECOMMENDATIONS.—

8 (A) IN GENERAL.—At the request of the Administrator, the Ad-
9 visory Committee shall develop recommendations for improvements
10 to aviation security.

11 (B) RECOMMENDATIONS OF SUBCOMMITTEES.—Recommendations
12 agreed on by the subcommittees established under this sec-
13 tion shall be approved by the Advisory Committee before trans-
14 mission to the Administrator.

15 (3) PERIODIC REPORTS.—The Advisory Committee shall periodically
16 submit to the Administrator—

17 (A) reports on matters identified by the Administrator; and

18 (B) reports on other matters identified by a majority of the
19 members of the Advisory Committee.

20 (4) ANNUAL REPORT.—The Advisory Committee shall submit to the
21 Administrator an annual report providing information on the activities,
22 findings, and recommendations of the Advisory Committee, including
23 its subcommittees, for the preceding year. Not later than 6 months
24 after the date that the Administrator receives the annual report, the
25 Administrator shall publish a public version describing the Advisory
26 Committee's activities and such related matters as would be inform-
27 ative to the public consistent with the policy of section 552(b) of title
28 5.

29 (5) FEEDBACK.—Not later than 90 days after receiving rec-
30 ommendations transmitted by the Advisory Committee under para-
31 graph (4), the Administrator shall respond in writing to the Advisory
32 Committee with feedback on each of the recommendations, an action
33 plan to implement any of the recommendations with which the Admin-
34 istrator concurs, and a justification for why any of the recommenda-
35 tions have been rejected.

36 (6) CONGRESSIONAL NOTIFICATION.—Not later than 30 days after
37 providing written feedback to the Advisory Committee under paragraph
38 (5), the Administrator shall notify the Committee on Commerce,
39 Science, and Transportation of the Senate and the Committee on
40 Homeland Security of the House of Representatives on the feedback,
41 and provide a briefing on request.

1 (7) REPORT TO CONGRESS.—Prior to briefing the Committee on
2 Commerce, Science, and Transportation of the Senate and the Com-
3 mittee on Homeland Security of the House of Representatives under
4 paragraph (6), the Administrator shall submit to the committees a re-
5 port containing information relating to the recommendations trans-
6 mitted by the Advisory Committee in accordance with paragraph (4).

7 (d) MEMBERSHIP.—

8 (1) IN GENERAL.—

9 (A) APPOINTMENT.—The Administrator shall appoint the mem-
10 bers of the Advisory Committee.

11 (B) COMPOSITION.—The Advisory Committee consists of indi-
12 viduals representing not more than 34 member organizations.
13 Each organization shall be represented by 1 individual (or the in-
14 dividual's designee).

15 (C) REPRESENTATION.—The membership of the Advisory Com-
16 mittee shall include representatives of—

- 17 (i) air carriers;
- 18 (ii) all-cargo air transportation;
- 19 (iii) indirect air carriers;
- 20 (iv) labor organizations representing air carrier employees;
- 21 (v) labor organizations representing transportation security
22 officers;
- 23 (vi) aircraft manufacturers;
- 24 (vii) airport operators;
- 25 (viii) airport construction and maintenance contractors;
- 26 (ix) labor organizations representing employees of airport
27 construction and maintenance contractors;
- 28 (x) general aviation;
- 29 (xi) privacy organizations;
- 30 (xii) the travel industry;
- 31 (xiii) airport-based businesses (including minority-owned
32 small businesses);
- 33 (xiv) businesses that conduct security screening operations
34 at airports;
- 35 (xv) aeronautical repair stations;
- 36 (xvi) passenger advocacy groups;
- 37 (xvii) the aviation security technology industry (including
38 screening technology and biometrics);
- 39 (xviii) victims of terrorist acts against aviation; and
- 40 (xix) law enforcement and security experts.

41 (2) TERM OF OFFICE.—

1 (A) IN GENERAL.—The term of each member of the Advisory
2 Committee shall be 2 years.

3 (B) REAPPOINTMENT.—A member of the Advisory Committee
4 may be reappointed.

5 (C) REMOVAL.—The Administrator may review the participation
6 of a member of the Advisory Committee and remove the member
7 for cause at any time.

8 (3) PROHIBITION ON COMPENSATION.—The members of the Advisory
9 Committee shall not receive pay, allowances, or benefits from the Gov-
10 ernment by reason of their service on the Advisory Committee.

11 (4) MEETINGS.—

12 (A) IN GENERAL.—The Administrator shall require the Advi-
13 sory Committee to meet at least semiannually and may convene
14 additional meetings as necessary.

15 (B) PUBLIC MEETINGS.—At least 1 of the meetings described
16 in subparagraph (A) shall be open to the public.

17 (C) ATTENDANCE.—The Advisory Committee shall maintain a
18 record of the individuals present at each meeting.

19 (5) MEMBER ACCESS TO SENSITIVE SECURITY INFORMATION.—Not
20 later than 60 days after the date of a member's appointment, the Ad-
21 ministrator shall determine if there is cause for the member to be re-
22 stricted from possessing sensitive security information. Without that
23 cause, and on the member voluntarily signing a non-disclosure agree-
24 ment, the member may be granted access to sensitive security informa-
25 tion that is relevant to the member's advisory duties. The member shall
26 protect the sensitive security information in accordance with part 1520
27 of title 49, Code of Federal Regulations.

28 (6) CHAIR.—A stakeholder representative on the Advisory Com-
29 mittee who is elected by the appointed membership of the Advisory
30 Committee shall chair the Advisory Committee.

31 (e) SUBCOMMITTEES.—

32 (1) MEMBERSHIP.—The Advisory Committee chairperson, in coordi-
33 nation with the Administrator, may establish in the Advisory Com-
34 mittee any subcommittee that the Administrator and Advisory Com-
35 mittee determine to be necessary. The Administrator and the Advisory
36 Committee shall create subcommittees to address aviation security
37 issues, including the following:

38 (A) The implementation of the air cargo security programs es-
39 tablished by the Transportation Security Administration to screen
40 air cargo on passenger aircraft and all-cargo aircraft in accordance
41 with established cargo screening mandates.

1 (B) General aviation facilities, general aviation aircraft, and heli-
2 copter operations at general aviation and commercial service air-
3 ports.

4 (C) Recommendations on airport perimeter security, exit lane
5 security, and technology at commercial service airports, and access
6 control issues.

7 (D) Security technology standards and requirements, including
8 their harmonization internationally, technology to screen pas-
9 sengers, passenger baggage, carry-on baggage, and cargo, and bio-
10 metric technology.

11 (2) CONSIDERATION OF RISK-BASED SECURITY.—All subcommittees
12 established by the Advisory Committee chairperson in coordination with
13 the Administrator shall consider risk-based security approaches in the
14 performance of their functions that weigh the optimum balance of costs
15 and benefits in transportation security, including for passenger screen-
16 ing, baggage screening, air cargo security policies, and general aviation
17 security matters.

18 (3) MEETINGS AND REPORTING.—Each subcommittee shall meet at
19 least quarterly and submit to the Advisory Committee for inclusion in
20 the annual report required under subsection (c)(4) information, includ-
21 ing recommendations, regarding issues in the subcommittee.

22 (4) CO-CHAIRS.—Each subcommittee shall be co-chaired by a Gov-
23 ernment official and an industry official.

24 (5) SUBJECT MATTER EXPERTS.—Each subcommittee shall include
25 subject matter experts with relevant expertise who are appointed by the
26 respective subcommittee co-chairs.

27 (f) NONAPPLICABILITY OF FACAA.—The Federal Advisory Committee Act
28 (5 U.S.C. App.) shall not apply to the Advisory Committee and its sub-
29 committees.

30 **SEC. 4. CONFORMING AMENDMENTS.**

31 (a) TITLE 5, UNITED STATES CODE.—Section 8331(3)(E)(ii) of title 5,
32 United States Code, is amended by striking “Department of Transpor-
33 tation” and inserting “Department of Homeland Security”.

34 (b) TITLE 6, UNITED STATES CODE.—Chapter 409 of title 6, United
35 States Code, as enacted by section 3, is amended as follows:

36 (1) Insert after section 40922(c)(4) the following:

37 “(d) SECURITY AND RESEARCH AND DEVELOPMENT ACTIVITIES.—

38 “(1) GENERAL REQUIREMENTS.—The Administrator shall conduct
39 research (including behavioral research) and development activities ap-
40 propriate to develop, modify, test, and evaluate a system, procedure, fa-

1 cility, or device to protect passengers and property against acts of
2 criminal violence, aircraft piracy, and terrorism, and to ensure security.

3 “(2) 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 subsection to another department, agency, or in-
6 strumentality of the United States Government.”.

7 (2) Insert after section 40961 the following:

8 **“§ 40962. General authority; indemnification**

9 “(a) GENERAL AUTHORITY.—The Administrator may take action the Ad-
10 ministrator considers necessary to carry out this chapter, including con-
11 ducting investigations, prescribing regulations, standards, and procedures,
12 and issuing orders.

13 “(b) INDEMNIFICATION.—The Administrator may indemnify an officer or
14 employee of the Transportation Security Administration against a claim or
15 judgment arising out of an act under this chapter that the Administrator
16 decides was committed within the scope of the official duties of the officer
17 or employee.

18 **“§ 40963. Withholding information**

19 “(a) OBJECTIONS TO DISCLOSURE.—

20 “(1) IN GENERAL.—A person may object to the public disclosure of
21 information—

22 “(A) in a record filed under this chapter; or

23 “(B) obtained under this chapter by the Secretary.

24 “(2) FORM OF OBJECTION; ACTION BY SECRETARY.—An objection
25 must be in writing and must state the reasons for the objection. The
26 Secretary shall order the information withheld from public disclosure
27 when the Secretary decides that disclosure of the information would—

28 “(A) prejudice the United States Government in preparing and
29 presenting its position in international negotiations; or

30 “(B) have an adverse effect on the competitive position of an
31 air carrier in foreign air transportation.

32 “(b) WITHHOLDING INFORMATION FROM CONGRESS.—This section does
33 not authorize information to be withheld from a committee of Congress au-
34 thorized to have the information.”.

35 (3) In the analysis for chapter 409, insert after the item relating to
36 40961 the following:

“40962. General authority; indemnification.

“40963. Withholding information.”.

37 (4) Insert after section 40963, as added by paragraph (2), the fol-
38 lowing:

“Subchapter IV—Investigations and Proceedings

“§ 40981. Complaints and investigations

“(a) IN GENERAL.—

“(1) FILING COMPLAINT.—A person may file a complaint in writing with the Administrator about a person violating this chapter or a requirement prescribed under this chapter. Except as provided in subsection (b), the Administrator shall investigate the complaint if a reasonable ground appears to the Administrator for the investigation.

“(2) CONDUCTING INVESTIGATION.—On the initiative of the Administrator, the Administrator may conduct an investigation, if a reasonable ground appears to the Administrator for the investigation, about—

“(A) a person violating this chapter or a requirement prescribed under this chapter; or

“(B) any question that may arise under this chapter.

“(3) DISMISSAL OF COMPLAINT.—The Administrator may dismiss a complaint without a hearing when the Administrator is of the opinion that the complaint does not state facts that warrant an investigation or action.

“(4) HEARINGS AND ORDERS.—After notice and an opportunity for a hearing and subject to section 40105(b) of title 49, the Administrator shall issue an order to compel compliance with this chapter if the Administrator finds in an investigation under this subsection that a person is violating this chapter.

“(b) COMPLAINTS AGAINST MEMBERS OF ARMED FORCES.—The Administrator shall refer a complaint against a member of the armed forces of the United States performing official duties to the Secretary of the department concerned for action. Not later than 90 days after receiving the complaint, the Secretary of that department shall inform the Administrator of the action taken on the complaint, including any corrective or disciplinary action taken.

“§ 40982. Proceedings

“(a) CONDUCTING PROCEEDINGS.—Subject to subchapter II of chapter 5 of title 5, the Administrator may conduct proceedings in a way conducive to justice and the proper dispatch of business.

“(b) APPEARANCE.—A person may appear and be heard before the Administrator in person or by an attorney.

“(c) RECORDING AND PUBLIC ACCESS.—Official action taken by the Administrator under this chapter shall be recorded. Proceedings before the Administrator shall be open to the public on the request of an interested party

1 unless the Administrator decides that secrecy is required because of national
2 defense.

3 “(d) CONFLICTS OF INTEREST.—The Administrator or an officer or em-
4 ployee of the Transportation Security Administration may not participate in
5 a proceeding referred to in subsection (a) of this section in which the indi-
6 vidual has a pecuniary interest.

7 **“§ 40983. Service of notice, process, and actions**

8 “(a) DESIGNATING AGENTS.—

9 “(1) IN GENERAL.—Each air carrier and foreign air carrier shall
10 designate an agent on whom service of notice and process in a pro-
11 ceeding before, and an action of, the Administrator, may be made.

12 “(2) FORM OF DESIGNATION; CHANGES.—The designation—

13 “(A) shall be in writing and filed with the Administrator; and

14 “(B) may be changed in the same way as originally made.

15 “(b) SERVICE.—

16 “(1) METHOD OF SERVICE.—Service may be made—

17 “(A) by personal service;

18 “(B) on a designated agent; or

19 “(C) by certified or registered mail to the person to be served
20 or the designated agent of the person.

21 “(2) DATE OF SERVICE.—The date of service made by certified or
22 registered mail is the date of mailing.

23 “(c) SERVING AGENTS.—Service on an agent designated under this sec-
24 tion shall be made at the office or usual place of residence of the agent.
25 If an air carrier or foreign air carrier does not have a designated agent,
26 service may be made by posting the notice, process, or action in the office
27 of the Administrator.

28 **“§ 40984. Evidence**

29 “(a) IN GENERAL.—In conducting a hearing or investigation under this
30 chapter, the Administrator may—

31 “(1) subpoena witnesses and records related to a matter involved in
32 the hearing or investigation from any place in the United States to the
33 designated place of the hearing or investigation;

34 “(2) administer oaths;

35 “(3) examine witnesses; and

36 “(4) receive evidence at a place in the United States the Adminis-
37 trator designates.

38 “(b) COMPLIANCE WITH SUBPENAS.—If a person disobeys a subpoena, the
39 Administrator or a party to a proceeding before the Administrator may peti-
40 tion a court of the United States to enforce the subpoena. A judicial pro-
41 ceeding to enforce a subpoena under this section may be brought in the juris-

1 diction in which the proceeding or investigation is conducted. The court may
2 punish a failure to obey an order of the court to comply with the subpoena
3 as a contempt of court.

4 “(c) DEPOSITIONS.—

5 “(1) IN GENERAL.—In a proceeding or investigation, the Adminis-
6 trator may order a person to give testimony by deposition and to
7 produce records. If a person fails to be deposed or to produce records,
8 the order may be enforced in the same way a subpoena may be enforced
9 under subsection (b) of this section.

10 “(2) TAKING OF DEPOSITION.—A deposition may be taken before an
11 individual designated by the Administrator and having the power to ad-
12 minister oaths.

13 “(3) NOTICE REQUIREMENTS.—Before taking a deposition, the party
14 or the attorney of the party proposing to take the deposition must give
15 reasonable notice in writing to the opposing party or the attorney of
16 record of that party. The notice shall state the name of the witness
17 and the time and place of taking the deposition.

18 “(4) DEPOSITION PROCESS.—The testimony of a person deposed
19 under this subsection shall be under oath. The person taking the depo-
20 sition shall prepare, or cause to be prepared, a transcript of the testi-
21 mony taken. The transcript shall be subscribed by the deponent. Each
22 deposition shall be filed promptly with the Administrator.

23 “(5) DEPOSITIONS ABROAD.—If the laws of a foreign country allow,
24 the testimony of a witness in that country may be taken by deposi-
25 tion—

26 “(A) by a consular officer or an individual commissioned by the
27 Administrator or agreed on by the parties by written stipulation
28 filed with the Administrator; or

29 “(B) under letters rogatory issued by a court of competent ju-
30 risdiction at the request of the Administrator.

31 “(d) WITNESS FEES AND MILEAGE AND CERTAIN FOREIGN COUNTRY
32 EXPENSES.—A witness summoned before the Administrator or whose depo-
33 sition is taken under this section and the individual taking the deposition
34 are each entitled to the same fee and mileage that the witness and indi-
35 vidual would have been paid for those services in a court of the United
36 States. Under regulations of the Administrator, the Administrator shall pay
37 the necessary expenses incident to executing, in another country, a commis-
38 sion or letter rogatory issued at the initiative of the Administrator.

39 “(e) DESIGNATING EMPLOYEES TO CONDUCT HEARINGS.—When des-
40 ignated by the Administrator, an employee appointed under section 3105 of
41 title 5 may conduct a hearing, subpoena witnesses, administer oaths, examine

1 witnesses, and receive evidence at a place in the United States the Adminis-
2 trator designates. On request of a party, the Administrator shall hear or
3 receive argument.

4 **“§ 40985. Regulations and orders**

5 “(a) EFFECTIVENESS OF ORDERS.—Except as provided in this chapter,
6 a regulation prescribed or order issued by the Administrator takes effect
7 within a reasonable time prescribed by the Administrator. The regulation or
8 order remains in effect under its own terms or until superseded. Except as
9 provided in this chapter, the Administrator may amend, modify, or suspend
10 an order in the way, and by giving the notice, that the Administrator de-
11 cides.

12 “(b) CONTENTS AND SERVICE OF ORDERS.—An order of the Adminis-
13 trator shall include the findings of fact on which the order is based and
14 shall be served on the parties to the proceeding and the persons affected
15 by the order.

16 **“§ 40986. Enforcement by the Department**

17 “The Administrator may bring a civil action against a person in a district
18 court of the United States to enforce this chapter or a requirement or regu-
19 lation prescribed or order issued under this chapter. The action may be
20 brought in the judicial district in which the person does business or the vio-
21 lation occurred.

22 **“§ 40987. Enforcement by Attorney General**

23 “(a) IN GENERAL.—On request of the Administrator, the Attorney Gen-
24 eral may bring a civil action in an appropriate court—

25 “(1) to enforce this chapter or a requirement or regulation pre-
26 scribed or order issued under this chapter; and

27 “(2) to prosecute a person violating this chapter or a requirement
28 or regulation prescribed or order issued under this chapter.

29 “(b) COSTS AND EXPENSES PAID OUT OF APPROPRIATIONS FOR COURT
30 EXPENSES.—The costs and expenses of a civil action under this chapter
31 shall be paid out of the appropriations for the expenses of the courts of the
32 United States.

33 “(c) PARTICIPATION OF ADMINISTRATOR.—On request of the Attorney
34 General, the Administrator may participate in a civil action under this chap-
35 ter.

36 **“§ 40988. Joinder and intervention**

37 “A person interested in or affected by a matter under consideration in
38 a proceeding before the Administrator, a civil action to enforce this chapter,
39 or a requirement or regulation prescribed or order issued under this chapter
40 may be joined as a party or permitted to intervene in the proceeding or civil
41 action.

1 “§ 40989. **Judicial review**

2 “(a) **FILING AND VENUE.**—A person disclosing a substantial interest in
3 an order issued by the Administrator, in whole or in part under this chapter
4 or sections 11307 or 11314 of this title, may apply for review of the order
5 by filing a petition for review in the United States Court of Appeals for the
6 District of Columbia Circuit or in the court of appeals of the United States
7 for the circuit in which the person resides or has its principal place of busi-
8 ness. The petition must be filed not later than 60 days after the order is
9 issued. The court may allow the petition to be filed after the 60th day only
10 if there are reasonable grounds for not filing by the 60th day.

11 “(b) **JUDICIAL PROCEDURES.**—When a petition is filed under subsection
12 (a), the clerk of the court immediately shall send a copy of the petition to
13 the Administrator. The Administrator shall file with the court a record of
14 any proceeding in which the order was issued, as provided in section 2112
15 of title 28.

16 “(c) **AUTHORITY OF COURT.**—When the petition is sent to the Adminis-
17 trator, the court has exclusive jurisdiction to affirm, amend, modify, or set
18 aside any part of the order and may order the Administrator to conduct
19 further proceedings. After reasonable notice to the Administrator, the court
20 may grant interim relief by staying the order or taking other appropriate
21 action when good cause for its action exists. Findings of fact by the Admin-
22 istrator, if supported by substantial evidence, are conclusive.

23 “(d) **REQUIREMENT FOR PRIOR OBJECTION.**—In reviewing an order
24 under this section, the court may consider an objection to an order of the
25 Administrator only if the objection was made in the proceeding conducted
26 by the Administrator or if there was a reasonable ground for not making
27 the objection in the proceeding.

28 “(e) **SUPREME COURT REVIEW.**—A decision by a court under this section
29 may be reviewed only by the Supreme Court under section 1254 of title
30 28.”.

31 (5) In the analysis for chapter 409, as amended by paragraph (3),
32 insert after the item relating to 40963 the following:

“**Subchapter IV—Investigations and Proceedings**

- “40981. Complaints and investigations.
- “40982. Proceedings.
- “40983. Service of notice, process, and actions.
- “40984. Evidence.
- “40985. Regulations and orders.
- “40986. Enforcement by the Department.
- “40987. Enforcement by Attorney General.
- “40988. Joinder and intervention.
- “40989. Judicial review.”.

33 (c) **TITLE 18, UNITED STATES CODE.**—

34 (1) **IN GENERAL.**—Title 18, United States Code is amended by add-
35 ing at the end of part I the following:

1 **“CHAPTER 125—AIR TRANSPORTATION SECURITY**

“Sec.

“2741. Reporting and recordkeeping violations.

“2742. Unlawful disclosure of information.

“2743. Refusing to appear or produce records.

“2744. Entering aircraft or airport area in violation of security requirements.

“2745. General criminal penalty when specific penalty not provided.

2 **“§ 2741. Reporting and recordkeeping violations**

3 “An air carrier or an officer, agent, or employee of an air carrier shall
4 be fined under this title for intentionally—

5 “(1) failing to make a report or keep a record under chapter 409
6 of title 6;

7 “(2) falsifying, mutilating, or altering a report or record under chap-
8 ter 409 of title 6; or

9 “(3) filing a false report or record under chapter 409 of title 6.

10 **“§ 2742. Unlawful disclosure of information**

11 “(a) CRIMINAL PENALTY.—The Administrator of the Transportation Se-
12 curity Administration, or an officer or employee of the Administration, shall
13 be fined under this title, imprisoned for not more than 2 years, or both,
14 if the Administrator, officer, or employee knowingly and willfully discloses
15 information that—

16 “(1) the Administrator, officer, or employee acquires when inspecting
17 the records of an air carrier; or

18 “(2) is withheld from public disclosure under section 40963 of title
19 6.

20 “(b) NONAPPLICATION.—Subsection (a) does not apply if—

21 “(1) the officer or employee is directed by the Administrator to dis-
22 close information that the Administrator had ordered withheld; or

23 “(2) the Administrator, officer, or employee is directed by a court
24 of competent jurisdiction to disclose the information.

25 “(c) WITHHOLDING INFORMATION FROM CONGRESS.—This section does
26 not authorize the Administrator to withhold information from a committee
27 of Congress authorized to have the information.

28 **“§ 2743. Refusing to appear or produce records**

29 “A person not obeying a subpoena or requirement of the Administrator of
30 the Transportation Security Administration to appear and testify or produce
31 records shall be fined under this title, imprisoned for not more than 1 year,
32 or both.

33 **“§ 2744. Entering aircraft or airport area in violation of se-
34 curity requirements**

35 “(a) PROHIBITION.—A person may not knowingly and willfully enter, in
36 violation of security requirements prescribed under section 40911, 40913(b)

1 or (e), or 40916 of title 6, an aircraft or an airport area that serves an
2 air carrier or foreign air carrier.

3 “(b) CRIMINAL PENALTY.—

4 “(1) IN GENERAL.—A person violating subsection (a) shall be fined
5 under this title, imprisoned for not more than 1 year, or both.

6 “(2) INCREASED PENALTY.—A person violating subsection (a) with
7 intent to evade security procedures or restrictions or with intent to
8 commit, in the aircraft or airport area, a felony under a law of the
9 United States or a State shall be fined under this title, imprisoned for
10 not more than 10 years, or both.

11 “(c) NOTICE OF PENALTIES.—

12 “(1) SIGNS.—Each operator of an airport in the United States that
13 is required to establish an air transportation security program under
14 section 40913(e) of title 6 shall ensure that signs that meet require-
15 ments the Secretary of Homeland Security may prescribe for providing
16 notice of the penalties imposed under subsection (b) and section
17 4201(b)(4)(A) of title 28 are displayed near all screening locations, all
18 locations where passengers exit the sterile area, and other locations at
19 the airport that the Secretary of Homeland Security determines appro-
20 priate.

21 “(2) EFFECT OF SIGNS ON PENALTIES.—An individual is subject to
22 a penalty imposed under subsection (b) or section 4201(b)(4)(A) of
23 title 28 without regard to whether signs are displayed at an airport as
24 required by paragraph (1).

25 **“§ 2745. General criminal penalty when specific penalty not**
26 **provided**

27 “When another criminal penalty is not provided under chapter 409 of
28 title 6, a person that knowingly and willfully violates section 40912,
29 40913(d), 40914, 40917, 40918, or 40919 of title 6, or a regulation pre-
30 scribed or order issued by the Administrator of the Transportation Security
31 Administration under section 40912, 40913(d), 40914, 40917, 40918, or
32 40919 of title 6, shall be fined under this title. A separate violation occurs
33 for each day the violation continues.

34 **“CHAPTER 127—SPECIAL AIRCRAFT JURISDICTION OF**
35 **THE UNITED STATES**

“Sec.

“2761. Definitions.

“2762. Aircraft piracy.

“2763. Interference with security screening personnel.

“2764. Interference with flight crew members and attendants.

“2765. Carrying a weapon or explosive on an aircraft.

“2766. Application of certain criminal laws to acts on an aircraft.

“2767. False information and threats.

1 **“§2761. Definitions**

2 “In this subchapter:

3 “(1) AIRCRAFT IN FLIGHT.—The term ‘aircraft in flight’ means an
4 aircraft from the moment all external doors are closed following board-
5 ing—

6 “(A) through the moment when one external door is opened to
7 allow passengers to leave the aircraft; or

8 “(B) until, if a forced landing, competent authorities take over
9 responsibility for the aircraft and individuals and property on the
10 aircraft.

11 “(2) COMMIT AN OFFENSE.—The term ‘commit an offense’ means,
12 in the case of an individual and for the purposes of the Convention for
13 the Suppression of Unlawful Seizure of Aircraft, when the individual,
14 when on an aircraft in flight—

15 “(A) by any form of intimidation, unlawfully seizes, exercises
16 control of, or attempts to seize or exercise control of, the aircraft;
17 or

18 “(B) is an accomplice of an individual referred to in subpara-
19 graph (A).

20 “(3) SPECIAL AIRCRAFT JURISDICTION OF THE UNITED STATES.—
21 The term ‘special aircraft jurisdiction of the United States’ includes
22 any of the following aircraft in flight:

23 “(A) A civil aircraft of the United States.

24 “(B) An aircraft of the armed forces of the United States.

25 “(C) Another aircraft in the United States.

26 “(D) Another aircraft outside the United States—

27 “(i) that has its next scheduled destination or last place of
28 departure in the United States, if the aircraft next lands in
29 the United States;

30 “(ii) on which an individual commits an offense (as speci-
31 fied in the Convention for the Suppression of Unlawful Sei-
32 zure of Aircraft) if the aircraft lands in the United States
33 with the individual still on the aircraft; or

34 “(iii) against which an individual commits an offense (as
35 specified in subsection (d) or (e) of article I, section I of the
36 Convention for the Suppression of Unlawful Acts against the
37 Safety of Civil Aviation) if the aircraft lands in the United
38 States with the individual still on the aircraft.

39 “(E) Any other aircraft leased without crew to a lessee whose
40 principal place of business is in the United States or, if the lessee

1 does not have a principal place of business, whose permanent resi-
2 dence is in the United States.

3 **“§ 2762. Aircraft piracy**

4 “(a) AIRCRAFT PIRACY IN SPECIAL AIRCRAFT JURISDICTION.—

5 “(1) DEFINITION OF AIRCRAFT PIRACY.—In this subsection, the
6 term ‘aircraft piracy’ means seizing or exercising control of an aircraft
7 in the special aircraft jurisdiction of the United States by force, vio-
8 lence, threat of force or violence, or any form of intimidation, and with
9 wrongful intent.

10 “(2) WHEN ATTEMPT TO COMMIT AIRCRAFT PIRACY DEEMED TO BE
11 IN SPECIAL AIRCRAFT JURISDICTION.—An attempt to commit aircraft
12 piracy is deemed to be in the special aircraft jurisdiction of the United
13 States, although the aircraft is not in flight at the time of the attempt,
14 if the aircraft would have been in the special aircraft jurisdiction of the
15 United States had the aircraft piracy been completed.

16 “(3) CRIMINAL PENALTY.—An individual committing or attempting
17 or conspiring to commit aircraft piracy—

18 “(A) shall be imprisoned for at least 20 years; or

19 “(B) notwithstanding section 3559(b) of this title, if the death
20 of another individual results from the commission or attempt, shall
21 be put to death or imprisoned for life.

22 “(b) AIRCRAFT PIRACY OUTSIDE SPECIAL AIRCRAFT JURISDICTION.—

23 “(1) DEFINITION OF NATIONAL OF THE UNITED STATES.—In this
24 subsection, the term ‘national of the United States’ has the meaning
25 given the term in section 101(a) of the Immigration and Nationality
26 Act (8 U.S.C. 1101(a)).

27 “(2) CRIMINAL PENALTY.—An individual committing or conspiring
28 to commit an offense (as specified in the Convention for the Suppres-
29 sion of Unlawful Seizure of Aircraft) on an aircraft in flight outside
30 the special aircraft jurisdiction of the United States—

31 “(A) shall be imprisoned for at least 20 years; or

32 “(B) notwithstanding section 3559(b) of this title, if the death
33 of another individual results from the commission or attempt, shall
34 be put to death or imprisoned for life.

35 “(3) JURISDICTION.—There is jurisdiction over the offense in para-
36 graph (2) if—

37 “(A) a national of the United States was aboard the aircraft;

38 “(B) an offender is a national of the United States; or

39 “(C) an offender is afterwards found in the United States.

1 **“§ 2763. Interference with security screening personnel**

2 “An individual in an area in a commercial service airport in the United
3 States who, by assaulting a Federal, airport, or air carrier employee who
4 has security duties in the airport, interferes with the performance of the du-
5 ties of the employee or lessens the ability of the employee to perform those
6 duties shall be fined under this title, imprisoned for not more than 10 years,
7 or both. If the individual uses a dangerous weapon in committing the as-
8 sult or interference, the individual may be imprisoned for any term of
9 years or for life.

10 **“§ 2764. Interference with flight crew members and attend-**
11 **ants**

12 “An individual on an aircraft in the special aircraft jurisdiction of the
13 United States who, by assaulting or intimidating a flight crew member or
14 flight attendant of the aircraft, interferes with the performance of the duties
15 of the member or attendant or lessens the ability of the member or attend-
16 ant to perform those duties, or attempts or conspires to do such an act,
17 shall be fined under this title, imprisoned for not more than 20 years, or
18 both. If a dangerous weapon is used in assaulting or intimidating the mem-
19 ber or attendant, the individual shall be imprisoned for any term of years
20 or for life.

21 **“§ 2765. Carrying a weapon or explosive on an aircraft**

22 “(a) DEFINITION OF LOADED FIREARM.—In this section, the term ‘loaded
23 firearm’ means a starter gun or a weapon designed or converted to expel
24 a projectile through an explosive, that has a cartridge, a detonator, or pow-
25 der in the chamber, magazine, cylinder, or clip.

26 “(b) GENERAL CRIMINAL PENALTY.—An individual shall be fined under
27 this title, imprisoned for not more than 10 years, or both, if the indi-
28 vidual—

29 “(1) when on, or attempting to get on, an aircraft in, or intended
30 for operation in, air transportation or intrastate air transportation, has
31 on or about the individual or the property of the individual a concealed
32 dangerous weapon that is or would be accessible to the individual in
33 flight;

34 “(2) has placed, attempted to place, or attempted to have placed a
35 loaded firearm on that aircraft in property not accessible to passengers
36 in flight; or

37 “(3) has on or about the individual, or has placed, attempted to
38 place, or attempted to have placed on that aircraft, an explosive or in-
39 cendiary device.

40 “(c) CRIMINAL PENALTY INVOLVING DISREGARD FOR HUMAN LIFE.—An
41 individual who willfully and without regard for the safety of human life, or

1 with reckless disregard for the safety of human life, violates subsection (b)
2 shall be fined under this title, imprisoned for not more than 20 years, or
3 both, and, if death results to any person, shall be imprisoned for any term
4 of years or for life.

5 “(d) NONAPPLICATION.—Subsection (b)(1) does not apply to—

6 “(1) a law enforcement officer of a State or political subdivision of
7 a State, or an officer or employee of the United States Government,
8 authorized to carry arms in an official capacity;

9 “(2) another individual the Administrator of the Transportation Se-
10 curity Administration by regulation authorizes to carry a dangerous
11 weapon in air transportation or intrastate air transportation; or

12 “(3) an individual transporting a weapon (except a loaded firearm)
13 in baggage not accessible to a passenger in flight if the air carrier was
14 informed of the presence of the weapon.

15 “(e) CONSPIRACY.—If 2 or more individuals conspire to violate subsection
16 (b) or (c), and any of the individuals does any act to effect the object of
17 the conspiracy, each of the parties to the conspiracy shall be punished as
18 provided in subsection (b) or (c).

19 **“§ 2766. Application of certain criminal laws to acts on an**
20 **aircraft**

21 “An individual on an aircraft in the special aircraft jurisdiction of the
22 United States who commits an act that—

23 “(1) if committed in the special maritime and territorial jurisdiction
24 of the United States (as defined in section 7 of this title) would violate
25 section 113, 114, 661, 662, 1111, 1112, 1113, or 2111 or chapter
26 109A of this title, shall be fined under this title, imprisoned under that
27 section or chapter, or both; or

28 “(2) if committed in the District of Columbia would violate section
29 9 of the Act of July 29, 1892 (D.C. Code 22-1312), shall be fined
30 under this title, imprisoned under section 9 of the Act, or both.

31 **“§ 2767. False information and threats**

32 “An individual shall be fined under this title, imprisoned for not more
33 than 5 years, or both, if the individual—

34 “(1) knowing the information to be false, willfully and maliciously or
35 with reckless disregard for the safety of human life, gives, or causes
36 to be given, under circumstances in which the information reasonably
37 may be believed, false information about an alleged attempt being made
38 or to be made to do an act that would violate section 2762(a), 2764,
39 2765, or 2766 of this title; or

1 “(2) threatens to violate section 2762(a), 2764, 2765, or 2766 of
2 this title, or causes a threat to violate any of those sections to be made,
3 and has the apparent determination and will to carry out the threat.”.

4 (2) TABLE OF CONTENTS.—The table of contents of part I of title
5 18, United States Code, is amended by adding at the end the following:

“125. Air Transportation Security	2741
“127. Special Aircraft Jurisdiction of the United States	2761”.

6 (d) TITLE 28, UNITED STATES CODE.—

7 (1) IN GENERAL.—Part VI of title 28, United States Code, is
8 amended by adding after section 4105 the following:

9 “**CHAPTER 182—AIR TRANSPORTATION SECURITY**

“Sec.

“4201. Civil penalties.

“4202. False information.

“4203. Carrying a weapon.

“4204. Interference with cabin or flight crew.

“4205. Actions to recover civil penalties.

10 “**§ 4201. Civil penalties**

11 “(a) DEFINITION OF SMALL BUSINESS CONCERN.—In this section, the
12 term ‘small business concern’ has the meaning given the term in section 3
13 of the Small Business Act (15 U.S.C. 632).

14 “(b) GENERAL PENALTY.—

15 “(1) CHAPTER 409 VIOLATIONS; REGULATION VIOLATIONS.—A per-
16 son is liable to the United States Government for a civil penalty of not
17 more than \$25,000 (or \$1,100 if the person is an individual or small
18 business concern) for violating—

19 “(A) chapter 409 (except sections 40912, 40913(d), 40914,
20 40917 (a) through (d)(1)(A) and (1)(C) through (f), and 40918)
21 of title 6; or

22 “(B) a regulation prescribed or order issued under any provision
23 to which subparagraph (A) applies.

24 “(2) SEPARATE VIOLATIONS.—A separate violation occurs under this
25 subsection for each day the violation continues or, if applicable, for
26 each flight involving the violation.

27 “(3) AVIATION SECURITY VIOLATIONS.—Notwithstanding paragraph
28 (1) of this subsection, the maximum civil penalty for violating chapter
29 409 of title 6 shall be \$10,000; except that the maximum civil penalty
30 shall be \$25,000 in the case of a person operating an aircraft for the
31 transportation of passengers or property for compensation (except an
32 individual serving as an airman).

33 “(4) PENALTIES APPLICABLE TO INDIVIDUALS AND SMALL BUSINESS
34 CONCERNS.—An individual (except an airman serving as an airman) or
35 small business concern is liable to the Government for a civil penalty
36 of not more than \$10,000 for violating—

1 “(A) chapter 409 (except sections 40912, 40913(d), 40914, and
2 40917 through 40919) of title 6; or

3 “(B) a regulation prescribed or order issued under any provision
4 to which subparagraph (A) applies.

5 “(5) FAILURE TO COLLECT AIRPORT SECURITY BADGES.—Notwith-
6 standing paragraph (1), an employer (other than a governmental entity
7 or airport operator) who employs an employee to whom an airport secu-
8 rity badge or other identifier used to obtain access to a secure area of
9 an airport is issued and who does not collect or make reasonable efforts
10 to collect the badge from the employee on the date that the employ-
11 ment of the employee is terminated and does not notify the operator
12 of the airport of the termination within 24 hours of the date of the
13 termination is liable to the Government for a civil penalty not to exceed
14 \$10,000.

15 “(c) PROCEDURAL REQUIREMENTS.—

16 “(1) IN GENERAL.—The Secretary of Homeland Security may im-
17 pose a civil penalty for the following violations only after notice and
18 an opportunity for a hearing:

19 “(A) A violation of section 40919 of title 6.

20 “(B) A violation of a regulation prescribed or order issued
21 under any provision to which subparagraph (A) of this paragraph
22 applies.

23 “(2) WRITTEN NOTICE.—The Secretary of Homeland Security shall
24 give written notice of the finding of a violation and the civil penalty
25 under paragraph (1) of this subsection.

26 “(d) ADMINISTRATIVE IMPOSITION OF PENALTIES.—

27 “(1) DEFINITIONS.—In this subsection:

28 “(A) FLIGHT ENGINEER.—The term ‘flight engineer’ means an
29 individual who holds a flight engineer certificate issued under part
30 63 of title 14, Code of Federal Regulations.

31 “(B) MECHANIC.—The term ‘mechanic’ means an individual
32 who holds a mechanic certificate issued under part 65 of title 14,
33 Code of Federal Regulations.

34 “(C) PILOT.—The term ‘pilot’ means an individual who holds
35 a pilot certificate issued under part 61 of title 14, Code of Federal
36 Regulations.

37 “(D) REPAIRMAN.—The term ‘repairman’ means an individual
38 who holds a repairman certificate issued under part 65 of title 14,
39 Code of Federal Regulations.

40 “(2) PENALTY COVERAGE.—

1 “(A) IN GENERAL.—The Secretary of Homeland Security may
2 impose a civil penalty for a violation of chapter 409 (except sec-
3 tions 40912, 40913(d), 40917 (a) through (d)(1)(A) and (1)(C)
4 through (f), 40918, and 40919) of title 6.

5 “(B) WRITTEN NOTICE.—The Secretary of Homeland Security
6 shall give written notice of the finding of a violation and the pen-
7 alty.

8 “(C) EXCEPTION.—In the case of a violation of section 4202 of
9 this title or a regulation prescribed or order issued under that pro-
10 vision, a penalty may not be imposed under this subsection for a
11 violation relating to section 2764 of title 18.

12 “(3) LIMIT ON REEXAMINATION.—In a civil action to collect a civil
13 penalty imposed by the Secretary of Homeland Security under this sub-
14 section, the issues of liability and the amount of the penalty may not
15 be reexamined.

16 “(4) DISTRICT COURT JURISDICTION.—Notwithstanding paragraph
17 (2) of this subsection, the district courts of the United States have ex-
18 clusive jurisdiction of a civil action involving a penalty the Secretary
19 of Homeland Security initiates if—

20 “(A) the amount in controversy is more than—

21 “(i) \$50,000 if the violation was committed by any person
22 before December 12, 2003;

23 “(ii) \$400,000 if the violation was committed by a person
24 other than an individual or small business concern on or after
25 that date; or

26 “(iii) \$50,000 if the violation was committed by an indi-
27 vidual or small business concern on or after that date;

28 “(B) the action is in rem or another action in rem based on the
29 same violation has been brought;

30 “(C) the action involves an aircraft subject to a lien that has
31 been seized by the Government; or

32 “(D) another action has been brought for an injunction based
33 on the same violation.

34 “(5) MAXIMUM PENALTY.—The maximum civil penalty the Secretary
35 of Homeland Security may impose under this subsection is—

36 “(A) \$50,000 if the violation was committed by any person be-
37 fore December 12, 2003;

38 “(B) \$400,000 if the violation was committed by a person other
39 than an individual or small business concern on or after that date;
40 or

1 “(C) \$50,000 if the violation was committed by an individual or
2 small business concern on or after that date.

3 “(6) LIMITATION.—This subsection applies only to a violation occur-
4 ring after August 25, 1992.

5 “(e) COMPROMISE AND SETOFF.—

6 “(1) COMPROMISE.—The Secretary of Homeland Security may com-
7 promise the amount of a civil penalty imposed for violating—

8 “(A) chapter 409 (except sections 40912, 40913(d), 40914,
9 40917(a) through (d)(1)(A) and (1)(C) through (f), 40918, and
10 40919) of title 6; or

11 “(B) a regulation prescribed or order issued under any provision
12 to which subparagraph (A) of this paragraph applies.

13 “(2) SETOFF.—The United States Government may deduct the
14 amount of a civil penalty imposed or compromised under this sub-
15 section from amounts it owes the person liable for the penalty.

16 “(f) JUDICIAL REVIEW.—An order of the Secretary of Homeland Security
17 imposing a civil penalty may be reviewed judicially only under section 40989
18 of title 6.

19 “(g) NONAPPLICATION.—

20 “(1) IN GENERAL.—This section does not apply to the following
21 when performing official duties:

22 “(A) A member of the armed forces of the United States.

23 “(B) A civilian employee of the Department of Defense subject
24 to the Uniform Code of Military Justice.

25 “(2) REPORT ON ACTION TAKEN.—The appropriate military author-
26 ity is responsible for taking necessary disciplinary action and submit-
27 ting to the Secretary of Homeland Security a timely report on action
28 taken.

29 “**§ 4202. False information**

30 “(a) CIVIL PENALTY.—A person that, knowing the information to be
31 false, gives, or causes to be given, under circumstances in which the infor-
32 mation reasonably may be believed, false information about an alleged at-
33 tempt being made or to be made to do an act that would violate section
34 2762(a), 2764, 2765, or 2766 of title 18 is liable to the United States Gov-
35 ernment for a civil penalty of not more than \$10,000 for each violation.

36 “(b) COMPROMISE AND SETOFF.—

37 “(1) COMPROMISE.—The Secretary of Homeland Security may com-
38 promise the amount of a civil penalty imposed under subsection (a).

39 “(2) SETOFF.—The United States Government may deduct the
40 amount of a civil penalty imposed or compromised under this section
41 from amounts it owes the person liable for the penalty.

1 **“§ 4203. Carrying a weapon**

2 “(a) CIVIL PENALTY.—An individual who, when on, or attempting to
3 board, an aircraft in, or intended for operation in, air transportation or
4 intrastate air transportation, has on or about the individual or the property
5 of the individual a concealed dangerous weapon that is or would be acces-
6 sible to the individual in flight is liable to the United States Government
7 for a civil penalty of not more than \$10,000 for each violation.

8 “(b) COMPROMISE AND SETOFF.—

9 “(1) COMPROMISE.—The Secretary of Homeland Security may com-
10 promise the amount of a civil penalty imposed under subsection (a).

11 “(2) SETOFF.—The United States Government may deduct the
12 amount of a civil penalty imposed or compromised under this section
13 from amounts it owes the individual liable for the penalty.

14 “(c) NONAPPLICATION.—This section does not apply to—

15 “(1) a law enforcement officer of a State or political subdivision of
16 a State, or an officer or employee of the United States Government,
17 authorized to carry arms in an official capacity; or

18 “(2) another individual the Secretary of Homeland Security or the
19 Administrator of the Federal Aviation Administration by regulation au-
20 thORIZES to carry arms in an official capacity.

21 **“§ 4204. Interference with cabin or flight crew**

22 “(a) IN GENERAL.—An individual who physically assaults or threatens to
23 physically assault a member of the flight crew or cabin crew of a civil air-
24 craft or any other individual on the aircraft, or takes any action that poses
25 an imminent threat to the safety of the aircraft or other individuals on the
26 aircraft is liable to the United States Government for a civil penalty of not
27 more than \$25,000.

28 “(b) COMPROMISE AND SETOFF.—

29 “(1) COMPROMISE.—The Secretary of Homeland Security may com-
30 promise the amount of a civil penalty imposed under this section.

31 “(2) SETOFF.—The United States Government may deduct the
32 amount of a civil penalty imposed or compromised under this section
33 from amounts the Government owes the person liable for the penalty.

34 **“§ 4205. Actions to recover civil penalties**

35 “A civil penalty under this chapter may be collected by bringing a civil
36 action against the person subject to the penalty, a civil action in rem
37 against an aircraft subject to a lien for a penalty, or both. The action shall
38 conform as nearly as practicable to a civil action in admiralty, regardless
39 of the place an aircraft in a civil action in rem is seized. However, a party
40 may demand a jury trial of an issue of fact in an action involving a civil
41 penalty under this chapter if the value of the matter in controversy is more

1 than \$20. Issues of fact tried by a jury may be reexamined only under com-
 2 mon law rules.”.

3 (2) TABLE OF CONTENTS.—The table of contents of part VI of title
 4 28, United States Code, is amended by adding after the item for chap-
 5 ter 181 the following:

“**182. Air Transportation Security** **4201**”.

6 (e) TITLE 49, UNITED STATES CODE.—Title 49, United States Code, is
 7 amended as follows:

8 (1) Section 106(g) is amended to read as follows:

9 “(g) DUTIES AND POWERS OF ADMINISTRATOR.—The Administrator
 10 shall carry out—

11 “(1) duties and powers of the Secretary of Transportation under
 12 subsection (f) of this section related to aviation safety (except those re-
 13 lated to transportation, packaging, marking, or description of haz-
 14 ardous material) and stated in sections 308(b), 1132(c) and (d),
 15 40101(e), 40103(b), 40106(a), 40108, 40109(b), 40113(a), 40113(e),
 16 40113(d), 40113(e), 40114(a), and 40119, chapter 445 (except sec-
 17 tions 44501(b), 44502(a)(2), 44502(a)(3), 44502(a)(4), 44503, 44506,
 18 44509, 44510, 44514, and 44515), chapter 447 (except sections
 19 44717, 44718(a), 44718(b), 44719, 44720, 44721(b), 44722, and
 20 44723), chapter 451, chapter 453, sections 46104, 46301(d) and
 21 (h)(2), 46303(e), 46304–46308, 46310, 46311, and 46313–46316,
 22 chapter 465, and sections 47504(b) (related to flight procedures),
 23 47508(a), and 48107 of this title; and

24 “(2) additional duties and powers prescribed by the Secretary of
 25 Transportation.”.

26 (2) Chapter 51 is amended—

27 (A) by inserting after section 5110 the following:

28 “**§ 5111. Hazardous material highway route plans**

29 “(a) ROUTE PLAN GUIDANCE.—The Secretary of Transportation, in con-
 30 sultation with the Secretary of Homeland Security, shall—

31 “(1) document existing and proposed routes for the transportation
 32 of radioactive and nonradioactive hazardous materials by motor carrier,
 33 and develop a framework for using a geographic information system-
 34 based approach to characterize routes in the national hazardous mate-
 35 rials route registry;

36 “(2) assess and characterize existing and proposed routes for the
 37 transportation of radioactive and nonradioactive hazardous materials
 38 by motor carrier for the purpose of identifying measurable criteria for
 39 selecting routes based on safety and security concerns;

1 “(3) analyze current route-related hazardous materials regulations in
2 the United States, Canada, and Mexico to identify cross-border dif-
3 ferences and conflicting regulations;

4 “(4) document the safety and security concerns of the public, motor
5 carriers, and State, local, territorial, and tribal governments about the
6 highway routing of hazardous materials;

7 “(5) prepare guidance materials for State officials to assist them in
8 identifying and reducing both safety concerns and security risks when
9 designating highway routes for hazardous materials consistent with the
10 13 safety-based nonradioactive materials routing criteria and radio-
11 active materials routing criteria in subparts C and D of part 397 of
12 title 49, Code of Federal Regulations;

13 “(6) develop a tool that will enable State officials to examine poten-
14 tial routes for the highway transportation of hazardous materials, as-
15 sess specific security risks associated with each route, and explore al-
16 ternative mitigation measures; and

17 “(7) transmit to the appropriate congressional committees (as de-
18 fined in section 10101 of title 6) a report on the actions taken to fulfill
19 paragraphs (1) through (6) and any recommended changes to the rout-
20 ing requirements for the highway transportation of hazardous materials
21 in part 397 of title 49, Code of Federal Regulations.

22 “(b) ROUTE PLANS.—

23 “(1) ASSESSMENT.—The Secretary of Transportation shall complete
24 an assessment of the safety and national security benefits achieved
25 under existing requirements for route plans, in written or electronic
26 format, for explosives and radioactive materials. The assessment shall,
27 at a minimum—

28 “(A) compare the percentage of Department of Transportation
29 recordable incidents and the severity of the incidents for shipments
30 of explosives and radioactive materials for which route plans are
31 required with the percentage of recordable incidents and the sever-
32 ity of the incidents for shipments of explosives and radioactive ma-
33 terials not subject to route plans; and

34 “(B) quantify the security and safety benefits, feasibility, and
35 costs of requiring each motor carrier that is required to have a
36 hazardous material safety permit under part 385 of title 49, Code
37 of Federal Regulations, to maintain, follow, and carry a route plan
38 that meets the requirements of section 397.101 of that title when
39 transporting the type and quantity of hazardous materials de-
40 scribed in section 385.403, taking into account the various seg-

1 ments of the motor carrier industry, including tank truck, truck-
2 load, and less-than-truckload carriers.

3 “(2) REPORT.—The Secretary of Transportation shall submit a re-
4 port to the appropriate congressional committees containing the find-
5 ings and conclusions of the assessment.

6 “(c) REQUIREMENT.—The Secretary shall require a motor carrier that
7 has a hazardous material safety permit under part 385 of title 49, Code
8 of Federal Regulations, to maintain, follow, and carry a route plan, in writ-
9 ten or electronic format, that meets the requirements of section 397.101 of
10 that title when transporting the type and quantity of hazardous materials
11 described in section 385.403 if the Secretary determines, under the assess-
12 ment required in subsection (b), that such a requirement would enhance se-
13 curity and safety without imposing unreasonable costs or burdens upon
14 motor carriers.”;

15 (B) by inserting the following after section 5118:

16 “**§ 5118a. Hazardous materials security inspections and**
17 **study**

18 “(a) IN GENERAL.—The Secretary of Transportation shall consult with
19 the Secretary of Homeland Security to limit, to the extent practicable, dupli-
20 cative reviews of the hazardous materials security plans required under part
21 172, title 49, Code of Federal Regulations.

22 “(b) TRANSPORTATION COSTS STUDY.—The Secretary of Transportation,
23 in conjunction with the Secretary of Homeland Security, shall study to what
24 extent the insurance, security, and safety costs borne by railroad carriers,
25 motor carriers, pipeline carriers, air carriers, and maritime carriers associ-
26 ated with the transportation of hazardous materials are reflected in the
27 rates paid by offerors of the commodities as compared to the costs and
28 rates, respectively, for the transportation of nonhazardous materials.”; and

29 (C) by amending the chapter analysis for chapter 51—

30 (i) by inserting the following after the item relating to sec-
31 tion 5110:

“5111. Hazardous material highway route plans.”;

32 and

33 (ii) by inserting the following after the item relating to sec-
34 tion 5118:

“5118a. Hazardous materials security inspections and study.”.

35 (3) Chapter 401 is amended—

36 (A) in section 40113—

37 (i) in subsection (a)—

38 (I) by striking “the Under Secretary of Transpor-
39 tation for Security with respect to security duties and

- 1 powers designated to be carried out by the Under Sec-
 2 retary or”; and
 3 (II) by striking “, Under Secretary,”; and
 4 (ii) in subsection (d)—
 5 (I) by striking “Under Secretary of Transportation for
 6 Security or the”;
 7 (II) by striking “Transportation Security Administra-
 8 tion or Federal Aviation Administration, as the case may
 9 be,” and inserting “Federal Aviation Administration”;
 10 and
 11 (III) by striking “Under Secretary or Administrator,
 12 as the case may be,” and inserting “Administrator”; and
 13 (B) in section 40119(a)—
 14 (i) by striking “Under Secretary of Transportation for Se-
 15 curity and the”; and
 16 (ii) by striking “each”.
- 17 (4) Chapter 461 is amended—
 18 (A) by striking “the Under Secretary of Transportation for Se-
 19 curity with respect to security duties and powers designated to be
 20 carried out by the Under Secretary or” and “, Under Secretary,”
 21 each place they appear;
 22 (B) in section 46102—
 23 (i) in subsection (b), by striking “, the Under Secretary,
 24 and” and inserting “or”; and
 25 (ii) in subsection (d), by striking “the Under Secretary,”;
 26 (C) in section 46104(b) as amended by subparagraph (A), by
 27 striking “, the Under Secretary”; and
 28 (D) in section 46111—
 29 (i) by striking “Under Secretary for Border and Transpor-
 30 tation Security of the Department of” and inserting “Sec-
 31 retary”; and
 32 (ii) by striking “Under Secretary” each place it appears
 33 and inserting “Secretary”.
- 34 (5) Section 46301(d) is amended—
 35 (A) in paragraph (2), by striking the last two sentences and in-
 36 serting “The Administrator shall give written notice of the finding
 37 of a violation and the penalty.”;
 38 (B) in paragraph (3), by striking “Secretary of Homeland Secu-
 39 rity or”;
 40 (C) in paragraph (4), by striking “Secretary of Homeland Secu-
 41 rity or”; and

1 (D) in paragraph (8), by striking “Under Secretary, Adminis-
2 trator,” and inserting “Administrator”.

3 (6) Section 46505(d)(2) is amended by striking “Under Secretary of
4 Transportation for Security” and inserting “Secretary of Homeland Se-
5 curity”.

6 (7) Section 367 of Public Law 108–7 (49 U.S.C. 47110 note) is
7 amended—

8 (A) in subsection (a), by striking “Under Secretary of Trans-
9 portation for Security” and inserting “Secretary of Homeland Se-
10 curity”; and

11 (B) by striking “Under Secretary” each place it appears and in-
12 serting “Secretary”.

13 (8) Chapter 483 is repealed.

14 (9) The table of contents for subtitle VII of title 49, United States
15 Code, is amended as follows:

16 (A) After the item for chapter 447, strike
17 “**449. Security** **44901**”.

(B) After the item for chapter 482, strike
18 “**483. Aviation Security Funding** **48301**”.

19 **SEC. 5. CONFORMING CROSS REFERENCES.**

20 (a) TITLE 5, UNITED STATES CODE.—Title 5, United States Code, is
21 amended as follows:

22 (1) Section 9701(g) is amended by striking “section 842 of the
23 Homeland Security Act of 2002” and inserting “section 10352 of title
24 6”.

25 (2) Section 10101 is amended—

26 (A) in paragraph (3), by striking “section 602 of the Post-
27 Katrina Emergency Management Reform Act of 2006” and insert-
28 ing “section 20101 of title 6”; and

29 (B) in paragraph (5), by striking “section 624 of the Post-
30 Katrina Emergency Management Reform Act of 2006” and insert-
31 ing “section 20301 of title 6”.

32 (3) Section 10103(b) is amended by striking “section 844 of the
33 Homeland Security Act of 2002” and inserting “section 10356 of title
34 6”.

35 (b) TITLE 8, UNITED STATES CODE.—Section 7202(g)(2)(H) of the In-
36 telligence Reform and Terrorism Prevention Act of 2004 (8 U.S.C.
37 1777(g)(2)(H)) is amended by striking “section 1016(b)” and inserting
38 “section 11708(b) of title 6, United States Code”.

39 (c) TITLE 10, UNITED STATES CODE.—Section 130d of title 10, United
40 States Code, is amended by striking “section 892 of the Homeland Security
Act of 2002 (6 U.S.C. 482)” and inserting “section 11707 of title 6”.

1 (d) TITLE 16, UNITED STATES CODE.—Section 402(b)(1)(H) of the
2 Magnuson-Stevens Fishery Conservation and Management Act (16 U.S.C.
3 1881a(b)(1)(H)) is amended by striking “as defined in section 888(a)(2) of
4 the Homeland Security Act of 2002 (6 U.S.C. 468(a)(2))”.

5 (e) TITLE 19, UNITED STATES CODE.—Title 19, United States Code, is
6 amended as follows:

7 (1) Section 13031(f)(2) of Public Law 99–272 (19 U.S.C. 58c(f)(2))
8 is amended by striking “section 415 of the Homeland Security Act of
9 2002 (other than functions performed by the Office of International
10 Affairs referred to in section 415(8) of that Act),” and inserting “sec-
11 tion 10911 of title 6, United States Code (other than functions per-
12 formed by the Office of International Affairs referred to in section
13 10911(8) of title 6),”.

14 (2) Section 301(h) of Public Law 99–272 (19 U.S.C. 2075(h)) is
15 amended—

16 (A) in paragraph (1), by striking “section 412(b)(2) of the
17 Homeland Security Act of 2002 (6 U.S.C. 212(b)(2))” and “sec-
18 tion 412(b)(1) of such Act” and inserting “section 10912(b)(2) of
19 title 6, United States Code” and “section 10912(b)(1) of such
20 title”, respectively; and

21 (B) in paragraph (2)(A), by striking “section 412(b) of the
22 Homeland Security Act of 2002 (6 U.S.C. 212(b))” and inserting
23 “section 10912(b) of title 6, United States Code,”.

24 (f) TITLE 26, UNITED STATES CODE.—Section 4261(f) of the Internal
25 Revenue Code of 1986 (26 U.S.C. 4261(f)) is amended by striking “44509
26 or 44913(b)” and inserting “40923(b) of title 6, United States Code, or sec-
27 tion 44509”.

28 (g) TITLE 31, UNITED STATES CODE.—Section 3516(f)(3)(A) of title 31,
29 United States Code, is amended by striking “section 874(b)(2) of the
30 Homeland Security Act of 2002” and inserting “section 10386(b)(2) of title
31 6”.

32 (h) TITLE 33, UNITED STATES CODE.—Section 303(b)(4) of Public Law
33 105–384 (33 U.S.C. 892a(b)(4)) is amended by striking “section 641 of the
34 Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 741)”
35 and inserting “section 20501 of title 6, United States Code”.

36 (i) TITLE 38, UNITED STATES CODE.—Section 8117(a)(2)(C) of title 38,
37 United States Code, is amended by striking “section 502(6) of the Home-
38 land Security Act of 2002” and inserting “section 11103(a)(6) of title 6”.

39 (j) TITLE 42, UNITED STATES CODE.—Title 42, United States Code, is
40 amended as follows:

1 (1) Section 319F-1(a)(2)(A) of the Act of July 1, 1944 (42 U.S.C.
2 247d-6a(a)(2)(A)) is amended by striking “sections 302(2) and 304(a)
3 of the Homeland Security Act of 2002” and inserting “sections
4 10701(2) and 10703(a) of title 6, United States Code,”.

5 (2) Section 319F-2(c) of the Act of July 1, 1944 (42 U.S.C. 247d-
6 6b(c)) is amended—

7 (A) in paragraph (1)(B)(i)(I), by striking “sections 302(2) and
8 304(a) of the Homeland Security Act of 2002” and inserting “sec-
9 tions 10701(2) and 10703(a) of title 6, United States Code,”; and

10 (B) in paragraph (2)(D), by striking “section 202 of the Home-
11 land Security Act of 2002” and inserting “section 10502 of title
12 6, United States Code”.

13 (3) Section 2801(a) of the Act of July 1, 1944 (42 U.S.C. 300hh(a))
14 is amended by striking “section 502(6) of the Homeland Security Act
15 of 2002” and inserting “section 11103(6) of title 6, United States
16 Code”.

17 (4) Section 2802(a)(1) of the Act of July 1, 1944 (42 U.S.C.
18 300hh-1(a)(1)) is amended by striking “section 502(6) of the Home-
19 land Security Act of 2002” and inserting “section 11103(6) of title 6,
20 United States Code”.

21 (5) Section 1061(d) of the Intelligence Reform and Terrorism Pre-
22 vention Act of 2004 (42 U.S.C. 2000ee(d)) is amended—

23 (A) in paragraph (1)(A), by striking “subsections (d) and (f) of
24 section 1016” and inserting “section 11708(c) and (d) of title 6,
25 United States Code”;

26 (B) in paragraph (1)(B), by striking “subsections (d) and (f)
27 of section 1016” and inserting “section 11708(c) and (d) of title
28 6, United States Code”; and

29 (C) in paragraph (2)(B), by striking “subsections (d) and (f) of
30 section 1016” and inserting “section 11708(c) and (d) of title 6,
31 United States Code,”.

32 (6) Section 303(b) of the Robert T. Stafford Disaster Relief and
33 Emergency Assistance Act (42 U.S.C. 5144(b)) is amended—

34 (A) in paragraph (1)(B), by striking “section 507 of the Home-
35 land Security Act of 2002” and inserting “section 11107 of title
36 6, United States Code,”;

37 (B) in paragraph (2), by striking “section 646(a) of the Post-
38 Katrina Emergency Management Reform Act of 2006” and insert-
39 ing “section 20506(a) of title 6, United States Code”; and

1 (C) in paragraph (4), by striking “section 652(a) of the Post-
 2 Katrina Emergency Management Reform Act of 2006” and insert-
 3 ing “section 20512(a) of title 6, United States Code”.

4 (k) TITLE 46, UNITED STATES CODE.—Title 46, United States Code, is
 5 amended as follows:

6 (1) Section 70105(l) is amended by striking “section 2(1) of the
 7 SAFE Port Act” and inserting “section 30101(1) of title 6”.

8 (2) Section 70107A(b)(4) is amended—

9 (A) in subparagraph (B), by striking “section 1016 of the Na-
 10 tional Security Intelligence Reform Act of 2004 (6 U.S.C. 485)
 11 and the Homeland Security Information Sharing Act (6 U.S.C.
 12 481 et seq.)” and inserting “sections 11707 and 11708 of title 6”;
 13 and

14 (B) in subparagraph (D), by striking “section 201(b)(10) of the
 15 SAFE Port Act” and inserting “section 30501(b)(10) of title 6”.

16 (l) TITLE 49, UNITED STATES CODE.—Title 49, United States Code, is
 17 amended as follows:

18 (1) Section 40109 is amended—

19 (A) in subsection (b), by striking “, 40119, 44901, 44903,
 20 44906, and 44935–44937” and inserting “and 40119”; and

21 (B) in subsection (c), by striking “sections 44909 and” and in-
 22 serting “section”.

23 (2) Section 46110(a) is amended by striking “this part, part B, or
 24 subsection (l) or (s) of section 114” and inserting “this part or part
 25 B”.

26 (3) Chapter 463 is amended—

27 (A) in section 46301—

28 (i) in subsection (a), by striking paragraph (4) and redesign-
 29 ating paragraph (5) as paragraph (4);

30 (ii) in subsection (a)(1)(A), by striking “chapter 449 (ex-
 31 cept sections 44902, 44903(d), 44904, 44907(a)–(d)(1)(A)
 32 and (d)(1)(C)–(f), and 44908),”;

33 (iii) in subsection (a)(4)(A)(i) as redesignated by clause (i),
 34 by striking “chapter 449 (except sections 44902, 44903(d),
 35 44904, and 44907–44909), or”;

36 (iv) in subsection (c)(1)(A), by striking “chapter 423, or
 37 section 44909” and inserting “or chapter 423”; and

38 (v) in subsection (f)(1)(A)(i), by striking “chapter 449 (ex-
 39 cept sections 44902, 44903(d), 44904, 44907(a)–(d)(1)(A)
 40 and (d)(1)(C)–(f), 44908, and 44909),”;

41 (B) in section 46302—

1 (i) in subsection (a), by striking “section 46502(a), 46504,
2 46505, or 46506” and inserting “section 46504”; and

3 (ii) in subsection (b)(1), by striking “The Secretary of
4 Homeland Security and, for a violation relating to section
5 46504, the Secretary of Transportation,” and inserting “The
6 Secretary of Transportation”;

7 (C) in section 46306(d)(1), by striking “Commissioner of Cus-
8 toms” and inserting “Commissioner of U. S. Customs and Border
9 Enforcement”;

10 (D) in section 46311—

11 (i) by striking “, Under Secretary,” each place it appears;
12 and

13 (ii) in subsection (a), by striking “ the Under Secretary of
14 Transportation for Security with respect to security duties
15 and powers designated to be carried out by the Under Sec-
16 retary,”;

17 (E) in section 46313, by striking “the Under Secretary of
18 Transportation for Security with respect to security duties and
19 powers designated to be carried out by the Under Secretary or”;
20 and

21 (F) in section 46316—

22 (i) in subsection (a), by striking “the Under Secretary of
23 Transportation for Security with respect to security duties
24 and powers designated to be carried out by the Under Sec-
25 retary or”; and

26 (ii) in subsection (b), by striking “chapter 447 (except sec-
27 tion 44718(a)), and chapter 449 (except sections 44902,
28 44903(d), 44904, and 44907–44909)” and inserting “and
29 chapter 447 (except section 44718(a))”.

30 (m) TITLE 50, UNITED STATES CODE.—Title 50, United States Code,
31 is amended as follows:

32 (1) Section 1414(b) of the National Defense Authorization Act for
33 Fiscal Year 1997 (50 U.S.C. 2314(b)) is amended by striking “section
34 502(6) of the Homeland Security Act of 2002” and inserting “section
35 11103(6) of title 6, United States Code.”

36 (2) Section 1415(a)(2) of the National Defense Authorization Act for
37 Fiscal Year 1997 (50 U.S.C. 2315(a)(2)) is amended by striking “sec-
38 tions 102(c) and 430(c)(1) of the Homeland Security Act of 2002” and
39 inserting “sections 10323(b)(1) and 10331(h) of title 6, United States
40 Code”.

1 (3) Section 102A(f)(1)(B)(iii) of the Act of July 26, 1947 (50
 2 U.S.C. 3024(f)(1)(B)(iii)) is amended by striking “sections 201 and
 3 892 of the Homeland Security Act of 2002 (6 U.S.C. 121, 482)” and
 4 inserting “sections 10501 and 11707 of title 6, United States Code”.

5 **SEC. 6. TRANSITIONAL AND SAVINGS PROVISIONS.**

6 (a) DEFINITIONS.—In this section:

7 (2) RESTATED PROVISION.—The term “restated provision” means a
 8 provision of title 6, United States Code, that is enacted by section 3
 9 or 4.

10 (2) SOURCE PROVISION.—The term “source provision” means a pro-
 11 vision of law that is replaced by a restated provision.

12 (b) CUTOFF DATE.—The restated provisions replace certain provisions of
 13 law enacted on or before May 8, 2017. If a law enacted after that date
 14 amends or repeals a source provision, that law is deemed to amend or re-
 15 peal, as the case may be, the corresponding restated provision. If a law en-
 16 acted after that date is otherwise inconsistent with a restated provision or
 17 a provision of this Act, that law supersedes the restated provision or provi-
 18 sion of this Act to the extent of the inconsistency.

19 (c) ORIGINAL DATE OF ENACTMENT UNCHANGED.—A restated provision
 20 is deemed to have been enacted on the date of enactment of the cor-
 21 responding source provision.

22 (d) REFERENCE TO RESTATED PROVISION.—A reference to a restated
 23 provision is deemed to refer to the corresponding source provision.

24 (e) REFERENCE TO SOURCE PROVISION.—A reference to a source provi-
 25 sion, including a reference in a regulation, order, or other law, is deemed
 26 to refer to the corresponding restated provision.

27 (f) REGULATIONS, ORDERS, AND OTHER ADMINISTRATIVE ACTIONS.—A
 28 regulation, order, or other administrative action in effect under a source
 29 provision continues in effect under the corresponding restated provision.

30 (g) ACTIONS TAKEN AND OFFENSES COMMITTED.—An action taken or
 31 an offense committed under a source provision is deemed to have been taken
 32 or committed under the corresponding restated provision.

33 **SEC. 7. REPEALS.**

34 The following provisions of law are repealed, except with respect to the
 35 rights and duties that matured, penalties that were incurred, or proceedings
 36 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	19 U.S.C. 2073(b).
	4	19 U.S.C. 2084.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
Act of August 10, 1956 (ch. 1041)	43	6 U.S.C. 765.
Aviation and Transportation Security Act (Public Law 107-71)	109	49 U.S.C. 114 note.
	111(d)	49 U.S.C. 44935 note.
Homeland Security Act of 2002 (Public Law 107-296)	2	6 U.S.C. 101.
	3	6 U.S.C. 102.
	4	6 U.S.C. 101 note.
	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.
	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. 124l.
	210F	6 U.S.C. 124m.
	212	6 U.S.C. 131.
	213	6 U.S.C. 132.
	214	6 U.S.C. 133.
	215	6 U.S.C. 134.
	221	6 U.S.C. 141.
	222	6 U.S.C. 142.
	223	6 U.S.C. 143.
	224	6 U.S.C. 144.
	225(a) through (c)	6 U.S.C. 145(a) through (c).
	225(d)(2)	6 U.S.C. 145(d)(2).
	226	6 U.S.C. 147.
	227	6 U.S.C. 148.
	228	6 U.S.C. 149.
	228A	6 U.S.C. 149a.
	229	6 U.S.C. 150.
	230	6 U.S.C. 151.
	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. 195c.	
318	6 U.S.C. 195d.	
319	6 U.S.C. 195e.	
319	6 U.S.C. 195f.	
402	6 U.S.C. 202.	
403	6 U.S.C. 203.	
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.	
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.	
441	6 U.S.C. 251.	
442	6 U.S.C. 252.	

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	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.
	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.
	516	6 U.S.C. 321e.
	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.
	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.
	801	6 U.S.C. 361.
	821	6 U.S.C. 381.
	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.
	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.
	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.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	878	6 U.S.C. 458.
	879	6 U.S.C. 459.
	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.
	892(a) through (c)(1), (c)(3) through (g)	6 U.S.C. 482(a) through (c)(1), (c)(3) through (g).
	893	6 U.S.C. 483.
	894	6 U.S.C. 484.
	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(c)(1)(A), (2)	6 U.S.C. 511(1)(A), (2).
	1006	6 U.S.C. 512.
	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.
	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.
	1901	6 U.S.C. 591.
	1902	6 U.S.C. 592.
	1903	6 U.S.C. 593.
	1904	6 U.S.C. 594.
	1905	6 U.S.C. 595.
	1906	6 U.S.C. 596.
	1907	6 U.S.C. 596a.
	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.
	2021(a) through (e)	6 U.S.C. 611(a) through (e).
	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.
Department of Homeland Security Appropriations Act, 2004 (Public Law 108-90)	505	6 U.S.C. 453a.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	520	6 U.S.C. 469.
	(2d proviso under heading “SALARIES AND EXPENSES” under heading “FEDERAL LAW ENFORCEMENT TRAINING CENTER”, 117 Stat. 1150).	6 U.S.C. 464b.
	(3d proviso under heading “SALARIES AND EXPENSES” under heading “FEDERAL LAW ENFORCEMENT TRAINING CENTER”, 117 Stat. 1151).	6 U.S.C. 464e.
	(4th proviso under heading “SALARIES AND EXPENSES” UNDER HEADING “FEDERAL LAW ENFORCEMENT TRAINING CENTER”, 117 Stat. 1151).	6 U.S.C. 464d.
	(last proviso under heading “SALARIES AND EXPENSES” under heading “FEDERAL LAW ENFORCEMENT TRAINING CENTER”, 117 Stat. 1151).	6 U.S.C. 464e.
Department of Homeland Security Ap- propriations Act, 2005 (Public Law 108–334)	515(b)	49 U.S.C. 44945 note.
Intelligence Reform and Terrorism Pre- vention Act of 2004 (Public Law 108– 458)	1016	6 U.S.C. 485.
	4015(a)	49 U.S.C. 44935 note.
	4016	49 U.S.C. 44917 note.
	7215	6 U.S.C. 123.
	7303(a) through (e), (e) through (g), (i)(1).	6 U.S.C. 194(a) through (e), (e) through (g), (i)(1).
	7405	6 U.S.C. 112 note.
	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.
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).
	689e	6 U.S.C. 775.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	689i	6 U.S.C. 776.
	689j	6 U.S.C. 777.
	691	6 U.S.C. 791.
	692	6 U.S.C. 792.
	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 or SAFE Port Act (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.
	122	6 U.S.C. 922.
	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.
	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.
	235	6 U.S.C. 984.
	236	6 U.S.C. 985.
	301(b)	6 U.S.C. 1001.
	301(c)	6 U.S.C. 239 note.
	302(c)	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 Account- ability Appropriations Act, 2007 (Pub- lic 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.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	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	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.
	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)	526	6 U.S.C. 453c.
	538	6 U.S.C. 190 note.
	546	6 U.S.C. 124j note.
	557	6 U.S.C. 222.
	(last provision in paragraph under heading “CONSTRUCTION AND FACILITIES MANAGEMENT”, 125 Stat. 949).	6 U.S.C. 214 note.
National Defense Authorization Act for Fiscal Year 2012 (Public Law 112- 81)	1090	6 U.S.C. 121 note.
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.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
Department of Homeland Security Appropriations Act, 2013 (Public Law 113-6)	div. D, title III, last proviso on p. 359.	6 U.S.C. 763a.
	div. D, title V, § 540	6 U.S.C. 416.
Department of Homeland Security Appropriation 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 Facilities from Terrorist Attacks Act of 2014 (Public Law 113-254)	5	6 U.S.C. 621 note.
Homeland Security Cybersecurity Workforce 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. 148 note.
Intelligence Authorization Act for Fiscal Year 2015 (Public Law 113-293)	324	6 U.S.C. 125.
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.
Department of Homeland Security Interoperable Communications Act (Public Law 114-29)	2	6 U.S.C. 194 note.
	3	6 U.S.C. 194 note, 341.
	4 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. 151 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.
Trade Facilitation and Trade Enforcement Act of 2015 (Public Law 114-125)	title VIII, § 802(j)	8 U.S.C. 1185 note.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
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 Code

Title	Section
49	114
.....	115
.....	44901
.....	44902
.....	44903
.....	44904
.....	44905
.....	44906
.....	44907
.....	44908
.....	44909
.....	44910
.....	44911
.....	44912
.....	44913
.....	44914
.....	44915
.....	44916
.....	44917
.....	44918
.....	44919
.....	44920
.....	44921
.....	44922
.....	44923
.....	44924
.....	44925
.....	44926
.....	44927
.....	44928
.....	44933
.....	44934
.....	44935
.....	44936
.....	44937
.....	44938
.....	44939
.....	44940
.....	44941
.....	44942
.....	44943
.....	44944
.....	44945
.....	44946

