Original Signature of Member

118TH CONGRESS
1ST SESSION

H.R. _____

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

IN THE HOUSE OF REPRESENTATIVES

——— —, 2023

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

A BILL

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

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

SECTION 1. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

SEC. 2. PURPOSES; CONFORMITY WITH ORIGINAL INTENT.

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

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

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

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

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

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

TITLE 6—DOMESTIC SECURITY

Subtitle I—Homeland Security Organization

Subtitle I—Homeland Security Organization
Chapter 101—General

§ 10101. Definitions

In this subtitle:

(1) AMERICAN HOMELAND; HOMELAND.—Each of the terms ''American homeland'' and ''homeland'' means the United States.

(2) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term ''appropriate congressional committee'' means a committee of the House of Representatives or the Senate having legislative or oversight jurisdiction under the Rules of the House of Representatives or the Senate, respectively, over the matter concerned.

(3) ASSETS.—The term ''assets'' includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).

(4) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given the term in subsection (e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c(e)).

(5) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(6) EMERGENCY RESPONSE PROVIDERS.—The term ''emergency response providers'' includes Federal, State, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.

(7) EMP.—The term ''EMP'' means an electromagnetic pulse caused by a nuclear device or nonnuclear device, including an electromagnetic pulse caused by an act of terrorism.

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

(9) FUNCTIONS.—The term ''functions'' includes authorities, powers, rights, privileges, immunities, programs, projects, activities, duties, and responsibilities.

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

(11) INTELLIGENCE COMPONENT OF THE DEPARTMENT.—The term ''intelligence component of the Department'' means an element or entity of the Department that collects, gathers, processes, analyzes, produces, or disseminates intelligence information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence (as defined under section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), except—

(A) the United States Secret Service; and

(B) the Coast Guard, when operating under the direct authority of the Secretary of Defense or Secretary of the Navy under section 103 of title 14, except that nothing in this paragraph shall affect or diminish the authority and responsibilities of the Commandant of the Coast Guard to command or control the Coast Guard as an armed force or the authority of the Director of National Intelligence with respect to the Coast Guard as an element of the intelligence community (as defined under section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

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

(13) LOCAL GOVERNMENT.—The term ''local government'' means—

(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

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

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

(14) MAJOR DISASTER.—The term ''major disaster'' has the meaning given the term in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(15) PERSONNEL.—The term ''personnel'' means officers and employees.

(16) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(17) STATE.—The term ''State'' means a State, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, or a possession of the United States.

(18) TERRORISM.—The term ''terrorism'' means an activity that—

(A) involves an act that—

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

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

(B) appears to be intended—

(i) to intimidate or coerce a civilian population;

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

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

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

(20) VOLUNTARY PREPAREDNESS STANDARDS.—The term ''voluntary preparedness standards'' means a common set of criteria for preparedness, disaster management, emergency management, and business continuity programs, such as the American National Standards Institute's National Fire Protection Association Standard on Continuity, Emergency, and Crisis Management (ANSI/NFPA 1600).

§ 10102. Construction; relationship to other laws

(a) CONSTRUCTION; SEVERABILITY.—A provision of this subtitle held to be invalid or unenforceable by its terms, or as applied to a person or circumstance, shall be construed so as to give it the maximum effect permitted by law, unless the holding shall be one of utter invalidity or unenforceability, in which event the provision shall be deemed severable from this subtitle and shall not affect the remainder of the subtitle, or the application of the provision to other persons not similarly situated or to other, dissimilar circumstances.

(b) RELATIONSHIP TO OTHER LAWS.—

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

(2) ATOMIC ENERGY ACT OF 1954.—Nothing in this subtitle shall supersede any requirement made by or under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted data or formerly restricted data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

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

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

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

Chapter 103—Department of Homeland Security

Subchapter I—Organization

§ 10301. Establishment; mission; seal

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

(b) MISSION.—

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

(A) prevent terrorist attacks within the United States;

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

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

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

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

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

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

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

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

not in the Department, but rather in Federal, State, and local law enforcement agencies with jurisdiction over the acts in question.

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

§ 10302. Secretary and other officers

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

(b) DEPUTY SECRETARY, UNDER SECRETARIES, ADMINISTRATOR, DIRECTORS, ASSISTANT SECRETARIES, AND GENERAL COUNSEL.—

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

(A) Deputy Secretary of Homeland Security, who shall be the Secretary's first assistant for purposes of subchapter III of chapter 33 of title 5.

(B) Under Secretary for Science and Technology.

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

(D) Administrator of the Federal Emergency Management Agency.

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

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

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

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

(I) Not more than 12 Assistant Secretaries.

(J) General Counsel, who is the chief legal officer of the Department.

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

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

(c) INSPECTOR GENERAL.—There is in the Department the Office of Inspector General and an Inspector General at the head of the office, as provided in chapter 4 of title 5.

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

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

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

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

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

(1) Director of the Secret Service.

(2) Chief Information Officer.

(3) Officer for Civil Rights and Civil Liberties.

(4) Assistant Secretary for the Countering Weapons of Mass Destruction Office.

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

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

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

(A) UNDER SECRETARY FOR MANAGEMENT TO SERVE AS ACTING SECRETARY.—Notwithstanding chapter 33 of title 5, the Under Secretary for Management shall serve as the Acting Secretary if by reason of absence, disability, or vacancy in office, neither the Secretary nor the Deputy Secretary is available to exercise the duties of the Secretary.

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

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

§ 10303. Office of Intelligence and Analysis

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

with the advice and consent of the Senate, and serves as the Chief Intelligence Officer of the Department.

(b) HOMELAND SECURITY INTELLIGENCE PROGRAM.—The Homeland Security Intelligence Program in the Department coordinates the intelligence activities of the Office of Intelligence and Analysis that serve predominantly department missions.

§ 10304. Cybersecurity and Infrastructure Security Agency

(a) IN GENERAL.—There is in the Department the Cybersecurity and Infrastructure Security Agency (in this section referred to as the ''Agency''). Any reference to the National Protection and Programs Directorate of the Department in a law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Agency.

(b) DIRECTOR.—

(1) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency (in this section referred to as the ''Director'') is the head of the Agency. The Director reports to the Secretary.

(2) QUALIFICATIONS.—

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

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

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

(B) SPECIFIED AREAS.—The areas specified in this subparagraph are the following:

(i) Cybersecurity.

(ii) Infrastructure security.

(iii) Security risk management.

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

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

(c) DEPUTY DIRECTOR.—The Agency has a Deputy Director of Cybersecurity and Infrastructure Security who shall—

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

(2) report to the Director.

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

(e) CYBERSECURITY DIVISION.—

(1) IN GENERAL.—There is in the Agency the Cybersecurity Division.

(2) EXECUTIVE ASSISTANT DIRECTOR.—The Executive Assistant Director for Cybersecurity is the head of the Cybersecurity Division. The Executive Assistant Director for Cybersecurity shall—

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

(B) be appointed by the President without the advice and consent of the Senate; and

(C) report to the Director.

(3) REFERENCE.—Any reference to the Assistant Secretary for Cybersecurity and Communications or Assistant Secretary for Cybersecurity in a law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Executive Assistant Director for Cybersecurity.

(f) INFRASTRUCTURE SECURITY DIVISION.—

(1) IN GENERAL.—There is in the Agency the Infrastructure Security Division.

(2) EXECUTIVE ASSISTANT DIRECTOR.—The Executive Assistant Director for Infrastructure Security is the head of the Infrastructure Security Division. The Executive Assistant Director for Infrastructure Security shall—

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

(B) be appointed by the President without the advice and consent of the Senate; and

(C) report to the Director.

(3) REFERENCE.—Any reference to the Assistant Secretary for Infrastructure Protection or Assistant Secretary for Infrastructure Security in a law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Executive Assistant Director for Infrastructure Security.

(g) EMERGENCY COMMUNICATIONS DIVISION.—

(1) IN GENERAL.—There is in the Agency the Emergency Communications Division.

(2) EXECUTIVE ASSISTANT DIRECTOR.—

(A) IN GENERAL.—The Executive Assistant Director for Emergency Communications (in this subsection referred to as the ''Executive Assistant Director'') is the head of the Emergency Communications Division. The Executive Assistant Director shall report directly to the Director. All decisions of the Executive Assistant Director that entail the exercise of significant authority shall be subject to the approval of the Director.

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

(h) NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.—There is in the Agency the National Cybersecurity and Communications Integration Center to carry out certain responsibilities of the Director. The head of the National Cybersecurity and Communications Integration Center shall report to the Executive Assistant Director for Cybersecurity.

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

(j) JOINT CYBER PLANNING OFFICE.—

(1) DEFINITION OF CYBER DEFENSE OPERATION.—In this subsection, the term ''cyber defense operation'' means defensive activities performed for a cybersecurity purpose.

(2) IN GENERAL.—There is in the Agency an office for joint cyber planning (in this subsection referred to as the ''Office'') to develop, for public- and private-sector entities, plans for cyber defense operations, including the development of a set of coordinated actions to protect, detect, respond to, and recover from cybersecurity risks or incidents or limit, mitigate, or defend against coordinated, malicious cyber operations that pose a potential risk to critical infrastructure or national interests.

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

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

(A) a central planning staff; and

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

(i) the Department;

(ii) United States Cyber Command;

(iii) the National Security Agency;

(iv) the Federal Bureau of Investigation;

(v) the Department of Justice; and

(vi) the Office of the Director of National Intelligence.

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

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

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

(C) ensure that plans for cyber defense operations are, to the greatest extent practicable, developed in collaboration with relevant private-sector entities, particularly in areas in which the entities have comparative advantages in limiting, mitigating, or defending against a cybersecurity risk or incident or coordinated, malicious cyber operation;

(D) ensure that plans for cyber defense operations, as appropriate, are responsive to potential adversary activity conducted in response to United States offensive cyber operations;

(E) facilitate the exercise of plans for cyber defense operations, including by developing and modeling scenarios based on an understanding of adversary threats to, vulnerability of, and potential consequences of disruption or compromise of critical infrastructure;

(F) coordinate with and, as necessary, support relevant Federal departments and agencies in the establishment of procedures, development of additional plans, including for offensive and intelligence activities in support of cyber defense operations, and creation of agreements necessary for the rapid execution of plans for cyber defense operations when a cybersecurity risk or incident or malicious cyber operation has been identified; and

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

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

(A) State, local, federally recognized Tribal, and territorial governments;

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

(C) owners and operators of critical information systems;

(D) private entities; and

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

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

(k) CYBERSECURITY ADVISORY COMMITTEE

(1) IN GENERAL.—There is in the Agency the Cybersecurity Advisory Committee, established by the Secretary.

(2) MEMBERSHIP.—

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

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

(i) Consist of subject matter experts.

(ii) Be geographically balanced.

(iii) Include representatives of State, local, and Tribal governments and of a broad range of industries, which may include the following:

(I) Defense.

(II) Education.

(III) Financial services and insurance.

(IV) Healthcare.

(V) Manufacturing.

(VI) Media and entertainment.

(VII) Chemicals.

(VIII) Retail.

(IX) Transportation.

(X) Energy.

(XI) Information technology.

(XII) Communications.

(XIII) Other relevant fields identified by the Director.

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

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

(E) TERM OF OFFICE.—

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

(ii) REAPPOINTMENT.—A member of the Cybersecurity Advisory Committee may be reappointed for an unlimited number of terms.

(iii) REMOVAL.—The Director may review the participation of a member of the Cybersecurity Advisory Committee and at any time remove the member at the discretion of the Director.

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

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

(i) a member to serve as chairperson of the Cyersecurity Advisory Committee; and

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

(H) MEETINGS.—

(i) IN GENERAL.—The Director shall require the Cybersecurity Advisory Committee to meet not less frequently than semiannually, and may convene additional meetings as necessary.

(ii) PUBLIC MEETINGS.—At least one of the meetings referred to in clause (i) shall be open to the public.

(iii) ATTENDANCE.—The Cybersecurity Advisory Committee shall maintain a record of the individuals present at each meeting.

(I) ACCESS TO CLASSIFIED INFORMATION.—

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

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

(iii) PROTECTING INFORMATION.—A member of the Cybersecurity Advisory Committee shall protect all classified information in accordance with the applicable requirements for the particular level of classification of the information.

(iv) RULE OF CONSTRUCTION.—Nothing in this subparagraph shall be construed to affect the security clearance of a member of the Cybersecurity Advisory Committee or the authority of a Federal agency to provide a member of the Cybersecurity Advisory Committee access to classified information.

(3) DUTIES.—

(A) IN GENERAL.—The Cybersecurity Advisory Committee shall advise, consult with, report to, and make recommendations to the Director, as appropriate, on the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

(B) RECOMMENDATIONS.—

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

(ii) RECOMMENDATIONS OF SUBCOMMITTEES.—Recommendations agreed on by subcommittees established under paragraph (4) for any year shall be approved by the Cybersecurity Advisory Committee before the Cybersecurity Advisory Committee submits to the Director the annual report under subparagraph (D) for that year.

(C) PERIODIC REPORTS.—The Cybersecurity Advisory Committee shall periodically submit to the Director—

(i) reports on matters identified by the Director; and

(ii) reports on other matters identified by a majority of the members of the Cybersecurity Advisory Committee.

(D) ANNUAL REPORT.—

(i) IN GENERAL.—The Cybersecurity Advisory Committee shall submit to the Director an annual report providing information on the activities, findings, and recommendations of the Cybersecurity Advisory Committee, including its subcommittees, for the preceding year.

(ii) PUBLICATION.—Not later than 180 days after the date on which the Director receives an annual report for a year under clause (i), the Director shall publish a public version of the report describing the activities of the Cybersecurity Advisory Committee and such related matters as would be informative to the public during that year, consistent with section 552(b) of title 5.

(E) FEEDBACK.—Not later than 90 days after receiving any recommendation submitted by the Cybersecurity Advisory Committee under subparagraph (B), (C), or (D), the Director shall respond in writing to the Cybersecurity Advisory Committee with feedback on the recommendation. The response shall include—

(i) with respect to a recommendation with which the Director concurs, an action plan to implement the recommendation; and

(ii) with respect to a recommendation with which the Director does not concur, a justification for why the Director does not plan to implement the recommendation.

(F) CONGRESSIONAL NOTIFICATION.—Not less frequently than once per year after January 1, 2021, the Director shall provide to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security, the Committee on Energy and Commerce, and the Committee on Appropriations of the House of Representatives a briefing on feedback from the Cybersecurity Advisory Committee.

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

(4) SUBCOMMITTEES.—

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

(i) Information exchange.

(ii) Critical infrastructure.

(iii) Risk management.

(iv) Public and private partnerships.

(B) MEETINGS AND REPORTING.—Each subcommittee shall meet not less frequently than semiannually, and submit to the Cybersecurity Advisory Committee for inclusion in the annual report required under paragraph (3)(D) information, including activities, findings, and recommendations, regarding subject matter considered by the subcommittee.

(C) QUALIFICATION OF MEMBERS.—The chairperson of the Cybersecurity Advisory Committee shall appoint members to subcommittees and shall ensure that each member appointed to a subcommittee has subject matter expertise relevant to the subject matter of the subcommittee.

(l) CYBERSECURITY EDUCATION AND TRAINING PROGRAMS

(1) IN GENERAL.—There is in the Agency the Cybersecurity Education and Training Assistance Program (in this subsection referred to as ''CETAP'').

(2) PURPOSE.—The purpose of CETAP shall be to support the effort of the Agency in building and strengthening a national cybersecurity workforce pipeline capacity through enabling elementary and secondary cybersecurity education, including by—

(A) providing foundational cybersecurity awareness and literacy;

(B) encouraging cybersecurity career exploration; and

(C) supporting the teaching of cybersecurity skills at the elementary and secondary education levels.

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

(A) ensure that the program—

(i) creates and disseminates cybersecurity-focused curricula and career awareness materials appropriate for use at the elementary and secondary education levels;

(ii) conducts professional development sessions for teachers;

(iii) develops resources for the teaching of cybersecurity-focused curricula described in clause (i);

(iv) provides direct student engagement opportunities through camps and other programming;

(v) engages with State educational agencies and local educational agencies to promote awareness of the program and ensure that offerings align with State and local curricula;

(vi) integrates with existing post-secondary education and workforce development programs at the Department;

(vii) promotes and supports national standards for elementary and secondary cyber education;

(viii) partners with cybersecurity and education stakeholder groups to expand outreach; and

(ix) engages in any other activity the Director determines necessary to meet the purpose described in paragraph (2); and

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

(4) BRIEFINGS.—

(A) IN GENERAL.—Not later than 1 year after the establishment of CETAP, and annually thereafter, the Secretary shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on the program.

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

(i) estimated figures on the number of students reached and teachers engaged;

(ii) information on outreach and engagement efforts, including the activities described in paragraph (3)(A)(v);

(iii) information on any grants or cooperative agreements made pursuant to paragraph (6), including how any of the grants or cooperative agreements are being used to enhance cybersecurity education for underserved populations or communities;

(iv) information on new curricula offerings and teacher training platforms; and

(v) information on coordination with post-secondary education and workforce development programs at the Department.

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

(6) GRANTS AND COOPERATIVE AGREEMENTS.—The Director may award financial assistance in the form of grants or cooperative agreements to States, local governments, institutions of higher education (as the term is defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)), nonprofit organizations, and other non-Federal entities as determined appropriate by the Director for the purpose of funding cybersecurity and infrastructure security education and training programs and initiatives to—

(A) carry out the purposes of CETAP; and

(B) enhance CETAP to address the national shortfall of cybersecurity professionals.

(m) INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING INITIATIVE

(1) IN GENERAL.—

(A) ESTABLISHMMENT.—There is in the Agency the Industrial Control Systems Cybersecurity Training Initiative (in this subsection referred to as the ''Initiative'').

(B) PURPOSE.—The purpose of the Initiative is to develop and strengthen the skills of the cybersecurity workforce related to securing industrial control systems.

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

(A) ensure the Initiative includes—

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

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

(iii) trainings and courses that cover cyber defense strategies for industrial control systems, including an understanding of the unique cyber threats facing industrial control systems and the mitigation of security vulnerabilities in industrial controlssystems technology; and

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

(B) engage in—

(i) collaboration with the national laboratories of the Department of Energy in accordance with section 1908 of this title;

(ii) consultation with Sector Risk Management Agencies; and

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

(C) consult, to the maximum extent practicable, with commercial training providers and academia to minimize the potential for duplication of other training opportunities.

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

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

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

(C) The number of participants in each course.

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

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

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

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

§ 10305. Directorate of Science and Technology

There is in the Department the Directorate of Science and Technology. The Under Secretary for Science and Technology is the head of the Directorate.

§ 10306. U.S. Customs and Border Protection

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

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

(c) COMMISSIONER.—

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

ferred to as the ''Commissioner'') is the head of U.S. Customs and Border Protection.

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

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

(e) U.S. BORDER PATROL.—

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

(2) CHIEF.–The Chief of the U.S. Border Patrol is the head of the U.S. Border Patrol. The Chief of the U.S. Border Patrol shall report to the Commissioner.

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

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

(B) deter and prevent illegal entry of terrorists, terrorist weapons, persons, and contraband; and

(C) carry out other duties and powers prescribed by the Commissioner.

(f) OFFICE OF AIR AND MARINE OPERATIONS.—

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

(2) ASSISTANT COMMISSIONER.—An Assistant Commissioner is the head of the Office of Air and Marine Operations. The Assistant Commissioner shall report to the Commissioner.

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

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

(B) conduct joint aviation and marine operations with U.S. Immigration and Customs Enforcement;

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

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

(E) carry out other duties and powers the Commissioner prescribes.

(4) AIR AND MARINE OPERATIONS CENTER.—

(A) IN GENERAL.—There is in the Office of Air and Marine Operations an Air and Marine Operations Center.

(B) EXECUTIVE DIRECTOR.—The Executive Director is the head of the Air and Marine Operations Center. The Executive Director shall report to the Assistant Commissioner of the Office of Air and Marine Operations.

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

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

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

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

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

(v) carry out other duties and powers prescribed by the Assistant Commissioner.

(g) OFFICE OF FIELD OPERATIONS.—

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

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

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

(A) deter and prevent terrorists and terrorist weapons from entering the United States at those ports of entry;

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

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

(D) in coordination with the Commissioner, facilitate and expedite the flow of legitimate travelers and trade;

(E) administer the National Targeting Center;

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

(G) carry out other duties and powers the Commissioner prescribes.

(4) NATIONAL TARGETING CENTER.—

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

(B) EXECUTIVE DIRECTOR.—An Executive Director is the head of the National Targeting Center. The Executive Director shall report to the Executive Assistant Commissioner of the Office of Field Operations.

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

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

(ii) identify, review, and target travelers and cargo for examination;

(iii) coordinate the examination of entry and exit of travelers and cargo;

(iv) develop and conduct commercial risk assessment targeting with respect to cargo destined for the United States;

(v) coordinate with the Transportation Security Administration, as appropriate;

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

(vii) carry out other duties and powers the Executive Assistant Commissioner prescribes.

(5) ANNUAL REPORT ON STAFFING.—

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

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

sistant Commissioner determines that a classified form is appropriate and informs the Committee on Homeland Security and the Committee on Ways and Means of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Finance of the Senate of the reasoning for a classified report.

(h) OFFICE OF INTELLIGENCE.—

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

(2) ASSISTANT COMMISSIONER.—An Assistant Commissioner is the head of the Office of Intelligence. The Assistant Commissioner shall report to the Commissioner.

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

(A) develop, provide, coordinate, and implement intelligence capabilities into a cohesive intelligence enterprise to support the execution of the duties and responsibilities of U.S. Customs and Border Protection;

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

(C) establish, in coordination with the Chief Intelligence Officer of the Department, as appropriate, intelligence-sharing relationships with Federal, State, local, and tribal agencies and intelligence agencies;

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

(E) carry out other duties and powers the Commissioner prescribes.

(i) OFFICE OF INTERNATIONAL AFFAIRS.—

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

(2) ASSISTANT COMMISSIONER.—An Assistant Commissioner is the head of the Office of International Affairs. The Assistant Commissioner shall report to the Commissioner.

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

(A) coordinate and support U.S. Customs and Border Protection's foreign initiatives, policies, programs, and activities;

(B) coordinate and support U.S. Customs and Border Protection's personnel stationed abroad;

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

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

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

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

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

(G) coordinate U.S. Customs and Border Protection's engagement in international negotiations;

(H) advise the Commissioner with respect to matters arising in the World Customs Organization and other international organizations on matters relating to the policies and procedures of U.S. Customs and Border Protection;

(I) advise the Commissioner regarding international agreements to which the United States is a party as the agreements relate to the policies and procedures of U.S. Customs and Border Protection; and

(J) carry out other duties and powers the Commissioner prescribes.

(j) OFFICE OF PROFESSIONAL RESPONSIBILITY.—

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

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

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

(A) investigate criminal and administrative matters and misconduct by officers, agents, and other employees of U.S. Customs and Border Protection;

(B) manage integrity-related programs and policies of U.S. Customs and Border Protection;

(C) conduct research and analysis regarding misconduct of officers, agents, and other employees of U.S. Customs and Border Protection; and

(D) carry out other duties and powers the Commissioner prescribes.

(k) OFFICE OF TRADE.—

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

tion'' have the meanings given the terms in section 2 of the Trade Facilitation and Trade Enforcement Act of 2015 (19 U.S.C. 4301).

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

(3) EXECUTIVE ASSISTANT COMMISSIONER.—An Executive Assistant Commissioner is the head of the Office of Trade. The Executive Assistant Commissioner shall report to the Commissioner.

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

(A) direct the development and implementation, pursuant to the customs and trade laws of the United States, of policies and regulations administered by U.S. Customs and Border Protection;

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

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

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

(E) otherwise advise the Commissioner with respect to the development and implementation of the joint strategic plan;

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

(G) oversee the trade modernization activities of U.S. Customs and Border Protection, including the development and implementation of the Automated Commercial Environment computer system authorized under section 13031(f)(5) of the Consolidated Omnibus Budget and Reconciliation Act of 1985 (19 U.S.C. 58c(f)(5)) and support for the establishment of the International Trade Data System under the oversight of the Department of Treasury pursuant to section 411(d) of the Tariff Act of 1930 (19 U.S.C. 1411(d));

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

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

(i) a summary of the changes to customs policies and regulations adopted by U.S. Customs and Border Protection during the preceding calendar year; and

(ii) a description of the public vetting and interagency consultation that occurred with respect to each change.

(5) TRANSFER OF ASSETS, FUNCTIONS, AND PERSONNEL.—The Commissioner may transfer any assets, functions, or personnel in U.S. Customs and Border Protection to the Office of Trade. Not less than 90 days prior to the transfer, the Commissioner shall notify the Committee on Finance of the Senate, the Committee on Homeland Security and Government Affairs of the Senate, the Committee on Ways and Means of the House of Representatives, and the Committee on Homeland Security of the House of Representatives of the specific assets, functions, or personnel to be transferred, and the reason for the transfer.

(l) OTHER AUTHORITIES.—

(1) IN GENERAL.–The Secretary may establish such other offices or positions of Assistant Commissioners (or other similar officers or officials) as the Secretary determines necessary to carry out the missions, duties, functions, and authorities of U.S. Customs and Border Protection.

(2) NOTIFICATION.—If the Secretary exercises the authority provided under paragraph (1), the Secretary shall notify the Committee on Homeland Security of the House of Representative and the Committee on Homeland Security and Governmental Affairs of the Senate not later than 30 days before exercising the authority

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

(n) AUTHORITY OF OTHER FEDERAL AGENCIES NOT AFFECTED.—Nothing in subsections (a) through (j), (l), and (m) may be construed as affecting in any manner the authority, existing on February 23, 2016, of any other Federal agency or component of the Department.

§ 10307. U.S. Immigration and Customs Enforcement

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

§ 10308. U.S. Citizenship and Immigration Services

There is in the Department an agency known as U.S. Citizenship and Immigration Services. The Director of U.S. Citizenship and Immigration Services is the head of U.S. Citizenship and Immigration Services. The Director of U.S. Citizenship and Immigration Services reports directly to the Deputy Secretary of Homeland Security, shall have a minimum of 5 years of management experience, and shall be paid at the same level as the Director of U.S. Immigration and Customs Enforcement.

§ 10309. Federal Emergency Management Agency

(a) ESTABLISHMENT.—There is in the Department the Federal Emergency Management Agency. The Federal Emergency Management Agency is a distinct entity in the Department.

(b) ADMINISTRATOR.—The Administrator of the Federal Emergency Management Agency is the head of the Agency. The Administrator shall be appointed by the President, by and with the advice and consent of the Senate, from among individuals who have—

(1) a demonstrated ability in and knowledge of emergency management and homeland security; and

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

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

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

§ 10310. Transportation Security Administration

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

(b) ADMINISTRATOR.—

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

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

(2) TERM.—The term of office of an individual appointed as the Administrator is 5 years.

(3) LIMITATION ON OWNERSHIP OF STOCKS AND BONDS.—The Administrator may not own stock in or bonds of a transportation or security enterprise or an enterprise that makes equipment that could be used for security purposes.

(c) DEPUTY ADMINISTRATOR.—

(1) IN GENERAL.—There is in the Transportation Security Administration a Deputy Administrator, who shall assist the Administrator in the management of the Transportation Security Administration. The Deputy Administrator shall be appointed by the President. The Deputy Administrator shall be a citizen of the United States and have experience in a field directly related to transportation or security.

(2) ACTING ADMINISTRATOR.—The Deputy Administrator shall be Acting Administrator during the absence or incapacity of the Administrator or during a vacancy in the office of Administrator.

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

(e) AIR CARGO SECURITY DIVISION.—

(1) ESTABLISHMENT.—The Administrator shall establish an air cargo security division to carry out and engage with stakeholders regarding the implementation of air cargo security programs established by the Transportation Security Administration.

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

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

(f) NATIONAL DEPLOYMENT OFFICE.—

(1) ESTABLISHMENT.—There is in the Transportation Security Administration a National Deployment Office. An individual with supervisory experience is the head of the National Deployment Office. The Administrator shall designate the individual.

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

(A) Maintaining a National Deployment Force in the Transportation Security Administration, including transportation security officers, supervisory transportation security officers, and lead transportation security officers, to provide the Transportation Security Administration with rapid and efficient response capabilities and augment the Department's homeland security operations to mitigate and reduce risk, including for the following:

(i) Airports temporarily requiring additional security personnel due to an emergency, seasonal demands, hiring shortfalls, severe weather conditions, passenger volume mitigation, equipment support, or other reasons.

(ii) Special events requiring enhanced security, including National Special Security Events, as determined by the Secretary.

(iii) Response in the aftermath of a manmade disaster, including a terrorist attack.

(iv) Other similar situations, as determined by the Administrator.

(B) Educating transportation security officers regarding how to participate in the Transportation Security Administration's National Deployment Force.

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

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

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

(3) CAREER DEVELOPMENT.—The Administrator may consider service in the National Deployment Force as a positive factor when evaluating applicants for promotion in the Transportation Security Administration.

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

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

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

(B) be responsible and accountable for that area.

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

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

(i) airport checkpoint and baggage screening operations;

(ii) workforce training and development programs; and

(iii) ensuring compliance with aviation security law, including regulations, and other specialized programs designed to secure air transportation.

(B) Surface transportation security operations and training, including risk-based, adaptive security focused on—

(i) accomplishing security systems assessments;

(ii) reviewing and prioritizing projects for appropriated surface transportation security grants;

(iii) operator compliance with surface transportation security law, including regulations, and voluntary industry standards; and

(iv) workforce training and development programs, and other specialized programs designed to secure surface transportation.

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

(D) International strategy and operations, including agency efforts to work with international partners to secure the global transportation network.

(E) Trusted and registered traveler programs, including the management and marketing of the agency's trusted traveler initiatives, including the PreCheck Program, and coordination with trusted traveler programs of other Department agencies and the private sector.

(F) Technology acquisition and deployment, including the oversight, development, testing, evaluation, acquisition, deployment,

and maintenance of security technology and other acquisition programs.

(G) Inspection and compliance, including the integrity, efficiency, and effectiveness of the agency's workforce, operations, and programs through objective audits, covert testing, inspections, criminal investigations, and regulatory compliance.

(H) Civil rights, liberties, and traveler engagement, including ensuring that agency employees and the traveling public are treated in a fair and lawful manner consistent with Federal laws and regulations protecting privacy and prohibiting discrimination and reprisal.

(I) Legislative and public affairs, including communication and engagement with internal and external audiences in a timely, accurate, and transparent manner, and development and implementation of strategies in the agency to achieve congressional approval or authorization of agency programs and policies.

(3) NOTIFICATION.—The Administrator shall submit to the appropriate committees of Congress—

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

(B) an update of the list not later than 5 days after a new individual is appointed under paragraph (1).

§ 10311. United States Secret Service

(a) IN GENERAL.—The United States Secret Service (in this section referred to as the ''Secret Service'') is a distinct entity in the Department. The Secretary succeeds to the functions, personnel, assets, and obligations of the Secret Service, including the functions of the Secretary of the Treasury relating to the Secret Service.

(b) NATIONAL COMPUTER FORENSICS INSTITUTE.—

(1) DEFINITIONS.—In this subsection:

(A) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given that term in section 10781 of this title.

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

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

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

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

(3) CURRICULUM.—In furtherance of paragraph (2), all education and training of the Institute shall be conducted in accordance with relevant Federal law regarding privacy, civil rights, and civil liberties protections. Education and training provided pursuant to paragrah (2) shall relate to the following:

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

(B) Conducting forensic examinations of computers, mobile devices, and other information systems.

(C) Prosecutorial and judicial considerations related to cybersecurity incidents, electronic crimes, related cybersecurity threats, and forensic examinations of computers, mobile devices, and other information systems.

(D) Methods to obtain, process, store, and admit digital evidence in court.

(4) PRINCIPLES.—In carrying out the functions specified in subsection (b), the Institute shall ensure, to the extent practicable, that timely, actionable, and relevant expertise and information related to cybersecurity incidents, electronic crimes, and related cybersecurity threats is shared with recipients of education and training provided pursuant to paragraph (2). When selecting participants for the training, the Institute shall prioritize, to the extent reasonable and practicable, providing education and training to individuals from geographically-diverse jurisdictions throughout the United States, and the Institute shall prioritize, to the extent reasonable and practicable, State, local, tribal, and territorial law enforcement officers, prosecutors, judges, and other employees.

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

and preventing cybersecurity incidents, electronic crimes, and related cybersecurity threats, and for forensic examinations of computers, mobile devices, and other information systems.

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

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

(8) Annual reports to congress.—

(A) IN GENERAL.— The Secretary shall include in the annual report required undersection 1116 of title 31information regarding the activities of the Institute, including, where possible, the following:

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

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

(iii) Any information regarding projected future demand for the education and training provided pursuant to paragraph (2).

(iv) Impacts of the activities of the Institute on the capability of jurisdictions to investigate and prevent cybersecurity incidents, electronic crimes, and related cybersecurity threats.

(v) A description of the nomination process for potential recipients of the information and training provided pursuant to paragraph (2).

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

(B) EXCEPTION.— Any information required under subparagraph (A) that is submitted as part of the annual budget submitted by the President to Congress undersection 1105 of title 31is not required to be included in the report required under subparagraph (A).

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

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

(1) IN GENERAL.—With respect to any undercover investigative operation of the Secret Service that is necessary for the detection and prosecution of crimes against the United States—

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

(B) sums appropriated for the Secret Service, including unobligated balances available from prior fiscal years, may be used to establish or to acquire proprietary corporations or business entities as part of the undercover operation, and to operate the corporations or business entities on a commercial basis, without regard to sections 9102 and 9103 of title 31;

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

(D) proceeds from the undercover operation may be used to offset necessary and reasonable expenses incurred in the operation, without regard to section 3302 of title 31.

(2) WRITTEN CERTIFICATION.—The authority set forth in paragraph (1) may be exercised only on the written certification of the Director of the Secret Service or designee that any action authorized by any subparagraph of paragraph (1) is necessary for the conduct of an undercover investigative operation. The certification shall continue in effect for the duration of the operation, without regard to fiscal years.

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

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

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

(5) FINANCIAL AUDITS AND REPORTS.—

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

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

§ 10312. Coast Guard

(a) IN GENERAL.—The Coast Guard is a distinct entity in the Department. The Commandant reports directly to the Secretary without being required to report through any other official of the Department.

(b) TRANSFER.—

(1) IN GENERAL.—The authorities, functions, personnel, and assets of the Coast Guard, including the authorities and functions of the Secretary of Transportation relating to the Coast Guard, are transferred to the Secretary. Notwithstanding this subtitle, the authorities, functions, and capabilities of the Coast Guard to perform its missions shall be maintained intact and without significant reduction, except as specified in Acts subsequent to the Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2135).

(2) CERTAIN TRANSFERS PROHIBITED.—No mission, function, or asset (including for purposes of this paragraph a ship, aircraft, or helicopter) of the Coast Guard may be diverted to the principal and continuing use of another organization, unit, or entity of the Department, except for details or assignments that do not reduce the Coast Guard's capability to perform its missions.

(c) CHANGES TO MISSIONS.—

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

quent to the Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2135).

(2) WAIVER.—The Secretary may waive the restrictions under paragraph (1) for a period of not to exceed 90 days upon a declaration and certification by the Secretary to Congress that a clear, compelling, and immediate need exists for a waiver. A certification under this paragraph shall include a detailed justification for the declaration and certification, including the reasons and specific information that demonstrate that the Nation and the Coast Guard cannot respond effectively if the restrictions under paragraph (1) are not waived.

(d) NONAPPLICABILITY TO OPERATION AS A SERVICE IN THE NAVY.—None of the conditions and restrictions in this section shall apply when the Coast Guard operates as a service in the Navy under section 103 of title 14.

§ 10313. Office for State and Local Government Coordination

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

§ 10314. Countering Weapons of Mass Destruction Office

(a) DEFINITIONS.—In this section:

(1) ASSISTANT SECRETARY.—The term ''Assistant Secretary'' means the Assistant Secretary for the Countering Weapons of Mass Destruction Office.

(2) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(3) OFFICE.—The term ''Office'' means the Countering Weapons of Mass Destruction Office.

(4) WEAPON OF MASS DESTRUCTION.—The term ''weapon of mass destruction'' has the meaning given the term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) IN GENERAL.—There is in the Department the Countering Weapons of Mass Destruction Office. The Assistant Secretary for the Countering Weapons of Mass Destruction Office is the head of the Office. The Assistant Secretary is appointed by the President.

(c) CHIEF MEDICAL OFFICER.—There is in the Office a Chief Medical Officer. The Chief Medical Officer is appointed by the President and reports to the Assistant Secretary. The individual appointed as Chief Medical Officer shall be a licensed physician possessing a demonstrated ability in and knowledge of medicine and public health.

(d) TERMINATION.—The Office shall terminate on December 21, 2023.

§ 10315. Office of Counternarcotics Enforcement

(a) OFFICE.—There is in the Department the Office of Counternarcotics Enforcement. The Director is the head of the Office. The Director is appointed by the President.

(b) ASSIGNMENT OF PERSONNEL.—

(1) IN GENERAL.—The Secretary shall assign permanent staff to the Office of Counternarcotics Enforcement, consistent with effective management of Department resources.

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

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

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

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

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

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

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

(5) to be a representative of the Department on all task forces, committees, or other entities whose purpose is to coordinate the counternarcotics enforcement activities of the Department and other Federal, State or local agencies.

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

(f) REPORTS TO CONGRESS.—

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

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

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

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

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

(2) EVALUATION OF COUNTERNARCOTICS ACTIVITIES.—The Director of the Office of Counternarcotics Enforcement shall, not later than February 1 each year, submit to the Committees on Appropriations and the authorizing committees of jurisdiction of the House of Representatives and the Senate a review and evaluation of the counternarcotics activities of the Department for the previous fiscal year. The review and evaluation shall—

(A) describe the counternarcotics activities of the Department and each subdivision of the Department (whether individually or in cooperation with other subdivisions of the Department, or in cooperation with other branches of the Federal Government or with State or local agencies), including the methods, procedures, and systems (including computer systems) for collecting, analyzing, sharing, and disseminating information concerning narcotics activity within the Department and between the Department and other Federal, State, and local agencies;

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

(C) state whether those activities were sufficient to meet the responsibility of the Department to stop the entry of illegal drugs into the United States, including a description of the performance measures of effectiveness that were used in making that determination; and

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

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

(3) CLASSIFIED OR LAW ENFORCEMENT SENSITIVE INFORMATION.—Any content of a review and evaluation described in the reports required in this subsection that involves information classified under criteria established by an Executive order, or whose public disclosure, as determined by the Secretary, would be detrimental to the law enforcement or national security activities of the Department or any other Federal, State, or local agency, shall be presented to Congress separately from the rest of the review and evaluation.

§ 10316. Office of International Affairs

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

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

(1) To promote information and education exchange with nations friendly to the United States in order to promote sharing of best practices and technologies relating to homeland security. The exchange shall include the following:

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

(B) Joint training exercises of first responders.

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

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

(3) To plan and undertake international conferences, exchange programs, and training activities.

(4) To manage international activities in the Department in coordination with other Federal officials responsible for counterterrorism matters.

§ 10317. Office for National Capital Region Coordination

There is in the Office of the Secretary the Office of National Capital Region Coordination. The Director is the head of the Office. The Director is appointed by the Secretary.

§ 10318. Office of Cargo Security Policy

There is in the Department the Office of Cargo Security Policy. The Director is the head of the Office. The Director is appointed by the Secretary. The Director reports to the Assistant Secretary for Policy.

§ 10319. Transportation Security Oversight Board

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

(b) MEMBERSHIP.—

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

(A) The Secretary, or the Secretary's designee.

(B) The Secretary of Transportation, or the Secretary of Transportation's designee.

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

(D) The Secretary of Defense, or the Secretary of Defense's designee.

(E) The Secretary of the Treasury, or the Secretary of the Treasury's designee.

(F) The Director of National Intelligence, or the Director's designee.

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

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

(c) DUTIES.—The Board shall—

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

(2) facilitate the coordination of intelligence, security, and law enforcement activities affecting transportation;

(3) facilitate the sharing of intelligence, security, and law enforcement information affecting transportation among Federal agencies and with carriers and other transportation providers as appropriate;

(4) explore the technical feasibility of developing a common database of individuals who may pose a threat to transportation or national security;

(5) review plans for transportation security;

(6) make recommendations to the Administrator of the Transportation Security Administration regarding matters reviewed under paragraph (5).

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

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

§ 10320. Special Assistant to the Secretary

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

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

(2) advising the Secretary on the impact of the Department's policies, regulations, processes, and actions on the private sector;

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

(4) creating and managing private-sector advisory councils composed of representatives of industries and associations designated by the Secretary to—

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

(B) advise the Secretary on homeland security policies, regulations, processes, and actions that affect the participating industries and associations; and

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

(i) promoting voluntary preparedness standards to the private sector; and

(ii) assisting the private sector in adopting voluntary preparedness standards;

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

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

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

(8) providing information to the private sector regarding voluntary preparedness standards and the business justification for preparedness, and promoting to the private sector the adoption of voluntary preparedness standards;

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

could be effective in supplementing Federal, State, and local government agency efforts to prevent or respond to a terrorist attack;

(10) coordinating with the Commissioner of U.S. Customs and Border Protection and the Assistant Secretary for Trade Development of the Department of Commerce on issues related to the travel and tourism industries; and

(11) consulting with the Office of State and Local Government Coordination amd Preparedness on all matters of concern to the private sector, including the tourism industry.

§ 10321. Border Enforcement Security Task Force

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

§ 10322. Office for Domestic Preparedness

(a) ESTABLISHMENT.—There is in the Department an Office for Domestic Preparedness. The Director is the head of the Office. The Director is appointed by the President.

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

(1) coordinating preparedness efforts at the Federal level, and working with all State, local, tribal, parish, and private-sector emergency response providers on all matters pertaining to combating terrorism, including training, exercises, and equipment support;

(2) coordinating or, as appropriate, consolidating communications and systems of communications relating to homeland security at all levels of government;

(3) directing and supervising terrorism preparedness grant programs of the Federal Government (other than those programs administered by the Department of Health and Human Services) for all emergency response providers;

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

(5) providing agency-specific training for agents and analysts within the Department, other agencies, State and local agencies, and international entities;

(6) as the lead executive branch agency for preparedness of the United States for acts of terrorism, cooperating closely with the Federal Emergency Management Agency, which shall have the primary responsibility within the executive branch to prepare for and mitigate the effects of nonterrorist-related disasters in the United States;

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

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

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

§ 10323. Social media working group

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

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

(c) MEMBERSHIP.—

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

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

(B) The Office of the Chief Information Officer of the Department.

(C) The Privacy Office of the Department.

(D) The Federal Emergency Management Agency.

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

(F) The American Red Cross.

(G) The Forest Service.

(H) The Centers for Disease Control and Prevention.

(I) The United States Geological Survey.

(J) The National Oceanic and Atmospheric Administration.

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

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

(B) include—

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

(ii) representatives from—

(I) State, local, tribal, and territorial entities, including from—

(aa) law enforcement;

(bb) fire services;

(cc) emergency management; and

(dd) public health entities;

(II) universities and academia; and

(III) nonprofit disaster relief organizations.

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

(d) CHAIRPERSON AND CO-CHAIRPERSON.—

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

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

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

(f) MEETINGS.—

(1) IN GENERAL.—The Group shall meet—

(A) at the call of the chairperson; and

(B) not less frequently than twice each year.

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

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

(1) A review and analysis of current and emerging social media technologies being used to support preparedness and response activities related to natural disasters and acts of terrorism and other man-made disasters.

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

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

(4) Recommendations to improve public awareness of—

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

(B) how to access the information.

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

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

(h) TERMINATION AND RENEWAL.—

(1) IN GENERAL.—The Group shall terminate on November 5, 2020, unless the chairperson renews the Group for a successive 5-year period, prior to November 5, 2020, by submitting to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a certification that the continued existence of the Group is necessary to fulfill the purpose described in subsection (b).

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

§ 10324. Office of Strategy, Policy, and Plans

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

(b) DEPUTY UNDER SECRETARY.—

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

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

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

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

(2) ESTABLISHMENT.—The Secretary may—

(A) establish in the Office of Strategy, Policy, and Plans a position of Deputy Under Secretary to support the Under Secretary for Strategy, Policy, and Plans in carrying out the Under Secretary's responsibilities; and

(B) appoint a career employee to the position.

(3) LIMITATION.—Except for the position provided for by paragraph (2), a Deputy Under Secretary position (or a substantially similar position) in the Office of Strategy, Policy, and Plans may not be established unless the Secretary receives prior authorization from Congress.

(c) COUNTERING UNMANNED AIRCRAFT SYSTEMS COORDINATOR.—

(1) DEFINITIONS.—In this subsection:

(A) COORDINATOR.—The term ''Coordinator'' means the Countering Unmanned Aircraft Systems Coordinator.

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

(2) DESIGNATION OF COORDINATOR.—The Secretary shall designate an individual in a Senior Executive Service position (as defined in section 3132 of title 5) of the Department in the Office of Strategy, Policy, and Plans as the Countering Unmanned Aircraft Systems Coordinator and provide appropriate staff to carry out the responsibilities of the Coordinator.

(3) RESPONSIBILITIES.—The Coordinator shall—

(A) oversee and coordinate with relevant Department offices and components, including the Office of Civil Rights and Civil Liberties and the Privacy Office, on the development of guidance and regulations to counter threats associated with UAS;

(B) promote research and development of counter UAS technologies in coordination within the Science and Technology Directorate;

(C) coordinate with the relevant components and offices of the Department, including the Office of Intelligence and Analysis, to ensure the sharing of information, guidance, and intelligence relating to countering UAS threats, counter UAS threat assessments, and counter UAS technology, including the retention of UAS and counter UAS incidents within the Department;

(D) serve as the Department liaison, in coordination with relevant components and offices of the Department, to the Department of Defense, Federal, State, local, and Tribal law enforcement

entities, and the private sector regarding the activities of the Department relating to countering UAS;

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

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

(4) COORDINATION WITH APPLICABLE FEDERAL LAWS.—The Coordinator shall, in addition to other assigned duties, coordinate with relevant Department components and offices to ensure testing, evaluation, or deployment of a system used to identify, assess, or defeat a UAS is carried out in accordance with applicable Federal laws.

(5) COORDINATION WITH PRIVATE SECTOR.—The Coordinator shall, among other assigned duties, working with the Office of Partnership and Engagement and other relevant Department offices and components, or other Federal agencies, as appropriate, serve as the principal Department official responsible for sharing with the private sector information regarding counter UAS technology, particularly information regarding instances in which counter UAS technology may impact lawful private-sector services or systems.

(B) patterns and practices of human trafficking;

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

(5) methods to be used by the Transportation Security Administration and personnel from other appropriate agencies to train employees of the Transportation Security Administration to—

(A) identify suspected victims of trafficking; and

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

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

(A) educate partners and stakeholders; and

(B) increase public awareness of human trafficking;

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

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

(d) ASSISTANT SECRETARY.—

(1) DEFINITIONS.—In this subsection:

(A) CRITICAL ECONOMIC SECURITY DOMAIN.—The term ''critical economic security domain'' means any infrastructure industry, technology, or intellectual property (or combination thereof) that is essential for the economic security of the United States.

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

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

(3) DUTIES.—At the direction of the Secretary the Assistant Secretary shall be responsible for policy formulation regarding matters relating to economic security and trade, as those matters relate to the mission and the operations of the Department.

(4) ADDITIONAL RESPONSIBILITIES.—In addition to the duties specified in paragraph (3) the Assistant Secretary, at the discretion of the Secretary may—

(A) oversee—

(i) coordination of supply chain policy; and

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

(B) coordinate with stakeholders in other Federal departments and agencies and nongovernmental entities with trade and economic security interests authorities, and responsibilities; and

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

§ 10325. Immigration Detention Ombudsman

(a) ESTABLISHMENT.—There is in the Department a position of Immigration Detention Ombudsman (in this section referred to as the ''Ombudsman''). The Ombudsman shall be independent of Department agencies and officers and shall report directly to the Secretary. The Ombudsman shall be a senior official with a background in civil rights enforcement, civil detention care and custody, and immigration law.

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

(1) establish and administer an independent, neutral, and confidential process to receive, investigate, resolve, and provide redress, including referral for investigation to the Office of the Inspector General, referral to U.S. Citizenship and Immigration Services for immigration relief, or other action determined appropriate, for cases in which Depart-

ment officers or other personnel, or contracted, subcontracted, or cooperating entity personnel, are found to have engaged in misconduct or violated the rights of individuals in immigration detention;

(2) establish an accessible and standardized process regarding complaints against an officer or employee of U.S. Customs and Border Protection or U.S. Immigration and Customs Enforcement, or contracted, subcontracted, or cooperating entity personnel, for violations of law, standards of professional conduct, contract terms, or policy related to immigration detention;

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

(4) review, examine, and make recommendations to address concerns or violations of contract terms identified in reviews, audits, investigations, or detainee interviews regarding immigration detention facilities and services;

(5) provide assistance to individuals affected by potential misconduct, excessive force, or violations of law or detention standards by Department officers or other personnel, or contracted, subcontracted, or cooperating entity personnel; and

(6) ensure that the functions performed by the Ombudsman are complementary to existing functions in the Department.

(c) ACCESS TO DETENTION FACILITIES.—The Ombudsman or designated personnel of the Ombudsman, shall be provided unfettered access to any location in each detention facility and shall be permitted confidential access to any detainee at the detainee's request and any departmental records concerning the detainee.

(d) COORDINATION WITH DEPARTMENT COMPONENTS.—

(1) RESPONSES TO RECOMMENDATIONS OF OMBUDSMAN.—The Director of U.S. Immigration and Customs Enforcement and the Commissioner of U.S. Customs and Border Protection shall each establish procedures to provide formal responses to recommendations submitted to those officials by the Ombudsman within 60 days of receiving the recommendations.

(2) ACCESS TO INFORMATION.—The Secretary shall establish procedures to provide the Ombudsman access to all departmental records necessary to execute the responsibilities of the Ombudsman under subsection (b) or (c) not later than 60 days after a request from the Ombudsman for the information.

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

§ 10326. Counter Threats Advisory Board

(a) ESTABLISHMENT.—There is authorized in the Department, for a period of 2 years beginning after December 27, 2020, a Counter Threats Advisory Board (in this section referred to as the ''Board'') that shall—

(1) be composed of senior representatives of departmental operational components and headquarters elements; and

(2) coordinate departmental intelligence activities and policy and information related to the mission and functions of the Department that counter threats.

(b) CHARTER.—There shall be a charter to govern the structure and mission of the Board that shall—

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

(2) be reviewed and updated as appropriate.

(c) MEMBERS.—

(1) IN GENERAL.—The Board shall be composed of senior representatives of departmental operational components and headquarters elements.

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

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

(A) The Transportation Security Administration.

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

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

(D) The Federal Emergency Management Agency.

(E) The Coast Guard.

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

(G) The United States Secret Service.

(H) The Cybersecurity and Infrastructure Security Agency.

(I) The Office of Operations Coordination.

(J) The Office of the General Counsel.

(K) The Office of Intelligence and Analysis.

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

(M) The Science and Technology Directorate.

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

(O) The Privacy Office.

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

(Q) Other departmental offices and programs as determined appropriate by the Secretary.

(d) MEETINGS.—The Board shall—

(1) meet on a regular basis to discuss intelligence and coordinate ongoing threat mitigation efforts and departmental activities, including coordination with other Federal, State, local, tribal, territorial, and private-sector partners; and

(2) make recommendations to the Secretary.

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

(f) PROHIBITION ON ADDITIONAL FUNDS.—No additional funds are authorized to carry out this section.

§ 10327. Economic security council

(a) DEFINITIONS.—In this section

(1) COUNCIL.—The term ''Council'' means the council established under subsection (b).

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

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

(c) DUTIES.—Pursuant to the scope of the mission of the Department as described in in subsection (b), the Council shall provide to the Secretary advice and recommendations on matters of economic security, including relating to the following:

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

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

(3) Coordinating Department-wide activity on trade and economic security matters.

(4) With respect to the development of the continuity of the economic plan of the President under section 11327 of this title.

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

(6) Any other matters the Secretary considers appropriate.

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

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

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

(e) MEETINGS.—The Council shall meet not less frequently than quarterly as well as—

(1) at the call of the Chair; or

(2) at the direction of the Secretary.

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

Subchapter II—Functions

§ 10341. In general

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

(b) REORGANIZATION.—

(1) IN GENERAL.—The Secretary may allocate or reallocate functions among the officers of the Department, and may establish, consolidate, alter, or discontinue organizational units within the Department, but only after the expiration of 60 days after providing notice of the action to the appropriate congressional committees, which shall include an explanation of the rationale for the action.

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

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

(d) REDELEGATION.—Unless otherwise provided in the delegation or by law, a function delegated under this subtitle may be redelegated to a subordinate.

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

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

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

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

(4) shall ensure that there is effective and ongoing coordination of Federal efforts to prevent, prepare for, and respond to acts of terrorism and other major disasters and emergencies among the divisions of the Department, including the Office for State and Local Government Coordination;

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

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

(f) REGULATORY AUTHORITY.—

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

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

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

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

(ii) on November 25, 2002, was exercised by another official of the executive branch with respect to the transferred agency, program, or function.

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

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

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

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

(1) coordinating with State and local government personnel, agencies, and authorities, and with the private sector, to ensure adequate planning, equipment, training, and exercise activities;

(2) coordinating and, as appropriate, consolidating, the Federal Government's communications and systems of communications relating to homeland security with State and local government personnel, agencies, and authorities, the private sector, other entities, and the public; and

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

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

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

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

(l) PLANNING REQUIREMENTS.—The Secretary shall ensure the head of each office and component of the Department takes into account the needs of children, including children in under-served communities, in mission planning and mission execution. In furtherance of this subsection, the Secretary shall require each office and component head to seek, to the extent practicable, advice and feedback from organizations representing the needs of

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

§ 10342. Trade and customs revenue functions

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

(b) TRADE AND CUSTOMS REVENUE FUNCTIONS.—

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

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

(B) monitor and report to Congress on the Department mandate to ensure that the trade and customs revenue functions of the Department are not diminished, including how spending, operations, and personnel related to these functions have kept pace with the level of trade entering the United States.

(2) DIRECTOR OF TRADE POLICY.—There is in the Department a Director of Trade Policy (in this subsection referred to as the ''Director''), who shall be subject to the direction and control of the official designated under paragraph (1). The Director shall—

(A) advise the official designated under paragraph (1) regarding all aspects of Department policies relating to the trade and customs revenue functions of the Department;

(B) coordinate the development of Department-wide policies regarding trade and customs revenue functions and trade facilitation; and

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

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

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

(2) CONGRESSIONAL NOTIFICATION.—

(A) IN GENERAL.—Subject to subparagraph (B), the Secretary shall notify the appropriate congressional committees not later than 30 days prior to the finalization of Department policies, initiatives, or actions that will have a major impact on trade and customs revenue functions. The notifications shall include a description of the proposed policies, initiatives, or actions and any comments or recommendations provided by the Commercial Customs Operations Advisory Committee and other relevant groups regarding the proposed policies, initiatives, or actions.

(B) EXCEPTION.—If the Secretary determines that it is important to the national security interest of the United States to finalize any Department policies, initiatives, or actions prior to the notification described in subparagraph (A), the Secretary shall—

(i) notify and provide any recommendations of the Commercial Customs Operations Advisory Committee received to the appropriate congressional committees not later than 45 days after the date on which the policies, initiatives, or actions are finalized; and

(ii) to the extent appropriate, modify the policies, initiatives, or actions based upon the consultations with the appropriate congressional committees.

(d) NOTIFICATION OF REORGANIZATION OF CUSTOMS REVENUE FUNCTIONS.—

(1) IN GENERAL.—Not less than 45 days prior to a change in the organization of any of the customs revenue functions of the Department, the Secretary shall notify the Committee on Appropriations, the Committee on Finance, and the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Appropriations, the Committee on Homeland Security, and the Committee on Ways and Means of the House of Representatives of the specific assets, functions, or personnel to be transferred as part of the reorganization, and the reason for the transfer. The notification shall also include—

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

(B) an explanation of how the reorganization meets the requirements of section 11132(b) of this title that the Department not diminish the customs revenue and trade facilitation functions formerly performed by the United States Customs Service; and

(C) any comments or recommendations provided by the Commercial Customs Operations Advisory Committee regarding the reorganization.

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

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

§ 10343. Military activities

Nothing in this subtitle shall confer upon the Secretary authority to engage in warfighting, the military defense of the United States, or other military activities, nor shall anything in this subtitle limit the existing authority of the Department of Defense or the armed forces to engage in warfighting, the military defense of the United States, or other military activities.

§ 10344. Sensitive Security Information

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

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

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

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

(2) PURPOSE OF GUIDANCE.—The guidance shall serve as the primary basis and authority for the marking of Departmental information as SSI by covered individuals.

§ 10345. Daily public report of covered contract awards

(a) DEFINITIONS.—In this section:

(1) COVERED CONTRACT AWARD.—The term ''covered contract award''—

(A) means a contract action of the Department with a total contract value of not less than $4,000,000, including unexercised options; and

(B) includes—

(i) contract awards covered by the Federal AcquisitionRegulation;

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

(iii) orders placed on a multiple-award or multiple-agency contract that includes delivery or quantity terms that are indefinite;

(iv) other transaction authority agreements; and

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

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

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

(4) TOTAL CONTRACT VALUE.—The term ''total contract value'' means the total amount of funds expected to be provided to the contractor at issue under the terms of the contract through the full period of performance.

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

(b) DAILY CONTRACT REPORTING REQUIREMENTS.—

(1) REPORT.—

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

(B) Contents.—Each report under this paragraph shall include for each covered contract award information relating to the following:

(i) The contract number, modification number, or delivery order number.

(ii) The contract type.

(iii) The amount obligated for the award.

(iv) The total contract value for the award, including all options.

(v) The description of the purpose for the award.

(vi) The number of proposals or bids received.

(vii) The name and address of the vendor and whether the vendor is a small business.

(viii) The period and primary place of performance for the award.

(ix) Whether the award is multiyear.

(x) The contracting office.

(2) UPDATE.—The Secretary shall make updates referred to in paragraph (1) not later than 5 business days after the date on which a covered contract is authorized or modified.

(3) EFFECTIVE DATE.—Paragraph (1) shall take effect on the date that is 180 days after December 23, 2022.

(c) UNDEFINITIZED CONTRACT ACTION OR DEFINITIZED AMOUNT.—If a covered contract amount reported under subsection (b) contains an undefinitized contract action, the Secretary shall—

(1) report the estimated total contract value for the award and the amount obligated on award; and

(2) once there is a definitized amount for the award, update the total contract value and the amount obligated.

(d) EXEMPTION.—Each report required under subsection (a) shall not include covered contract awards for which synopses were exempted under section 5.202(a)(1) of the Federal Acquisition Regulation, or any successor to the Regulation.

(e) TERMINATION.—This section shall cease to have force and effect on December 23, 2027.

Subchapter III—Acquisitions

§ 10351. Personal services

The Secretary—

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

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

services, including the services of experts or consultants (or organizations thereof), without regard to the pay limitations of section 3109.

§ 10352. Prohibition on contracts with corporate expatriates

(a) DEFINITIONS AND SPECIAL RULES.—

(1) DEFINITIONS.—In this section:

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

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

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

(D) FOREIGN INCORPORATED ENTITY.—The term ''foreign incorporated entity'' means an entity that is, or but for subsection (c) would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986 (26 U.S.C. 1 et seq.).

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

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

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

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

(ii) stock of the entity which is sold in a public offering related to the acquisition described in subsection (c)(1).

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

(C) CERTAIN TRANSFERS DISREGARDED.—The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if the transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(D) SPECIAL RULE FOR RELATED PARTNERSHIPS.—For purposes of applying subsection (c) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships that are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986 (26 U.S.C. 482)) shall be treated as one partnership.

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

(i) treat warrants, options, contracts to acquire stock, convertible debt instruments, and other similar interests as stock; and

(ii) treat stock as not stock.

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

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

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

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

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

(B) in the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

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

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

§ 10353. Lead system integrator; financial interests

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

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

(1) the Secretary certifies to the Committees on Appropriations of the Senate and the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Transportation and Infrastructure of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Commerce, Science and Transportation of the Senate that—

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

(B) the Department took appropriate steps to prevent an organizational conflict of interest in the selection process; or

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

(c) CONSTRUCTION.—Nothing in this section shall be construed to preclude an entity described in subsection (a) from performing work necessary to integrate two or more individual systems or elements of a system of systems with each other.

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

(1) a precise and comprehensive definition of the term ''lead system integrator'', modeled after that used by the Department of Defense; and

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

§ 10354. Requirements to buy certain items related to national security interests

(a) DEFINITIONS.—In this section:

(1) COVERED ITEM.—The term ''covered item'' means any of the following:

(A) Footwear provided as part of a uniform.

(B) Uniforms.

(C) Holsters and tactical pouches.

(D) Patches, insignia, and embellishments.

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

(F) Body armor components intended to provide ballistic protection for an individual, consisting of 1 or more of the following:

(i) Soft ballistic panels.

(ii) Hard ballistic plates.

(iii) Concealed armor carriers worn under a uniform.

(iv) External armor carriers worn over a uniform.

(G) Any other item of clothing or protective equipment as determined appropriate by the Secretary.

(2) FRONTLINE OPERATIONAL COMPONENT.—The term ''frontline operational component'' means any of the following entities of the Department:

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

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

(C) The United States Secret Service.

(D) The Transportation Security Administration.

(E) The Federal Protective Service.

(F) The Federal Emergency Management Agency.

(G) The Federal Law Enforcement Training Centers.

(H) The Cybersecurity and Infrastructure Security Agency.

(b) REQUIREMENTS.—

(1) IN GENERAL.—The Secretary shall ensure that any procurement of a covered item for a frontline operational component meets the following criteria:

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

(ii) Covered items may only be supplied pursuant to clause (i) to the extent that United States entities that qualify as small business concerns—

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

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

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

(i) is an entity registered with the System for Award Management (or successor system) administered by the General Services Administration; and

(ii) is in compliance with ISO 9001:2015 of the International Organization for Standardization (or successor standard) or a standard determined appropriate by the Secretary to ensure the quality of products and adherence to applicable statutory and regulatory requirements.

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

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

(ii) report any pilferage or theft of the covered item with the insignia or the insignia occurring at any stage before delivery of the covered item with the insignia or the insignia; and

(iii) destroy any defective or unusable covered item with insignia or insignia in a manner established by the Secretary, and maintain records, for 3 years after the creation of the records, of the destruction that include the date of the destruction, a description of the covered item with insignia or insignia destroyed, the quantity of the covered item with insignia or insignia destroyed, and the method of destruction.

(2) WAIVER.—

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

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

(B) NOTICE.— Not later than 60 days after the date on which the Secretary determines a waiver under subparagraph (A) is necessary, the Secretary shall provide to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security, the Committee on Oversight and Reform, and the Committee on Appropriations of the House of Representatives notice of the determination, which shall include the following:

(i) Identification of the national emergency or major disaster declared by the President.

(ii) Identification of the covered item for which the Secretary intends to issue the waiver.

(iii) A description of the demand for the covered item and corresponding lack of supply from contractors able to meet the criteria described in subparagraph (B) or (C) of paragraph (1).

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

(d) REPORT.—Not later than December 23, 2023, and annually thereafter, the Secretary shall provide to the Committee on Homeland Security, the Committee on Oversight and Reform, the Committee on Small Business, and the Committee on Appropriations of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs, the Committee on Small Business and Entrepreneurship, and the Committee on Appropriations of the Senate a briefing on instances in which vendors have failed to meet deadlines for delivery of covered items and corrective actions taken by the Department in response to those instances.

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

Subchapter IV—Human Resources Management

§ 10361. Establishment of human resources management system

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

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

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

§ 10362. Labor-management relations

(a) LIMITATION ON EXCLUSIONARY AUTHORITY.—

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

(A) the mission and responsibilities of the agency (or subdivision) materially change; and

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

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

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

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

(b) PROVISIONS RELATING TO BARGAINING UNITS.—

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

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

(B) a majority of the employees within the unit (or subdivision) have as their primary duty intelligence, counterintelligence, or investigative work directly related to terrorism investigation.

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

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

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

(c) WAIVER.—If the President determines that the application of subsections (a), (b), and (d) would have a substantial adverse impact on the ability of the Department to protect homeland security, the President may waive the application of the subsections 10 days after the President has submitted to Congress a written explanation of the reasons for the determination.

(d) COORDINATION RULE.—No other provision of this subtitle or the Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2135), or of an amendment made by the Act, may be construed or applied in a manner so as to limit, supersede, or otherwise affect 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 that 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.

§ 10363. 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 Director of the Office of Counternarcotics Enforcement; 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.

§ 10364. Compliance with laws protecting equal employment opportunity and providing whistleblower protections

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

(1) to provide equal employment protection for employees of the Department (including under section 2302(b)(1) of title 5 and the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (Public Law 107–174, 5 U.S.C. 2301 note)); or

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

§ 10365. Use of protective equipment or measures by employees

No funds may be used to propose or effect a disciplinary or adverse action, with respect to any Department employee who engages regularly with the public in the performance of his or her official duties, solely because that employee elects to utilize protective equipment or measures, including surgical masks, N95 respirators, gloves, or hand-sanitizers, where use of the equipment or measures is in accord with Department policy, and Centers

for Disease Control and Prevention and Office of Personnel Management guidance.

§ 10366. Homeland Security Rotation Program

(a) ESTABLISHMENT.—The Secretary shall establish the Homeland Security Rotation Program (in this section referred to as the ''Rotation Program'') for employees of the Department. The Rotation Program shall use applicable best practices, including those from the Chief Human Capital Officers Council.

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

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

(2) provide middle and senior level employees in the Department the opportunity to broaden their knowledge through exposure to other components of the Department;

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

(4) build professional relationships and contacts among the employees in the Department;

(5) invigorate the workforce with exciting and professionally rewarding opportunities;

(6) incorporate Department human capital strategic plans and activities, and address critical human capital deficiencies, recruitment and retention efforts, and succession planning in the Federal workforce of the Department; and

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

(c) ADMINISTRATION.—

(1) IN GENERAL.—The Chief Human Capital Officer shall administer the Rotation Program.

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

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

(B) establish a framework that supports the goals of the Rotation Program and promotes cross-disciplinary rotational opportunities;

(C) establish eligibility for employees to participate in the Rotation Program and select participants from employees who apply;

(D) establish incentives for employees to participate in the Rotation Program, including promotions and employment preferences;

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

(F) ensure that the Rotation Program develops qualified employees and future leaders with broad-based experience throughout the Department;

(G) provide for greater interaction among employees in components of the Department; and

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

(d) ALLOWANCES, PRIVILEGES, AND BENEFITS.—All allowances, privileges, rights, seniority, and other benefits of employees participating in the Rotation Program shall be preserved.

§ 10367. Rotational cybersecurity research program

To enhance the Department's cybersecurity capacity, the Secretary may establish a rotational research, development, and training program for—

(1) detail to the Cybersecurity and Infrastructure Security Agency (including the National Cybersecurity and Communications Integration Center authorized by section 10706 of this title) of Coast Guard Academy graduates and faculty; and

(2) detail to the Coast Guard Academy, as faculty, of individuals with expertise and experience in cybersecurity who are employed by—

(A) the Cybersecurity and Infrastructure Security Agency (including the National Cybersecurity and Communications Integration Center);

(B) the Directorate of Science and Technology; or

(C) institutions that have been designated by the Department as a Center of Excellence for Cyber Defense, or the equivalent.

§ 10368. Homeland Security Education Program

(a) ESTABLISHMENT.—The Secretary, acting through the Administrator of the Federal Emergency Management Agency, shall establish a graduate-level Homeland Security Education Program in the National Capital Region to provide educational opportunities to senior Federal officials and selected State and local officials with homeland security and emergency management responsibilities. The Administrator shall appoint an individual to administer the activities under this section.

(b) LEVERAGING OF EXISTING RESOURCES.—To maximize efficiency and effectiveness in carrying out the Homeland Security Education Program, the Administrator shall use existing Department-reviewed master's degree curricula in homeland security, including curricula pending accreditation, together with associated learning materials, quality assessment tools, digital libraries, exercise systems, and other educational facilities, including the Na-

tional Domestic Preparedness Consortium, the National Fire Academy, and the Emergency Management Institute. The Administrator may develop additional educational programs, as appropriate.

(c) STUDENT ENROLLMENT.—

(1) SOURCES.—The student body of the Homeland Security Education Program shall include officials from Federal, State, local, and tribal governments, and from other sources designated by the Administrator.

(2) ENROLLMENT PRIORITIES AND SELECTION CRITERIA.—The Administrator shall establish policies governing student enrollment priorities and selection criteria that are consistent with the mission of the Homeland Security Education Program.

(3) DIVERSITY.—The Administrator shall take reasonable steps to ensure that the student body represents racial, gender, and ethnic diversity.

(d) SERVICE COMMITMENT.—

(1) IN GENERAL.—Before an employee selected for the Homeland Security Education Program may be assigned to participate in the program, the employee shall agree in writing—

(A) to continue in the service of the agency sponsoring the employee during the 2-year period beginning on the date on which the employee completes the program, unless the employee is involuntarily separated from the service of that agency for reasons other than a reduction in force; and

(B) to pay to the Government the amount of the additional expenses incurred by the Government in connection with the employee's education if the employee is voluntarily separated from the service of the agency before the end of the period described in subparagraph (A).

(2) PAYMENT OF EXPENSES.—

(A) EXEMPTION.—An employee who leaves the service of the sponsoring agency to enter into the service of another agency in any branch of the Government shall not be required to make a payment under paragraph (1)(B), unless the head of the agency that sponsored the education of the employee notifies that employee before the date on which the employee enters the service of the other agency that payment is required under that paragraph.

(B) AMOUNT OF PAYMENT.—If an employee is required to make a payment under paragraph (1)(B), the agency that sponsored the education of the employee shall determine the amount of the pay-

ment, except that the amount may not exceed the pro rata share of the expenses incurred for the time remaining in the 2-year period.

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

(A) setoff against accrued pay, compensation, amount of retirement credit, or other amount due the employee from the Government; or

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

§ 10369. Annual employee award program

(a) IN GENERAL.—The Secretary may establish an annual employee award program to recognize Department employees or groups of employees for significant contributions to the achievement of the Department's goals and missions. If such a program is established, the Secretary shall—

(1) establish within the program categories of awards, each with specific criteria, that emphasize honoring employees who are at the nonsupervisory level;

(2) publicize within the Department how any employee or group of employees may be nominated for an award;

(3) establish an internal review board comprised of representatives from Department components, headquarters, and field personnel to submit to the Secretary award recommendations regarding specific employees or groups of employees;

(4) select recipients from the pool of nominees submitted by the internal review board under paragraph (3) and convene a ceremony at which employees or groups of employees receive the awards from the Secretary; and

(5) publicize the program within the Department.

(b) CONSULTATION.—The internal review board described in subsection (a)(3) shall, when carrying out its function under subsection (a)(3), consult with representatives from operational components and headquarters, including supervisory and nonsupervisory personnel, and employee labor organizations that represent Department employees.

(c) RULE OF CONSTRUCTION.—Nothing in this section may be construed to authorize additional funds to carry out the requirements of this section or to require the Secretary to provide monetary bonuses to recipients of an award under this section.

Subchapter V—Cybersecurity

§ 10381. Workforce assessment and strategy

(a) DEFINITIONS.—In this section:

(1) CYBERSECURITY CATEGORY.—The term ''Cybersecurity Category'' means a position's or incumbent's primary work function involving cybersecurity, which is further defined by Specialty Area.

(2) SPECIALTY AREA.—The term ''Specialty Area'' means any of the common types of cybersecurity work as recognized by the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework report.

(b) WORKFORCE ASSESSMENT.—The Secretary shall assess the cybersecurity workforce of the Department. The assessment shall include, at a minimum—

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

(2) information on where cybersecurity workforce positions are located in the Department;

(3) information on which cybersecurity workforce positions are—

(A) performed by—

(i) permanent full-time equivalent employees of the Department, including, to the greatest extent practicable, demographic information about the employees;

(ii) independent contractors; and

(iii) individuals employed by other Federal agencies, including the National Security Agency; or

(B) vacant; and

(4) information on–

(A) the percentage of individuals in each Cybersecurity Category and Specialty Area who received essential training to perform their jobs; and

(B) in cases in which that essential training was not received, what challenges, if any, were encountered with respect to the provision of the essential training.

(c) WORKFORCE STRATEGY.—

(1) ESTABLISHMENT, MAINTENANCE, AND UPDATES.—The Secretary shall—

(A) develop a comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department; and

(B) maintain and, as necessary, update the comprehensive workforce strategy developed under subparagraph (A).

(2) CONTENTS.—The comprehensive workforce strategy developed under paragraph (1) shall include a description of—

(A) a multi-phased recruitment plan, including with respect to experienced professionals, members of disadvantaged or underserved communities, the unemployed, and veterans;

(B) a 5-year implementation plan;

(C) a 10-year projection of the cybersecurity workforce needs of the Department;

(D) any obstacle impeding the hiring and development of a cybersecurity workforce in the Department; and

(E) any gap in the existing cybersecurity workforce of the Department and a plan to fill the gap.

(d) UPDATES.—The Secretary shall submit to the appropriate congressional committees annual updates on—

(1) the cybersecurity workforce assessment required under subsection (b); and

(2) the progress of the Secretary in carrying out the comprehensive workforce strategy required to be developed under subsection (c).

§ 10382. Homeland Workforce Measurement Initiative

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

(B) the Committee on Homeland Security of the House of Representatives; and

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

(2) CYBERSECURITY WORK CATEGORY; DATA ELEMENT CODE; SPECIALTY AREA.—The terms ''Cybersecurity Work Category'', ''Data Element Code'', and ''Specialty Area'' have the same meanings given those terms in the Office of Personnel Management's Guide to Data Standards.

(3) DIRECTOR.—-The term ''Director'' means the Director of the Office of Personnel Management.

(b) NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIATIVE.—

(1) IN GENERAL.—The Secretary shall—

(A) identify all cybersecurity workforce positions in the Department;

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

(C) assign the corresponding Data Element Code, as set forth in the Office of Personnel Management's Guide to Data Standards that is aligned with the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework report, in accordance with paragraph (2).

(2) EMPLOYMENT CODES.—

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

(i) identify open positions that include cybersecurity functions (as defined in the Office of Personnel Management's Guide to Data Standards); and

(ii) assign the appropriate employment code to each position, using agreed-on standards and definitions.

(B) CODE ASSIGNMENTS.—The Secretary shall assign the appropriate employment code to—

(i) each employee in the Department who carries out cybersecurity functions; and

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

(3) PROGRESS REPORT.—The Director shall submit a progress report on the implementation of this subsection to the appropriate congressional committees.

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

(1) IN GENERAL.—Annually through 2021, the Secretary, in consultation with the Director, shall—

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

(B) submit a report to the Director that—

(i) describes the Cybersecurity Work Categories and Specialty Areas identified under subparagraph (A); and

(ii) substantiates the critical need designations.

(2) GUIDANCE.—The Director shall provide the Secretary with timely guidance for identifying Cybersecurity Work Categories and Specialty Areas of critical need, including—

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

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

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

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

(B) submit a progress report on the implementation of this subsection to the appropriate congressional committees.

(d) COMPTROLLER GENERAL STATUS REPORTS.—The Comptroller General shall—

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

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

Subchapter VI—Miscellaneous Provisions

§ 10391. Advisory committees

(a) IN GENERAL.—The Secretary may establish, appoint members of, and use the services of, advisory committees, that the Secretary considers necessary. An advisory committee established under this section may be exempted by the Secretary from chapter 10 of title 5, but the Secretary shall publish notice in the Federal Register announcing the establishment of the committee and identifying its purpose and membership. Notwithstanding the preceding sentence, members of an advisory committee that is exempted by the Secretary under the preceding sentence who are special Government employees (as that term is defined in section 202 of title 18) shall be eligible for certifications under section 208(b)(3) of title 18, for official actions taken as a member of the advisory committee.

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

§ 10392. Use of appropriated funds

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

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

(2) Purchase of insurance for official motor vehicles operated in foreign countries;

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

(4) Services authorized by section 3109 of title 5; and

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

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

(c) DISPOSAL OF PROPERTY.—

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

(2) DEPOSIT OF PROCEEDS.—The Secretary shall deposit the proceeds of an exercise of property disposal authority into the miscellaneous receipts of the Treasury under section 3302(b) of title 31.

(d) GIFTS.—Except as authorized by section 10397 or 11321 of this title, section 2601 of title 10, or section 504 of title 14, gifts or donations of services or property of or for the Department may not be accepted, used, or disposed of unless specifically permitted in advance in an appropriations Act and only under the conditions and for the purposes specified in the appropriations Act.

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

§ 10393. Reports and consultation addressing use of appropriated funds

(a) IN GENERAL.—Notwithstanding this subtitle, a report, notification, or consultation addressing directly or indirectly the use of appropriated funds and stipulated by this subtitle to be submitted to, or held with, Congress or a Congressional committee shall also be submitted to, or held with, the Committees on Appropriations of the Senate and the House of Representatives under the same conditions and with the same restrictions as stipulated by this subtitle.

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

§ 10394. Buy America requirements

(a) DEFINITION OF UNITED STATES.—In this section, the term ''United States'' includes the possessions of the United States.

(b) REQUIREMENT.—Except as provided in subsections (d) and (e), funds appropriated or otherwise available to the Department may not be used for the procurement of an item described in subsection (c) under a contract entered into by the Department on and after August 16, 2009, if the item is not grown, reprocessed, reused, or produced in the United States.

(c) COVERED ITEMS.—An item referred to in subsection (b) is an article or item of any of the following, if the item is directly related to the national security interests of the United States:

(1) Clothing and the materials and components of clothing, other than sensors, electronics, or other items added to, and not normally associated with, clothing (and the materials and components of clothing).

(2) Tents, tarpaulins, covers, textile belts, bags, protective equipment (including body armor), sleep systems, load carrying equipment (including fieldpacks), textile marine equipment, parachutes, or bandages.

(3) Cotton and other natural fiber products, woven silk or woven silk blends, spun silk yarn for cartridge cloth, synthetic fabric or coated synthetic fabric (including all textile fibers and yarns that are for use in the fabrics), canvas products, or wool (whether in the form of fiber or yarn or contained in fabrics, materials, or manufactured articles).

(4) An item of individual equipment manufactured from or containing the fibers, yarns, fabrics, or materials.

(d) APPLICABILITY TO CONTRACTS AND SUBCONTRACTS FOR PROCUREMENT OF COMMERCIAL PRODUCTS.—

(1) DEFINITION OF COMMERCIAL PRODUCT.—In this section, the word ''commercial product'' has the meaning given the term in section 103 of title 41.

(2) IN GENERAL.—This section is applicable to contracts and subcontracts for the procurement of commercial products notwithstanding section 1906 of title 41, with the exception of commercial products listed under paragraphs (3) and (4) of subsection (c).

(e) EXCEPTIONS.—

(1) AVAILABILITY.—

(A) MATERIALS.—Subsection (b) does not apply to covered items that are, or include, materials determined to be non-available in accordance with Federal Acquisition Regulation 25.104 Nonavailable Articles.

(B) UNSATISFACTORY QUALITY AND INSUFFICIENT QUANTITY.—Subsection (b) does not apply to the extent that the Sec-

retary determines that satisfactory quality and sufficient quantity of an article or item described in subsection (c) grown, reprocessed, reused, or produced in the United States cannot be procured as and when needed at United States market prices.

(2) DE MINIMIS NONCOMPLIANCE.—Notwithstanding subsection (b), the Secretary may accept delivery of an item covered by subsection (c) that contains non-compliant fibers if the total value of non-compliant fibers contained in the end item does not exceed 10 percent of the total purchase price of the end item.

(3) CERTAIN PROCUREMENTS OUTSIDE THE UNITED STATES.—Subsection (b) does not apply to the following:

(A) Procurements by vessels in foreign waters.

(B) Emergency procurements.

(4) SMALL PURCHASES.—Subsection (b) does not apply to purchases for amounts not greater than the simplified acquisition threshold referred to in section 3205 of title 10.

(f) NOTIFICATION REQUIRED WITHIN 7 DAYS AFTER CONTRACT AWARD IF CERTAIN EXCEPTIONS APPLIED.—In the case of a contract for the procurement of an item described in subsection (c), if the Secretary applies an exception set forth in subsection (e)(1) with respect to that contract, the Secretary shall, not later than 7 days after the award of the contract, post a notification that the exception has been applied on the Internet site maintained by the General Services Administration known as FedBizOpps.gov (or a successor site).

(g) INCLUSION OF INFORMATION IN NEW TRAINING PROGRAMS.—The Secretary shall ensure that a training program for the acquisition workforce includes comprehensive information on the requirements of this section and the regulations implementing this section.

(h) CONSISTENCY WITH INTERNATIONAL AGREEMENTS.—This section shall be applied in a manner consistent with United States obligations under international agreements.

§ 10395. Horse adoption program

With respect to a horse or other equine belonging to a component or agency of the Department, no funds made available in any Act may be used to destroy or put out to pasture any horse or other equine that has become unfit for service, unless the trainer or handler is first given the option to take possession of the equine through an adoption program that has safeguards against slaughter and inhumane treatment.

§ 10396. 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).

§ 10397. 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;

(C) a Government corporation as defined in section 9101 of title 31;

(D) the Government Printing Office;

(E) the United States Capitol Police;

(F) the United States Supreme Court Police; and

(G) Government agencies with law enforcement related duties.

(7) LAW ENFORCEMENT PERSONNEL.—The term ''law enforcement personnel'' means an individual, including a criminal investigator (commonly known as ''agent'') and uniformed police (commonly known as ''officer''), who has statutory authority to search, seize, make arrests, or carry firearms.

(8) LOCAL.—The term ''local'' means—

(A) of or pertaining to any county, parish, municipality, city, town, township, rural community, unincorporated town or village, local public authority, educational institution, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, agency or instrumentality of a local government, or other political subdivision of a State; and

(B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation.

(9) PARTNER ORGANIZATION.—The term ''partner organization'' means a Federal agency participating in FLETC's training programs under a formal memorandum of understanding.

(10) STATE.—The term ''State'' means a State, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any possession of the United States.

(11) STUDENT INTERN.—The term ''student intern'' means any eligible baccalaureate or graduate degree student participating in FLETC's College Intern Program.

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

(1) is the head of FLETC;

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

(3) shall report to the Secretary.

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

(1) develop training goals and establish strategic and tactical organizational program plans and priorities;

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

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

(4) monitor progress toward strategic and tactical FLETC plans regarding training curricula, including curricula relating to domestic preparedness and response to threats or acts of terrorism, and facilities;

(5) ensure the timely dissemination of homeland security information as necessary to Federal, State, local, tribal, territorial, and international law enforcement and security agencies and the private sector to achieve the training goals for those entities, in accordance with paragraph (1);

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

(A) fully complies with—

(i) Federal law;

(ii) the Federal Acquisition Regulation, including requirements regarding agency obligations to contract only with responsible prospective contractors; and

(iii) Department acquisition management directives; and

(B) maximizes opportunities for small business participation;

(7) coordinate and share information with the heads of relevant components and offices on digital learning and training resources, as appropriate;

(8) advise the Secretary on matters relating to executive level policy and program administration of Federal, State, local, tribal, territorial, and international law enforcement and security training activities and private-sector security agency training activities, including training activities relating to domestic preparedness and response to threats or acts of terrorism;

(9) collaborate with the Secretary and relevant officials at other Federal departments and agencies, as appropriate, to improve international instructional development, training, and technical assistance provided by the Federal Government to foreign law enforcement; and

(10) carry out such other functions as the Secretary determines are appropriate.

(d) TRAINING RESPONSIBILITIES.—

(1) IN GENERAL.—The Director may provide training to employees of Federal agencies who are engaged, directly or indirectly, in homeland security operations or Federal law enforcement activities, including operations or activities relating to domestic preparedness and response to threats or acts of terrorism. In carrying out the training, the Director shall—

(A) evaluate best practices of law enforcement training methods and curriculum content to maintain state-of-the-art expertise in adult learning methodology;

(B) provide expertise and technical assistance, including on domestic preparedness and response to threats or acts of terrorism, to Federal, State, local, tribal, territorial, and international law enforcement and security agencies and private-sector security agencies; and

(C) maintain a performance evaluation process for students.

(2) RELATIONSHIP WITH LAW ENFORCEMENT AGENCIES.—The Director shall consult with relevant law enforcement and security agencies in the development and delivery of FLETC's training programs.

(3) TRAINING DELIVERY LOCATIONS.—The training required under paragraph (1) may be conducted at FLETC facilities, at appropriate off-site locations, or by distributed learning.

(4) STRATEGIC PARTNERSHIPS.—

(A) IN GENERAL.—The Director may—

(i) execute strategic partnerships with State and local law enforcement to provide them with specific training, including maritime law enforcement training; and

(ii) coordinate with the Director of the Cybersecurity and Infrastructure Security Agency and with private-sector stakeholders, including critical infrastructure owners and operators, to provide training pertinent to improving coordination, security, and resiliency of critical infrastructure.

(B) PROVISION OF INFORMATION.—The Director shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, on request, information on activities undertaken in the previous year pursuant to subparagraph (A).

(5) FLETC DETAILS TO DEPARTMENT.—The Director may detail employees of FLETC to positions throughout the Department in furtherance of improving the effectiveness and quality of training provided by

the Department and, as appropriate, the development of critical departmental programs and initiatives.

(6) DETAIL OF INSTRUCTORS TO FLETC.—Partner organizations that wish to participate in FLETC training programs shall assign non-reimbursable detailed instructors to FLETC for designated time periods to support all training programs at FLETC, as appropriate. The Director shall determine the number of detailed instructors that is proportional to the number of training hours requested by each partner organization scheduled by FLETC for each fiscal year. If a partner organization is unable to provide a proportional number of detailed instructors, the partner organization shall reimburse FLETC for the salary equivalent for the detailed instructors, as appropriate.

(7) PARTNER ORGANIZATION EXPENSES REQUIREMENTS.—

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

(i) Salaries, travel expenses, lodging expenses, and miscellaneous per diem allowances of their personnel attending training courses at FLETC.

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

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

(8) PROVISION OF NON-FEDERAL TRAINING.—

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

(i) State, local, tribal, and territorial law enforcement personnel.

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

(iii) Private-sector security officers, participants in the Federal Flight Deck Officer program under section 40932 of this title, and other appropriate private-sector individuals.

(B) WAIVER.—The Director may waive the requirement for reimbursement of any cost under this section and shall maintain records regarding the reasons for any requirements waived.

(9) REIMBURSEMENT.—The Director may reimburse travel or other expenses for non-Federal personnel who attend activities relating to training sponsored by FLETC, at travel and per diem rates established by the General Services Administration.

(10) STUDENT SUPPORT.—In furtherance of FLETC's training mission, the Director may provide the following support to students:

(A) Athletic and related activities.

(B) Short-term medical services.

(C) Chaplain services.

(11) AUTHORITY TO HIRE FEDERAL ANNUITANTS.—

(A) IN GENERAL.—Notwithstanding another law, the Director may appoint and maintain, as necessary, Federal annuitants who have expert knowledge and experience to meet the training responsibilities under this subsection.

(B) NO REDUCTION IN RETIREMENT PAY.—A Federal annuitant employed pursuant to this paragraph shall not be subject to any reduction in pay for annuity allocable to the period of actual employment under section 8344 or 8468 of title 5 or a similar provision of any other retirement system for employees.

(C) RE-EMPLOYED ANNUITANTS.—A Federal annuitant employed pursuant to this paragraph shall not be considered an employee for purposes of subchapter III of chapter 83 or chapter 84 of title 5 or such other retirement system (referred to in subparagraph (B)) as may apply.

(D) COUNTING.—Federal annuitants shall be counted on a full-time equivalent basis.

(E) LIMITATION.—No appointment under this paragraph may be made that would result in the displacement of any employee.

(12) TRAVEL FOR INTERMITTENT EMPLOYEES.—The Director may reimburse intermittent Federal employees traveling from outside a commuting distance (to be predetermined by the Director) for travel expenses.

(e) HOUSING.—Individuals attending training at any FLETC facility shall, to the extent practicable and in accordance with FLETC policy, reside in on-FLETC or FLETC-provided housing.

(f) ADDITIONAL FISCAL AUTHORITIES.—To further the goals and objectives of FLETC, the Director may—

(1) expend funds for public awareness and to enhance community support of law enforcement training, including the advertisement of available law enforcement training programs;

(2) accept and use gifts of property, both real and personal, and accept gifts of services, for purposes that promote the functions of the Director pursuant to subsection (c) and the training responsibilities of the Director under subsection (d);

(3) accept reimbursement from other Federal agencies for the construction or renovation of training and support facilities and the use of equipment and technology on government owned-property;

(4) obligate funds in anticipation of reimbursements from agencies receiving training at FLETC, except that total obligations at the end of a fiscal year may not exceed total budgetary resources available at the end of the fiscal year;

(5) in accordance with the purchasing authority provided under section 10392(a) and (b) of this title—

(A) purchase employee and student uniforms; and

(B) purchase and lease passenger motor vehicles, including vehicles for police-type use;

(6) provide room and board for student interns; and

(7) expend funds each fiscal year to honor and memorialize FLECT graduates who have died in the line of duty.

(g) PROHIBITION ON NEW FUNDING.—No funds are authorized to carry out this section. This section shall be carried out using amounts otherwise appropriated or made available for that purpose.

§ 10398. Fees

(a) FEES FOR CREDENTIALING AND BACKGROUND INVESTIGATIONS IN TRANSPORTATION.—The Secretary shall charge reasonable fees for providing credentialing and background investigations in the field of transportation. The establishment and collection of fees shall be subject to the following requirements:

(1) Fees, in the aggregate, shall not exceed the costs incurred by the Department associated with providing the credential or performing the background record checks.

(2) The Secretary shall charge fees in amounts that are reasonably related to the costs of providing services in connection with the activity or item for which the fee is charged.

(3) A fee may not be collected except to the extent the fee will be expended to pay for—

(A) the costs of conducting or obtaining a criminal history record check and a review of available law enforcement databases and commercial databases and records of other governmental and international agencies;

(B) reviewing and adjudicating requests for waiver and appeals of agency decisions with respect to providing the credential, performing the background record check, and denying requests for waiver and appeals; and

(C) other costs related to providing the credential or performing the background record check.

(4) A fee collected shall be available for expenditure only to pay the costs incurred in providing services in connection with the activity or item for which the fee is charged and shall remain available until expended.

(b) RECURRENT TRAINING OF ALIENS IN OPERATION OF AIRCRAFT.—

(1) PROCESS FOR REVIEWING THREAT ASSESSMENTS.—Notwithstanding section 40959(a)(1) of this title, the Secretary shall establish a process to ensure that an alien (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)) applying for recurrent training in the operation of an aircraft is properly identified and has not, since the time of a prior threat assessment conducted under section 40959(a)(2) of this title, become a risk to aviation or national security.

(2) INTERRUPTION OF TRAINING.—If the Secretary determines, in carrying out the process established under paragraph (1), that an alien is a present risk to aviation or national security, the Secretary shall immediately notify the person providing the training of the determination and that person shall not provide the training or, if training has commenced, that person shall immediately terminate the training.

(3) FEES.—The Secretary may charge reasonable fees under subsection (a) for providing credentialing and background investigations for aliens in connection with the process for recurrent training established under paragraph (1). The fees shall be promulgated by notice in the Federal Register.

(c) COLLECTION OF FEES FROM NON-FEDERAL PARTICIPANTS IN MEETINGS.—

(1) IN GENERAL.—The Secretary may collect fees from a non-Federal participant in a conference, seminar, exhibition, symposium, or similar meeting conducted by the Department in advance of the conference, either directly or by contract, and those fees shall be credited to the appropriation or account from which the costs of the conference,

seminar, exhibition, symposium, or similar meeting are paid and shall be available to pay the costs of the Department with respect to the conference or to reimburse the Department for costs incurred with respect to the conference.

(2) DEPOSIT OF EXCESS FEES.—If the total amount of fees collected with respect to a conference exceeds the actual costs of the Department with respect to the conference, the excess amount shall be deposited into the Treasury as miscellaneous receipts.

§ 10399. Reports to Committee on Commerce, Science, and Transportation

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

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

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

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

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

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

§ 10400. Annual ammunition and weaponry reports

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

(1) A comprehensive report on the purchase and usage of ammunition, subdivided by ammunition type.

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

(b) CONTENTS.—

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

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

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

(C) details on all contracting practices applied by the Department, including comparative details regarding other contracting options with respect to cost and availability.

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

(A) the quantity of weapons in inventory at the end of the preceding calendar year, and the amount of weapons, subdivided by weapon type, included in the budget request for each relevant component or agency in the Department;

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

(C) details on all contracting practices applied by the Department, including comparative details regarding other contracting options with respect to cost and availability.

(c) REPORT SUBMITTED IN APPROPRIATE FORMAT.—Each report shall be submitted in an appropriate format to ensure the safety of law enforcement personnel.

§ 10401. National identification system not authorized

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

§ 10402. Functions and authorities of Administrator of General Services not affected

(a) OPERATION, MAINTENANCE, AND PROTECTION OF FEDERAL BUILDINGS AND GROUNDS.—Nothing in this subtitle may be construed to affect the functions or authorities of the Administrator of General Services with respect to the operation, maintenance, and protection of buildings and grounds owned or occupied by the Federal Government and under the jurisdiction, custody, or control of the Administrator. Except for the law enforcement and related security functions transferred under section 11101(b)(1)(C) of this title, the Administrator shall retain all powers, functions, and authorities vested in the Administrator under chapters 1 (except section 121(e)(2)(A)) and 5 through 11 of title 40, and other provisions of law that are necessary for the operation, maintenance, and protection of the buildings and grounds.

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

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

(A) to direct the transfer of, or affect, the authority of the Administrator of General Services to collect rents and fees, including fees collected for protective services; or

(B) to authorize the Secretary or another official in the Department to obligate amounts in the Federal Buildings Fund established by section 592 of title 40.

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

§ 10403. Research and development pilot program

(a) AUTHORITY.—Until September 30, 2024, and subject to subsection (c), the Secretary may carry out a pilot program under which the Secretary may exercise the following authorities:

(1) RESEARCH AND DEVELOPMENT PROJECTS.—When the Secretary carries out basic, applied, and advanced research and development projects, including the expenditure of funds for the projects, the Secretary may exercise the same authority (subject to the same limitations and conditions) with respect to the research and projects as the Secretary of Defense may exercise under section 4021 of title 10 (except for subsections (b) and (f)), after making a determination that the use of a contract, grant, or cooperative agreement for the project is not feasible or appropriate.

(2) PROTOTYPE PROJECTS.—The Secretary—

(A) may, under the authority of paragraph (1), carry out prototype projects under section 4022 of title 10; and

(A) in applying the authorities of section 4022 of title 10, shall perform the functions of the Secretary of Defense as prescribed in section 4022.

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

(1) procure the temporary or intermittent services of experts or consultants (or organizations of experts or consultants) in accordance with section 3109(b) of title 5; and

(2) whenever necessary due to an urgent homeland security need, procure temporary (not to exceed 1 year) or intermittent personal services, including the services of experts or consultants (or organizations

of experts or consultants), without regard to the pay limitations of section 3109 of title 5.

(c) ADDITIONAL REQUIREMENTS.—

(1) IN GENERAL.—The authority of the Secretary under this section shall terminate September 30, 2024, unless before that date the Secretary—

(A) issues policy guidance detailing the appropriate use of that authority; and

(B) provides training to each employee who may exercise that authority.

(2) REPORT.—The Secretary shall provide an annual report to the Committees on Appropriations of the Senate and the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives detailing the projects for which the authority granted by subsection (a) was used, the rationale for its use, the funds spent using that authority, the outcome of each project for which that authority was used, and the results of any audits of the projects.

§ 10404. Protection of certain facilities and assets from unmanned aircraft

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Homeland Security, the Committee on Transportation and Infrastructure, the Committee on Energy and Commerce, and the Committee on the Judiciary of the House of Representatives.

(2) BUDGET.—The term ''budget'', with respect to a fiscal year, means the budget for that fiscal year that is submitted to Congress by the President under section 1105(a) of title 31.

(3) COVERED FACILITY OR ASSET.—The term ''covered facility or asset'' means a facility or asset that—

(A) is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Secretary or the Attorney General, in coordination with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section (except that in the case of the missions described in clauses (i)(II) and (iii)(I) of subpara-

graph (C), the missions shall be presumed to be for the protection of a facility or asset that is assessed to be high-risk and a potential target for unlawful unmanned aircraft activity);

(B) is located in the United States (including the territories and possessions, territorial seas, or navigable waters of the United States); and

(C) directly relates to 1 or more—

(i) missions authorized to be performed by the Department, consistent with governing statutes, regulations, and orders issued by the Secretary, pertaining to—

(I) security or protection functions of U.S. Customs and Border Protection, including securing or protecting facilities, aircraft, and vessels, whether moored or underway;

(II) United States Secret Service protection operations pursuant to sections 3056(a) and 3056A(a) of title 18 and the Presidential Protection Assistance Act of 1976 (18 U.S.C. 3056 note); or

(III) protection of facilities pursuant to section 1315(a) of title 40;

(ii) missions authorized to be performed by the Department of Justice, consistent with governing statutes, regulations, and orders issued by the Attorney General, pertaining to—

(I) personal protection operations by—

(aa) the Federal Bureau of Investigation as specified in section 533 of title 28; and

(bb) the United States Marshals Service of Federal jurists, court officers, witnesses, and other threatened individuals in the interests of justice, as specified in section 566(e)(1)(A) of title 28;

(II) protection of penal, detention, and correctional facilities and operations conducted by the Federal Bureau of Prisons; or

(III) protection of the buildings and grounds leased, owned, or operated by or for the Department of Justice, and the provision of security for Federal courts, as specified in section 566(a) of title 28;

(iii) missions authorized to be performed by the Department or the Department of Justice, acting together or separately, consistent with governing statutes, regulations, and or-

ders issued by the Secretary or the Attorney General, respectively, pertaining to—

(I) protection of a National Special Security Event and Special Event Assessment Rating event;

(II) the provision of support to State, local, territorial, or tribal law enforcement, on request of the chief executive officer of the State or territory, to ensure protection of people and property at mass gatherings, that is limited to a specified time frame and location, within available resources, and without delegating any authority under this section to State, local, territorial, or tribal law enforcement; or

(III) protection of an active Federal law enforcement investigation, emergency response, or security function, that is limited to a specified time frame and location; or

(iv) missions authorized to be performed by the Coast Guard, including those described in clause (iii) as directed by the Secretary, and as further set forth in section 528 of title 14, and consistent with governing statutes, regulations, and orders issued by the Secretary of the Department in which the Coast Guard is operating.

(4) ELECTRONIC COMMUNICATION; INTERCEPT; ORAL COMMUNICATION; WIRE COMMUNICATION.—The terms ''electronic communication'', ''intercept'', ''oral communication'', and ''wire communication'' have the meanings given those terms in section 2510 of title 18.

(5) HOMELAND SECURITY OR JUSTICE BUDGET MATERIALS.—The term ''homeland security or justice budget materials'', with respect to a fiscal year, means the materials submitted to Congress by the Secretary and the Attorney General in support of the budget for that fiscal year.

(6) RISK-BASED ASSESSMENT.—The term ''risk-based assessment'' includes an evaluation of threat information specific to a covered facility or asset and, with respect to potential impacts on the safety and efficiency of the national airspace system and the needs of law enforcement and national security at each covered facility or asset identified by the Secretary or the Attorney General, respectively, an evaluation of each of the following factors:

(A) Potential impacts to safety, efficiency, and use of the national airspace system, including potential effects on manned aircraft and unmanned aircraft systems, aviation safety, airport operations, infrastructure, and air navigation services related to the

use of any system or technology for carrying out the actions described in subsection (c)(1).

(B) Options for mitigating identified impacts to the national airspace system related to the use of any system or technology, including minimizing when possible the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

(C) Potential consequences of the impacts of actions taken under subsection (c)(1) to the national airspace system and infrastructure if not mitigated.

(D) The ability to provide reasonable advance notice to aircraft operators consistent with the safety of the national airspace system and the needs of law enforcement and national security.

(E) The setting and character of a covered facility or asset, including whether it is located in a populated area or near other structures, whether the facility is open to the public, whether the facility is also used for nongovernmental functions, and any potential for interference with wireless communications or for injury or damage to individuals or property.

(F) The setting, character, time frame, and national airspace system impacts of National Special Security Events and Special Event Assessment Rating events.

(G) Potential consequences to national security, public safety, or law enforcement if threats posed by unmanned aircraft systems are not mitigated or defeated.

(7) UNMANNED AIRCRAFT; UNMANNED AIRCRAFT SYSTEM.—The terms ''unmanned aircraft'' and ''unmanned aircraft system'' have the meanings given those terms in section 44801 of title 49.

(b) AUTHORITY.—Notwithstanding section 41062 of this title or sections 32, 1030, and 1367 and chapters 119 and 206 of title 18, the Secretary and the Attorney General may, for their respective Departments, take, and may authorize officers and employees of the Department or the Department of Justice with assigned duties that include the security or protection of people, facilities, or assets, to take such actions as are described in subsection (c)(1) that are necessary to mitigate a credible threat (as defined by the Secretary or the Attorney General, in consultation with the Secretary of Transportation) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset.

(c) ACTIONS DESCRIBED.—

(1) IN GENERAL.—The actions authorized in subsection (b) are the following:

(A) During the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and direct or indirect physical, electronic, radio, and electromagnetic means.

(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

(D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.

(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

(F) Use reasonable force, if necessary, to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

(2) COORDINATION WITH SECRETARY OF TRANSPORTATION.—The Secretary and the Attorney General shall develop for their respective Departments the actions described in paragraph (1) in coordination with the Secretary of Transportation.

(3) RESEARCH, TESTING, TRAINING, AND EVALUATION.—The Secretary and the Attorney General shall conduct research, testing, and training on, and evaluation of equipment, including electronic equipment, to determine its capability and utility prior to the use of that technology for an action described in paragraph (1).

(4) COORDINATION WITH ADMINISTRATOR OF FEDERAL AVIATION ADMINISTRATION.—The Secretary and the Attorney General shall coordinate with the Administrator of the Federal Aviation Administration when an action authorized by this section might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of airspace.

(d) FORFEITURE.—An unmanned aircraft system or unmanned aircraft described in subsection (b) that is seized by the Secretary or the Attorney General is subject to forfeiture to the United States.

(e) REGULATIONS AND GUIDANCE.—

(1) IN GENERAL.—The Secretary, the Attorney General, and the Secretary of Transportation may prescribe regulations and shall issue guidance in their respective areas to carry out this section.

(2) COORDINATION.—

(A) COORDINATION WITH SECRETARY OF TRANSPORTATION.—The Secretary and the Attorney General shall coordinate the development of their respective guidance under paragraph (1) with the Secretary of Transportation.

(B) COORDINATION WITH SECRETARY OF TRANSPORTATION AND ADMINISTRATOR OF FEDERAL AVIATION ADMINISTRATION.—The Secretary and the Attorney General shall respectively coordinate with the Secretary of Transportation and the Administrator of the Federal Aviation Administration before issuing any guidance, or otherwise implementing this section, if the guidance or implementation might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of airspace.

(f) PRIVACY PROTECTION.—The regulations or guidance issued to carry out actions authorized under subsection (c) by the Secretary, the Secretary of Transportation, or the Attorney General, as the case may be, shall ensure that—

(1) the interception or acquisition of, or access to, or maintenance or use of, communications to or from an unmanned aircraft system under this section is conducted in a manner consistent with the 1st and 4th Amendments to the Constitution and applicable provisions of Federal law;

(2) communications to or from an unmanned aircraft system are intercepted or acquired only to the extent necessary to support an action described in subsection (c)(1);

(3) records of the communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Secretary or the Attorney General determines that maintenance of the records is necessary to investigate or prosecute a violation of law or to directly support an ongoing security operation, is required under Federal law, or is necessary for the purpose of any litigation;

(4) the communications are not disclosed outside the Department or the Department of Justice unless the disclosure—

(A) is necessary to investigate or prosecute a violation of law;

(B) would support the Department of Defense, a Federal law enforcement agency, or the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or a regulatory, statutory, or other en-

forcement action relating to, an action described in subsection (c)(1);

(C) is between the Department and the Department of Justice in the course of a security or protection operation of either agency or a joint operation of the agencies; or

(D) is otherwise required by law; and

(5) to the extent necessary, the Department and the Department of Justice may share threat information, which shall not include communications referred to in subsection (c), with State, local, territorial, or tribal law enforcement agencies in the course of a security or protection operation.

(g) BUDGET.—The Secretary and the Attorney General shall submit to Congress, as a part of the homeland security or justice budget materials for each fiscal year a consolidated funding display that identifies the funding source for the actions described in subsection (c)(1) in the Department or the Department of Justice. The funding display shall be in unclassified form but may contain a classified annex.

(h) SEMIANNUAL BRIEFINGS AND NOTIFICATIONS.—

(1) BRIEFINGS.—

(A) IN GENERAL.—On a semiannual basis during the period beginning 6 months after October 5, 2018, and ending on the date specified in subsection (l), the Secretary and the Attorney General shall, respectively, provide a briefing to the appropriate congressional committees on the activities carried out pursuant to this section.

(B) JOINT BRIEFING REQUIRED.—Each briefing shall be conducted jointly with the Secretary of Transportation.

(C) CONTENT.—Each briefing shall include—

(i) policies, programs, and procedures to mitigate or eliminate impacts of the activities on the national airspace system;

(ii) a description of instances in which actions described in subsection (c)(1) have been taken, including all instances that may have resulted in harm, damage, or loss to a person or to private property;

(iii) a description of the guidance, policies, or procedures established to address privacy, civil rights, and civil liberties issues implicated by the actions allowed under this section, as well as any changes or subsequent efforts that would significantly affect privacy, civil rights or civil liberties;

(iv) a description of options considered and steps taken to mitigate identified impacts to the national airspace system re-

lated to the use of any system or technology, including the minimization of the use of technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1);

(v) a description of instances in which communications intercepted or acquired during the course of operations of an unmanned aircraft system were held for more than 180 days or shared outside of the Department or the Department of Justice;

(vi) how the Secretary, the Attorney General, and the Secretary of Transportation have informed the public as to the possible use of authorities under this section; and

(vii) how the Secretary, the Attorney General, and the Secretary of Transportation have engaged with Federal, State, and local law enforcement agencies to implement and use the authorities under this section.

(D) BRIEFING TO BE IN UNCLASSIFIED FORM.—Each briefing shall be in unclassified form but may be accompanied by an additional classified briefing.

(2) NOTIFICATION.—Within 30 days of deploying new technology to carry out the actions described in subsection (c)(1), the Secretary and the Attorney General shall, respectively, submit a notification to the appropriate congressional committees. The notification shall include a description of options considered to mitigate identified impacts on the national airspace system related to the use of any system or technology, including the minimization of the use of technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

(i) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

(1) vest in the Secretary or the Attorney General any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration;

(2) vest in the Secretary of Transportation or the Administrator of the Federal Aviation Administration any authority of the Secretary or the Attorney General;

(3) vest in the Secretary any authority of the Attorney General;

(4) vest in the Attorney General any authority of the Secretary; or

(5) provide a new basis of liability for State, local, territorial, or tribal law enforcement officers who participate in the protection of a mass gathering identified by the Secretary or Attorney General under sub-

section (a)(3)(C)(iii)(II), act within the scope of their authority, and do not exercise the authority granted to the Secretary and Attorney General by this section.

(j) SCOPE OF AUTHORITY.—Nothing in this section shall be construed to provide the Secretary or the Attorney General with additional authorities beyond those described in subsections (a)(3)(C)(iii) and (b).

(k) DEPARTMENT ASSESSMENT.—

(1) REPORT.—Not later than 1 year after October 5, 2018, the Secretary shall conduct, in coordination with the Attorney General and the Secretary of Transportation, an assessment to the appropriate congressional committees, including—

(A) an evaluation of the threat from unmanned aircraft systems to United States critical infrastructure (as defined in section 10101 of this title) and to domestic large hub airports (as defined in section 40102 of title 49);

(B) an evaluation of current Federal, State, local, territorial, or tribal law enforcement authorities to counter the threat identified in subparagraph (A), and recommendations, if any, for potential changes to existing authorities to allow State, local, territorial, and tribal law enforcement to assist Federal law enforcement to counter the threat where appropriate;

(C) an evaluation of the knowledge of, efficiency of, and effectiveness of current procedures and resources available to owners of critical infrastructure and domestic large hub airports when they believe a threat from unmanned aircraft systems is present and what additional actions, if any, the Department or the Department of Transportation could implement under existing authorities to assist these entities to counter the threat identified in subparagraph (A);

(D) an assessment of what, if any, additional authorities are needed by each Department and by law enforcement to counter the threat identified in subparagraph (A); and

(E) an assessment of what, if any, additional research and development the Department needs to counter the threat identified in subparagraph (A).

(2) REPORT TO BE IN UNCLASSIFIED FORM.—The report shall be submitted in unclassified form but may contain a classified annex.

(l) TERMINATION.—The authority to carry out this section with respect to a covered facility or asset specified in subsection (a)(3) shall terminate on November 18, 2023.

§ 10405. Homeland security critical domain research and development

(a) DEFINITIONS.—In this section

(1) ECONOMIC SECURITY.— The term ''economic security'' means the condition of having secure and resilient domestic production capacity, combined with reliable access to the global resources necessary to maintain an acceptable standard of living and to protect core national values.

(2) UNITED STATES CRITICAL DOMAINS FOR ECONOMIC SECURITY.— The term ''United States critical domains for economic security'' means the critical infrastructure and other associated industries, technologies, and intellectual property, or any combination thereof, that are essential to the economic security of the United States.

(b) IN GENERAL.—

(1) RESEARCH AND DEVELOPMENT.—The Secretary may conduct research and development to—

(A) identify United States critical domains for economic security and homeland security; and

(B) evaluate the extent to which disruption, corruption, exploitation, or dysfunction of any critical domain poses a substantial threat to homeland security.

(2) REQUIREMENTS.—

(A) RISK ANALYSIS OF CRITICAL DOMAINS.—The research under paragraph (1) shall include a risk analysis of each identified United States critical domain for economic security to determine the degree to which there exists a present or future threat to homeland security in the event of disruption, corruption, exploitation, or dysfunction to the domain. The research shall consider, to the extent possible, the following:

(i) The vulnerability and resilience of relevant supply chains.

(ii) Foreign production, processing, and manufacturing methods.

(iii) Influence of malign economic actors.

(iv) Asset ownership.

(v) Relationships in the supply chains of the domains.

(vi) The degree to which the conditions referred to in clauses (i) through (v) would place a domain at risk of disruption, corruption, exploitation, or dysfunction.

(B) ADDITIONAL RESEARCH INTO HIGH-RISK CRITICAL DOMAINS.—Based on the identification and risk analysis of United

States critical domains for economic security pursuant to paragraph (1) and subparagraph (A), respectively, the Secretary may conduct additional research into those critical domains, or specific elements of those domains, with respect to which there exists the highest degree of a present or future threat to homeland security in the event of disruption, corruption, exploitation, or dysfunction to a domain. For each high-risk domain, or element of a domain, the research shall—-

(i) describe the underlying infrastructure and processes;

(ii) analyze present and projected performance of industries that comprise or support the domain;

(iii) examine the extent to which the supply chain of a product or service necessary to the domain is concentrated, either through a small number of sources, or if multiple sources are concentrated in one geographic area;

(iv) examine the extent to which the demand for supplies of goods and services of those industries can be fulfilled by present and projected performance of other industries, identify strategies, plans, and potential barriers to expand the supplier industrial base, and identify the barriers to the participation of those other industries;

(v) consider each domain's performance capacities in stable economic environments, under adversarial supply conditions, and under crisis economic constraints;

(vi) identify and define needs and requirements to establish supply resiliency within each domain; and

(vii) consider the effects of sector consolidation, including foreign consolidation, either through mergers or acquisitions, or due to recent geographic realignment, on those industries' performances.

(3) CONSULTATION.—In conducting the research under paragraphs (1) and (2)(B), the Secretary may consult with appropriate Federal agencies, State agencies, and private sector stakeholders.

(4) PUBLICATION.— Beginning December 27, 2022, the Secretary shall publish a report containing information relating to the research under paragraphs (1) and (2)(B), including findings, evidence, analysis, and recommendations. The report shall be updated annually through 2026.

(c) SUMISSION OF REPORT TO CONGRESS.—Not later than 90 days after the publication of each report required under subsection (b)(4), the Secretary shall transmit to the Committee on Homeland Security of the House

of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the report, together with a description of actions the Secretary, in consultation with appropriate Federal agencies, will undertake or has undertaken in response to the report.

(d) AUTHORIZATOIN OF APPROPRIATIONS.—There is authorized to be appropriated $1,000,000 for each of fiscal years 2023 through 2026 to carry out this section.

§ 10406. Department of Homeland Security Nonrecurring Expenses Fund

(a) ESTABLISHMENT.—There is in the Treasury the Department of Homeland Security Nonrecurring Expenses Fund (in this section referred to as ''the Fund'').

(b) TRANSFER OF UNOBLIGATED BALANCES OF EXPIRED DISCRETIONARY AMOUNTS.—Unobligated balances of expired discretionary amounts appropriated for a fiscal year from the General Fund of the Treasury to the Department by any Act may be transferred (not later than the end of the 5th fiscal year after the last fiscal year for which the amounts are available for the purposes for which appropriated) into the Fund.

(c) AVAILABILITY OF AMOUNTS.—Amounts deposited in the Fund shall be available until expended, in addition to such other funds as may be available for those purposes, for information technology system modernization and facilities infrastructure improvements necessary for the operation of the Department, subject to approval by the Office of Management and Budget.

NOTIFICATION OF PLANNED USE OF AMOUNTS.—Amounts in the Fund may be obligated only after the Committees on Appropriations of the House of Representatives and the Senate are notified at least 15 days in advance of the planned use of amounts.

§ 10407. Mentor firm-protege firm program

(a) DEFINITIONS.—In this section:

(1) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term ''historically Black college or university'' has the meaning given the term ''part B institution'' insection 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

(2) MENTOR FIRM.—The term ''mentor firm'' means a for-profit business concern that is not a small business concern that—

(A) has the ability to assist and commits to assisting a protege to compete for Federal prime contracts and subcontracts; and

(B) satisfies any other requirements imposed by the Secretary.

(3) MINORITY-SERVING INSTITUTION.—The term ''minority-serving institution'' means an institution of higher education described

insection 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

(4) PROTEGE FIRM.—The term ''protege firm'' means a small business concern, a historically Black college or university, or a minority-serving institution that—-

(A) is eligible to enter into a prime contract or subcontract with the Department; and

(B) satisfies any other requirements imposed by the Secretary.

(5) SMALL BUSINESS ACT DEFINITIONS.—The terms ''small business concern'', ''small business concern owned and controlled by veterans'', ''small business concern owned and controlled by service-disabled veterans'', ''qualified HUBZone small business concern'', and ''smallbusiness concern owned and controlled by women'' have the meanings giventhe terms, respectively, undersection 3 of the Small Business Act (15 U.S.C. 632). The term ''small business concern owned and controlled by socially and economically disadvantaged individuals'' has the meaning given the term insection 8(d)(3)(C) of the Small business Act (15 U.S.C. 637(d)(3)(C)).

(b) ESTABLISHMENT.—There is in the Department a mentor-protege program (in this section referred to as the ''Program'') under which a mentor firm enters into an agreement with a protege firm for the purpose of assisting the protege firm to compete for prime contracts and subcontracts of the Department.

(c) ELIGIBILITY.—The Secretary shall establish criteria for mentor firms and protege firms to be eligible to participate in the Program, including a requirement that a firm is not included on any list maintained by the Federal Government of contractors that have been suspended or debarred.

(d) PROGRAM APPLICATION AND APPROVAL.—

(1) APPLICATION.— The Secretary, acting through the Office of Small and Disadvantaged Business Utilization of the Department, shall establish a process for submission of an application jointly by a mentor firm and the protege firm selected by the mentor firm. The application shall include each of the following:

(A) A description of the assistance to be provided by the mentor firm, including, to the extent available, the number and a brief description of each anticipated subcontract to be awarded to the protege firm.

(B) A schedule with milestones for achieving the assistance to be provided over the period of participation in the Program.

(C) An estimate of the costs to be incurred by the mentor firm for providing assistance under the Program.

(D) Attestations that Program participants will submit to the Secretary reports at times specified by the Secretary to assist the Secretary in evaluating the protege firm's developmental progress.

(E) Attestations that Program participants will inform the Secretary in the event of a change in eligibility or voluntary withdrawal from the Program.

(2) APPROVAL.—Not later than 60 days after receipt of an application pursuant to paragraph (1), the head of the Office of Small and Disadvantaged Business Utilization shall notify applicants of approval or, in the case of disapproval, the process for resubmitting an application for reconsideration.

(3) RESCISSION.—The head of the Office of Small and Disadvantaged Business Utilization may rescind the approval of an application under this subsection if it determines that the action is in the best interest of the Department.

(e) PROGRAM DURATION.—A mentor firm and protege firm approved under subsection (d) shall enter into an agreement to participate in the Program for a period of not less than 36 months.

(f) PROGRAM BENEFITS.—A mentor firm and protege firm that enter into an agreement under subsection (e) may receive the following Program benefits:

(1) With respect to an award of a contract that requires a subcontracting plan, a mentor firm may receive evaluation credit for participating in the Program.

(2) With respect to an award of a contract that requires a subcontracting plan, a mentor firm may receive credit for a protege firm performing as a first tier subcontractor or a subcontractor at any tier in an amount equal to the total dollar value of any subcontracts awarded to the protege firm.

(3) A protege firm may receive technical, managerial, financial, or any other mutually agreed upon benefit from a mentor firm, including a subcontract award.

(g) REPORTING.—Not later than December 23, 2023, and annually thereafter, the head of the Office of Small and Disadvantaged Business Utilization shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Small Business and Entrepreneurship of the Senate and the Committee on Homeland Security and the Committee on Small Business of the House of Representatives a report that—

(1) identifies each agreement between a mentor firm and a protege firm entered into under this section, including the number of protege firm participants that are—

(A) small business concerns;

(B) small business concerns owned and controlled by veterans;

(C) small business concerns owned and controlled by service-disabled veterans;

(D) qualified HUBZone small business concerns;

(E) small business concerns owned and controlled by socially and economically disadvantaged individuals;

(F) small business concerns owned and controlled by women;

(G) historically Black colleges and universities; and

(H) minority-serving institutions;

(2) describes the type of assistance provided by mentor firms to protege firms;

(3) identifies contracts in the Department in which a mentor firm serving as the prime contractor provided subcontracts to a protege firm under the Program; and

(4) assesses the degree to which there has been—

(A) an increase in the technical capabilities of protege firms; and

(B) an increase in the quantity and estimated value of prime contract and subcontract awards to protege firms for the period covered by the report.

(h) RULE OF CONSTRUCTION.—Nothing in this section may be construed to limit, diminish, impair, or otherwise affect the authority of the Department to participate in any program carried out by or requiring approval of the Small Business Administration or adopt or follow any regulation or policy that the Administrator of the Small Business Administration may promulgate, except that, to the extent that any provision of this section (including subsection (a)) conflicts with any other provision of law, regulation, or policy, this section shall control.Bottom of FormTop of Form

Chapter 105—Information Analysis

§ 10501. Discharging responsibilities

(a) IN GENERAL.—The Secretary shall ensure that the responsibilities of the Department relating to information analysis, including those described in subsection (b), are carried out through the Under Secretary for Intelligence and Analysis.

(b) RESPONSIBILITIES OF SECRETARY.—The responsibilities of the Secretary relating to intelligence and analysis shall be as follows:

(1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private-sector entities, and to integrate the information, in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 (50 U.S.C. 3056), to—

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

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

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

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

(3) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether the information, analysis, or assessments are provided by or produced by the Department) in order to—

(A) identify priorities for protective and support measures regarding terrorist and other threats to homeland security by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities; and

(B) prepare finished intelligence and information products in both classified and unclassified formats, as appropriate, whenever reasonably expected to be of benefit to a State, local, or tribal government (including a State, local, or tribal law enforcement agency) or a private-sector entity.

(4) To ensure, under section 10502 of this title, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining the information from other agencies of the Federal Government.

(5) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information within the scope of the information sharing environment established under section 11908 of this title, including homeland security information, terrorism information, and weapons of mass destruction information, and policies, guidelines, procedures, instructions, or standards established under that section.

(6) To disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private-sector entities with equivalent responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

(7) To consult with the Director of National Intelligence and other appropriate intelligence, law enforcement, or other elements of the Federal Government to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism against the United States through such means as the representation of the Department in discussions regarding requirements and priorities in the collection of the information.

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

(9) To ensure that—

(A) material received pursuant to this subtitle is protected from unauthorized disclosure and handled and used only for the performance of official duties; and

(B) intelligence information under this subtitle is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and

methods under the National Security Act of 1947 (50 U.S.C. 3001 et seq.) and related procedures and, as appropriate, similar authorities of the Attorney General concerning sensitive law enforcement information.

(10) To request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain the information.

(11) To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(12) To ensure, in conjunction with the chief information officer of the Department, that information databases and analytical tools developed or utilized by the Department—

(A) are compatible with one another and with relevant information databases of other agencies of the Federal Government; and

(B) treat information in the databases in a manner that complies with applicable Federal law on privacy.

(13) To coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

(14) To coordinate with elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.

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

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

(17) To establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and

procedures for the intelligence components of the Department, consistent with directions from the President and, as applicable, the Director of National Intelligence.

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

(19) To ensure that, whenever possible, the Department—

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

(B) produces and disseminates the reports and analytic products contemporaneously with reports or analytic products concerning the same or similar information that the Department produced and disseminated in a classified format.

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

(21) Based on intelligence priorities set by the President, and guidance from the Secretary and, as appropriate, the Director of National Intelligence—

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

(B) to present to the Secretary a recommendation for a consolidated budget for the intelligence components of the Department, together with comments from the heads of the components.

(22) To perform such other duties relating to the responsibilities as the Secretary may provide.

(23)(A) Not later than 6 months after December 23, 2016, to conduct an intelligence-based review and comparison of the risks and consequences of EMP and GMD facing critical infrastructure and submit to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate a recommended strategy to protect and prepare the critical infrastructure of the homeland against threats of EMP and GMD. The recommended strategy shall—

(i) be based on findings of the research and development conducted under section 10918 of this title;

(ii) be developed in consultation with the relevant Federal Sector Risk Management Agencies (as defined under Presidential Policy Directive–21) for critical infrastructure;

(iii) be developed in consultation with the relevant sector coordinating councils for critical infrastructure;

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

(v) be submitted in unclassified form, but may include a classified annex.

(B) Not less frequently than every 2 years after the strategy is submitted, for the next 6 years, to submit updates of the recommended strategy.

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

(c) STAFF.—

(1) IN GENERAL.—The Secretary shall provide the Office of Intelligence and Analysis with a staff of analysts having appropriate expertise and experience to assist the offices in discharging responsibilities under this section.

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

(3) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(d) DETAIL OF PERSONNEL.—

(1) IN GENERAL.—To assist the Office of Intelligence and Analysis in discharging responsibilities under this section, personnel of the agencies listed in paragraph (2) may be detailed to the Department for the performance of analytic functions and related duties.

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

(A) The Department of State.

(B) The Central Intelligence Agency.

(C) The Federal Bureau of Investigation.

(D) The National Security Agency.

(E) The National Geospatial-Intelligence Agency.

(F) The Defense Intelligence Agency.

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

(3) COOPERATIVE AGREEMENTS.—The Secretary and the head of the agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

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

(e) FUNCTIONS TRANSFERRED.—The Secretary succeeds to, and there is assigned to the Office of Intelligence and Analysis and the Office of Infrastructure Protection, the functions, personnel, assets, and liabilities of the following entities:

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

(2) The National Communications System of the Department of Defense, including the functions of the Secretary of Defense relating thereto.

(3) The Critical Infrastructure Assurance Office of the Department of Commerce, including the functions of the Secretary of Commerce relating thereto.

(4) The National Infrastructure Simulation and Analysis Center of the Department of Energy and the energy security and assurance program and activities of the Department of Energy, including the functions of the Secretary of Energy relating thereto.

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

§ 10502. Access to information

(a) IN GENERAL.—

(1) THREAT AND VULNERABILITY INFORMATION.—Except as otherwise directed by the President, the Secretary shall have access the Secretary considers necessary to all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary, and to all information concerning infrastructure or other vulnerabilities of the United States to terrorism, whether or not the information has been analyzed, that may be collected, possessed, or prepared by an agency of the Federal Government.

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

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

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

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

(A) all reports (including information reports containing intelligence which has not been fully evaluated), assessments, and analytical information relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary;

(B) all information concerning the vulnerability of the infrastructure of the United States, or other vulnerabilities of the United States, to terrorism, whether or not the information has been analyzed;

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

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

(c) TREATMENT UNDER CERTAIN LAWS.—The Secretary shall be deemed to be a Federal law enforcement, intelligence, protective, national defense, immigration, or national security official, and shall be provided with all information from law enforcement agencies that is required to be given to the Director of National Intelligence, under any provision of the following:

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

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

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

(d) ACCESS TO INTELLIGENCE AND OTHER INFORMATION.—

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

(2) SHARING OF INFORMATION.—The Secretary, in consultation with the Director of National Intelligence, shall work to ensure that intelligence or other information relating to terrorism to which the De-

partment has access is appropriately shared with the elements of the Federal Government referred to in paragraph (1), as well as with State and local governments, as appropriate.

§ 10503. Terrorist travel program

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

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

(1) the Assistant Secretary for Policy; or

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

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

(1) developing relevant strategies and policies;

(2) reviewing the effectiveness of existing programs and recommending improvements, if necessary;

(3) making recommendations on budget requests and on the allocation of funding and personnel;

(4) ensuring effective coordination, with respect to policies, programs, planning, operations, and dissemination of intelligence and information relating to terrorist travel—

(A) among appropriate subdivisions of the Department, as determined by the Secretary and including—

(i) U.S. Customs and Border Protection;

(ii) U.S. Immigration and Customs Enforcement;

(iii) U.S. Citizenship and Immigration Services;

(iv) the Transportation Security Administration; and

(v) the Coast Guard; and

(B) between the Department and other appropriate Federal agencies; and

(5) serving as the Secretary's primary point of contact with the National Counterterrorism Center for implementing initiatives related to terrorist travel and ensuring that the recommendations of the Center related to terrorist travel are carried out by the Department.

§ 10504. Homeland Security Advisory System

(a) IN GENERAL.—The Secretary shall administer the Homeland Security Advisory System under this section to provide advisories or warnings regarding the threat or risk that acts of terrorism will be committed on the homeland to Federal, State, local, and tribal government authorities and to the people of the United States, as appropriate. The Secretary shall exercise primary responsibility for providing the advisories or warnings.

(b) REQUIRED ELEMENTS.—In administering the Homeland Security Advisory System, the Secretary shall—

(1) establish criteria for the issuance and revocation of the advisories or warnings;

(2) develop a methodology, relying on the criteria established under paragraph (1), for the issuance and revocation of the advisories or warnings;

(3) provide, in each advisory or warning, specific information and advice regarding appropriate protective measures and countermeasures that may be taken in response to the threat or risk, at the maximum level of detail practicable, to enable individuals, government entities, emergency response providers, and the private sector to act appropriately;

(4) whenever possible, limit the scope of each advisory or warning to a specific region, locality, or economic sector believed to be under threat or at risk; and

(5) not, in issuing an advisory or warning, use color designations as the exclusive means of specifying homeland security threat conditions that are the subject of the advisory or warning.

§ 10505. Homeland security information sharing

(a) INFORMATION SHARING.—Consistent with section 11908 of this title, the Secretary, acting through the Under Secretary for Intelligence and Analysis, shall integrate the information and standardize the format of the products of the intelligence components of the Department containing homeland security information, terrorism information, weapons of mass destruction information, or national intelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) except for internal security protocols or personnel information of the intelligence components, or other administrative processes that are administered by any chief security officer of the Department.

(b) INFORMATION SHARING AND KNOWLEDGE MANAGEMENT OFFICERS.—For each intelligence component of the Department, the Secretary shall designate an information sharing and knowledge management officer who shall report to the Under Secretary for Intelligence and Analysis re-

garding coordinating the different systems used in the Department to gather and disseminate homeland security information or national intelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

(c) STATE, LOCAL, AND PRIVATE-SECTOR SOURCES OF INFORMATION.—

(1) ESTABLISHMENT OF BUSINESS PROCESSES.—The Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate, shall—

(A) establish Department-wide procedures for the review and analysis of information provided by State, local, and tribal governments and the private sector;

(B) as appropriate, integrate the information into the information gathered by the Department and other departments and agencies of the Federal Government; and

(C) make available the information, as appropriate, within the Department and to other departments and agencies of the Federal Government.

(2) FEEDBACK.—The Secretary shall develop mechanisms to provide feedback regarding the analysis and utility of information provided by an entity of State, local, or tribal government or the private sector that provides the information to the Department.

(d) TRAINING AND EVALUATION OF EMPLOYEES.—

(1) TRAINING.—The Secretary, acting through the Under Secretary for Intelligence and Analysis or the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate, shall provide to employees of the Department opportunities for training and education to develop an understanding of—

(A) the definitions of homeland security information and national intelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)); and

(B) how information available to the employees as part of their duties—

(i) might qualify as homeland security information or national intelligence; and

(ii) might be relevant to the Office of Intelligence and Analysis and the intelligence components of the Department.

(2) EVALUATIONS.—The Under Secretary for Intelligence and Analysis shall—

(A) on an ongoing basis, evaluate how employees of the Office of Intelligence and Analysis and the intelligence components of the Department are utilizing homeland security information or na-

tional intelligence, sharing information within the Department, as described in this title, and participating in the information sharing environment established under section 11908 of this title; and

(B) provide to the appropriate component heads regular reports regarding the evaluations under subparagraph (A).

(e) RECEIPT OF INFORMATION FROM UNITED STATES SECRET SERVICE.—

(1) IN GENERAL.—The Under Secretary for Intelligence and Analysis shall receive from the United States Secret Service homeland security information, terrorism information, weapons of mass destruction information (as these terms are defined in section 11908 of this title), or national intelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), as well as suspect information obtained in criminal investigations. The United States Secret Service shall cooperate with the Under Secretary for Intelligence and Analysis with respect to activities under this section and section 10506 of this title.

(2) SAVINGS CLAUSE.—Nothing in the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 266) shall interfere with the operation of section 3056(g) of title 18, or with the authority of the Secretary or the Director of the United States Secret Service regarding the budget of the United States Secret Service.

§ 10506. Comprehensive information technology network architecture

(a) DEFINITION OF COMPREHENSIVE INFORMATION TECHNOLOGY NETWORK ARCHITECTURE.—The term ''comprehensive information technology network architecture'' means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the strategic management and information resources management goals of the Office of Intelligence and Analysis.

(b) ESTABLISHMENT.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall establish, consistent with the policies and procedures developed under section 11908 of this title, and consistent with the enterprise architecture of the Department, a comprehensive information technology network architecture for the Office of Intelligence and Analysis that connects the various databases and related information technology assets of the Office of Intelligence and Analysis and the intelligence components of the Department in order to promote internal information sharing among the intelligence and other personnel of the Department.

§ 10507. Coordination with information sharing environment

(a) GUIDANCE.—All activities to comply with sections 10504, 10505, and 10506 of this title shall be—

(1) consistent with policies, guidelines, procedures, instructions, or standards established under section 11908 of this title;

(2) implemented in coordination with, as appropriate, the program manager for the information sharing environment established under that section;

(3) consistent with applicable guidance issued by the Director of National Intelligence; and

(4) consistent with applicable guidance issued by the Secretary relating to the protection of law enforcement information or proprietary information.

(b) CONSULTATION.—In carrying out the duties and responsibilities under this chapter, the Under Secretary for Intelligence and Analysis shall take into account the views of the heads of the intelligence components of the Department.

§ 10508. Intelligence components

Subject to the direction and control of the Secretary, and consistent with applicable guidance issued by the Director of National Intelligence, the responsibilities of the head of each intelligence component of the Department are as follows:

(1) To ensure that the collection, processing, analysis, and dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, weapons of mass destruction information, and national intelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), are carried out effectively and efficiently in support of the intelligence mission of the Department, as led by the Under Secretary for Intelligence and Analysis.

(2) To otherwise support and implement the intelligence mission of the Department, as led by the Under Secretary for Intelligence and Analysis.

(3) To incorporate the input of the Under Secretary for Intelligence and Analysis with respect to performance appraisals, bonus or award recommendations, pay adjustments, and other forms of commendation.

(4) To coordinate with the Under Secretary for Intelligence and Analysis in developing policies and requirements for the recruitment and selection of intelligence officials of the intelligence component.

(5) To advise and coordinate with the Under Secretary for Intelligence and Analysis on any plan to reorganize or restructure the intelligence component that would, if implemented, result in realignments of intelligence functions.

(6) To ensure that employees of the intelligence component have knowledge of, and comply with, the programs and policies established by the Under Secretary for Intelligence and Analysis and other appropriate officials of the Department and that the employees comply with all applicable laws and regulations.

(7) To perform other activities relating to the responsibilities the Secretary may provide.

§ 10509. Training for employees of intelligence components

The Secretary shall provide training and guidance for employees, officials, and senior executives of the intelligence components of the Department to develop knowledge of laws, regulations, operations, policies, procedures, and programs that are related to the functions of the Department relating to the collection, processing, analysis, and dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence (as the term is defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

§ 10510. Intelligence training development for State and local government officials

(a) CURRICULUM.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall—

(1) develop a curriculum for training State, local, and tribal government officials, including law enforcement officers, intelligence analysts, and other emergency response providers, in the intelligence cycle and Federal laws, practices, and regulations regarding the development, handling, and review of intelligence and other information; and

(2) ensure that the curriculum includes executive level training for senior level State, local, and tribal law enforcement officers, intelligence analysts, and other emergency response providers.

(b) TRAINING.—To the extent possible, the Federal Law Enforcement Training Center and other existing Federal entities with the capacity and expertise to train State, local, and tribal government officials based on the curriculum developed under subsection (a) shall be used to carry out the training programs created under this section. If the entities do not have the capacity, resources, or capabilities to conduct the training, the Secretary may approve another entity to conduct the training.

(c) CONSULTATION.—In carrying out the duties described in subsection (a), the Under Secretary for Intelligence and Analysis shall consult with the Director of the Federal Law Enforcement Training Center, the Attorney General, the Director of National Intelligence, the Administrator of the Federal Emergency Management Agency, and other appropriate parties, such as private industry, institutions of higher education, nonprofit institutions, and other intelligence agencies of the Federal Government.

§ 10511. Information sharing incentives

(a) AWARDS.—In making cash awards under chapter 45 of title 5, the President or the head of an agency, in consultation with the program manager designated under section 11908 of this title, may consider the success of an employee in appropriately sharing information within the scope of the information sharing environment established under that section, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), in a manner consistent with policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of that environment for the implementation and management of that environment.

(b) OTHER INCENTIVES.—The head of each department or agency described in section 11908(f), in consultation with the program manager designated under section 11908, shall adopt best practices regarding effective ways to educate and motivate officers and employees of the Federal Government to participate fully in the information sharing environment, including—

(1) promotions and other nonmonetary awards; and

(2) the publicizing of information sharing accomplishments by individual employees and, where appropriate, the tangible end benefits that resulted.

§ 10512. Department of Homeland Security State, Local, and Regional Fusion Center Initiative

(a) DEFINITIONS.—In this section:

(1) FUSION CENTER.—The term ''fusion center'' means a collaborative effort of two or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of the agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity.

(2) INFORMATION SHARING ENVIRONMENT.—The term ''information sharing environment'' means the information sharing environment established under section 11908 of this title.

(3) INTELLIGENCE ANALYST.—The term ''intelligence analyst'' means an individual who regularly advises, administers, supervises, or performs work in the collection, gathering, analysis, evaluation, reporting, production, or dissemination of information on political, economic, social, cultural, physical, geographical, scientific, or military conditions, trends, or forces in foreign or domestic areas that directly or indirectly affect national security.

(4) INTELLIGENCE-LED POLICING.—The term ''intelligence-led policing'' means the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision-making at the tactical and strategic levels.

(5) TERRORISM INFORMATION.—The term ''terrorism information'' has the meaning given the term in section 11908 of this title.

(b) ESTABLISHMENT.—The Secretary, in consultation with the program manager of the information sharing environment established under section 11908 of this title, the Attorney General, the Privacy Officer of the Department, the Officer for Civil Rights and Civil Liberties of the Department, and the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee), shall establish a Department of Homeland Security State, Local, and Regional Fusion Center Initiative to establish partnerships with State, local, and regional fusion centers.

(c) DEPARTMENT SUPPORT AND COORDINATION.—Through the Department of Homeland Security State, Local, and Regional Fusion Center Initiative, and in coordination with the principal officials of participating State, local, or regional fusion centers and the officers designated as the Homeland Security Advisors of the States, the Secretary shall—

(1) provide operational and intelligence advice and assistance to State, local, and regional fusion centers;

(2) support efforts to include State, local, and regional fusion centers in efforts to establish an information sharing environment;

(3) conduct tabletop and live training exercises to regularly assess the capability of individual and regional networks of State, local, and regional fusion centers to integrate the efforts of the networks with the efforts of the Department;

(4) coordinate with other relevant Federal entities engaged in homeland security-related activities;

(5) provide analytic and reporting advice and assistance to State, local, and regional fusion centers;

(6) review information within the scope of the information sharing environment, including homeland security information, terrorism infor-

mation, and weapons of mass destruction information, that is gathered by State, local, and regional fusion centers, and to incorporate the information, as appropriate, into the Department's own information;

(7) provide management assistance to State, local, and regional fusion centers;

(8) serve as a point of contact to ensure the dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(9) facilitate close communication and coordination between State, local, and regional fusion centers and the Department;

(10) provide State, local, and regional fusion centers with expertise on Department resources and operations;

(11) provide training to State, local, and regional fusion centers and encourage the fusion centers to participate in terrorism threat-related exercises conducted by the Department; and

(12) carry out other duties the Secretary determines are appropriate.

(d) PERSONNEL ASSIGNMENT.—

(1) IN GENERAL.—The Under Secretary for Intelligence and Analysis shall, to the maximum extent practicable, assign officers and intelligence analysts from components of the Department to participating State, local, and regional fusion centers.

(2) PERSONNEL SOURCES.—Officers and intelligence analysts assigned to participating fusion centers under this subsection may be assigned from the following Department components, in coordination with the respective component head and in consultation with the principal officials of participating fusion centers:

(A) Office of Intelligence and Analysis.

(B) Cybersecurity and Infrastructure Security Agency.

(C) Transportation Security Administration.

(D) U.S. Customs and Border Protection.

(E) U.S. Immigration and Customs Enforcement.

(F) Coast Guard.

(G) Other components of the Department, as determined by the Secretary.

(3) QUALIFYING CRITERIA.—

(A) IN GENERAL.—The Secretary shall develop qualifying criteria for a fusion center to participate in the assigning of Department officers or intelligence analysts under this section.

(B) CRITERIA.—Criteria developed under subparagraph (A) may include—

(i) whether the fusion center, through its mission and governance structure, focuses on a broad counterterrorism approach, and whether that broad approach is pervasive through all levels of the organization;

(ii) whether the fusion center has sufficient numbers of adequately trained personnel to support a broad counterterrorism mission;

(iii) whether the fusion center has—

(I) access to relevant law-enforcement, emergency-response, private-sector, open-source, and national-security data; and

(II) the ability to share and analytically utilize that data for lawful purposes;

(iv) whether the fusion center is adequately funded by the State, local, or regional government to support its counterterrorism mission; and

(v) the relevancy of the mission of the fusion center to the particular source component of Department officers or intelligence analysts.

(4) PREREQUISITE.—

(A) INTELLIGENCE ANALYSIS, PRIVACY, AND CIVIL LIBERTIES TRAINING.—Before being assigned to a fusion center under this section, an officer or intelligence analyst shall undergo—

(i) appropriate intelligence analysis or information sharing training using an intelligence-led policing curriculum that is consistent with—

(I) standard training and education programs offered to Department law enforcement and intelligence personnel; and

(II) the Criminal Intelligence Systems Operating Policies under part 23 of title 28, Code of Federal Regulations (or any corresponding similar rule or regulation);

(ii) appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer appointed under section 10520 of this title and the Officer for Civil Rights and Civil Liberties of the Department, in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee); and

(iii) other training prescribed by the Under Secretary for Intelligence and Analysis.

(B) PRIOR WORK EXPERIENCE IN AREA.—In determining the eligibility of an officer or intelligence analyst to be assigned to a fusion center under this section, the Under Secretary for Intelligence and Analysis shall consider the familiarity of the officer or intelligence analyst with the State, locality, or region, as determined by such factors as whether the officer or intelligence analyst—

(i) has been previously assigned in the geographic area; or

(ii) has previously worked with intelligence officials or law enforcement or other emergency response providers from that State, locality, or region.

(5) EXPEDITED SECURITY CLEARANCE PROCESSING.—The Under Secretary for Intelligence and Analysis—

(A) shall ensure that each officer or intelligence analyst assigned to a fusion center under this section has the appropriate security clearance to contribute effectively to the mission of the fusion center; and

(B) may request that security clearance processing be expedited for each officer or intelligence analyst and may use available funds for this purpose.

(6) ADDITIONAL QUALIFICATIONS.—Each officer or intelligence analyst assigned to a fusion center under this section shall satisfy any other qualifications the Under Secretary for Intelligence and Analysis may prescribe.

(e) RESPONSIBILITIES.—An officer or intelligence analyst assigned to a fusion center under this section shall—

(1) assist law enforcement agencies and other emergency response providers of State, local, and tribal governments and fusion center personnel in using information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to develop a comprehensive and accurate threat picture;

(2) review homeland security-relevant information from law enforcement agencies and other emergency response providers of State, local, and tribal government;

(3) create intelligence and other information products derived from the information and other homeland security-relevant information provided by the Department; and

(4) assist in the dissemination of the products, as coordinated by the Under Secretary for Intelligence and Analysis, to law enforcement agencies and other emergency response providers of State, local, and tribal government, other fusion centers, and appropriate Federal agencies.

(f) BORDER INTELLIGENCE PRIORITY.—

(1) IN GENERAL.—The Secretary shall make it a priority to assign officers and intelligence analysts under this section from U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Coast Guard to participating State, local, and regional fusion centers located in jurisdictions along land or maritime borders of the United States in order to enhance the integrity of and security at the borders by helping Federal, State, local, and tribal law enforcement authorities to identify, investigate, and otherwise interdict persons, weapons, and related contraband that pose a threat to homeland security.

(2) BORDER INTELLIGENCE PRODUCTS.—When performing the responsibilities described in subsection (e), officers and intelligence analysts assigned to participating State, local, and regional fusion centers under this section shall have, as a primary responsibility, the creation of border intelligence products that—

(A) assist State, local, and tribal law enforcement agencies in deploying their resources most efficiently to help detect and interdict terrorists, weapons of mass destruction, and related contraband at land or maritime borders of the United States;

(B) promote more consistent and timely sharing of border security-relevant information among jurisdictions along land or maritime borders of the United States; and

(C) enhance the Department's situational awareness of the threat of acts of terrorism at or involving the land or maritime borders of the United States.

(g) DATABASE ACCESS.—To fulfill the objectives described under subsection (e), each officer or intelligence analyst assigned to a fusion center under this section shall have appropriate access to all relevant Federal databases and information systems, consistent with policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment for the implementation and management of that environment.

(h) CONSUMER FEEDBACK.—

(1) IN GENERAL.—The Secretary shall create a voluntary mechanism for a State, local, or tribal law enforcement officer or other emergency response provider who is a consumer of the intelligence or other infor-

mation products referred to in subsection (e) to provide feedback to the Department on the quality and utility of the intelligence products.

(2) REPORT.—The Secretary shall submit annually to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that includes a description of the consumer feedback obtained under paragraph (1) and, if applicable, how the Department has adjusted its production of intelligence products in response to that consumer feedback.

(i) RULE OF CONSTRUCTION.—

(1) IN GENERAL.—The authorities granted under this section shall supplement the authorities granted under section 10501(b) of this title, and nothing in this section shall be construed to abrogate the authorities granted under section 10501(b).

(2) PARTICIPATION.—Nothing in this section shall be construed to require a State, local, or regional government or entity to accept the assignment of officers or intelligence analysts of the Department into the fusion center of that State, locality, or region.

(j) GUIDELINES.—The Secretary, in consultation with the Attorney General, shall establish guidelines for fusion centers created and operated by State and local governments, to include standards that a fusion center shall—

(1) collaboratively develop a mission statement, identify expectations and goals, measure performance, and determine effectiveness for that fusion center;

(2) create a representative governance structure that includes law enforcement officers and other emergency response providers and, as appropriate, the private sector;

(3) create a collaborative environment for the sharing of intelligence and information among Federal, State, local, and tribal government agencies (including law enforcement officers and other emergency response providers), the private sector, and the public, consistent with policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment;

(4) leverage the databases, systems, and networks available from public- and private-sector entities, in accordance with all applicable laws, to maximize information sharing;

(5) develop, publish, and adhere to a privacy and civil liberties policy consistent with Federal, State, and local law;

(6) provide, in coordination with the Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department, appropriate privacy and civil liberties training for all State, local, tribal, and private-sector representatives at the fusion center;

(7) ensure appropriate security measures are in place for the facility, data, and personnel;

(8) select and train personnel based on the needs, mission, goals, and functions of that fusion center;

(9) offer a variety of intelligence and information services and products to recipients of fusion center intelligence and information; and

(10) incorporate law enforcement officers, other emergency response providers, and, as appropriate, the private sector, into all relevant phases of the intelligence and fusion process, consistent with the mission statement developed under paragraph (1), either through full-time representatives or liaison relationships with the fusion center to enable the receipt and sharing of information and intelligence.

(k) Fusion Center Information Sharing Strategy.—Not later than 1 year after March 2, 2020, and not less frequently than once every 5 years thereafter, the Secretary shall develop or update a strategy for Department engagement with fusion centers. The strategy shall be developed and updated in consultation with the heads of intelligence components of the Department, the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, officials of fusion centers, officers designated as Homeland Security Advisors, and the heads of other relevant agencies, as appropriate. The strategy shall include the following:

(1) Specific goals and objectives for sharing information and engaging with fusion centers through—

(A) the direct deployment of personnel from intelligence components of the Department;

(B) the use of Department unclassified and classified information sharing systems, including the Homeland Security Information Network and the Homeland Secure Data Network, or any successor systems; and

(C) any additional means.

(2) The performance metrics to be used to measure success in achieving the goals and objectives referred to in paragraph (1).

(3) A 5-year plan for continued engagement with fusion centers.

(l) Threat Information Sharing

(1) Definitions.—In this subsection:

(A) SURFACE TRANSPORTATION ASSET.—The term ''surface transportation asset'' includes facilities, equipment, or systems used to provide transportation services by—

(i) a public transportation agency (as that term is defined insection 40501 of this title);

(ii) a railroad carrier (as that term is defined insection 20102(3) of title 49);

(iii) an owner or operator of—

(I) an entity offering scheduled, fixed-route transportation services by over-the-road bus (as that term is defined insection 40701 of this title); or

(II) a bus terminal; or

(iv) other transportation facilities, equipment, or systems, as determined by the Secretary.

(B) TARGETED VIOLENCE.—The term ''targeted violence'' means an incident of violence in which an attacker selected a particular target to inflict mass injury or death with no discernable political or ideological motivation beyond mass injury or death.

(C) TERRORISM.—The term ''terrorism'' means—

(i) domestic terrorism (as that term is defined insection 2331(5) of title 18); and

(ii) international terrorism (as that term is defined insection 2331(1) of title 18).

(2) PRIORIZATION OF ASSIGNMENT OF OFFICERS AND INTELLIGENCE OFFICERS.—The Secretary shall prioritize the assignment of officers and intelligence analysts underthis section from the Transportation Security Administration and, as appropriate, from the Office of Intelligence and Analysis of the Department, to locations with participating State, local, and regional fusion centers in jurisdictions with a high-risk surface transportation asset to enhance the security of those assets, including by improving timely sharing, in a manner consistent with the protection of privacy rights, civil rights, and civil liberties, of information regarding threats of terrorism and other threats, including targeted violence.

(3) INTELLIGENCE PRODUCTS.—Officers and intelligence analysts assigned to locations with participating State, local, and regional fusion centers under this subsection shall participate in the generation and dissemination, to surface transportation assets, of transportation security intelligence products, with an emphasis on those products that relate to threats of terrorism and other threats, including targeted violence, that—

(A) assist State, local, and Tribal law enforcement agencies in deploying their resources, including personnel, most efficiently to help detect, prevent, investigate, apprehend, and respond to the threats;

(B) promote more consistent and timely sharing with and among jurisdictions of threat information; and

(C) enhance the Department's situational awareness of the threats.

(4) CLEARANCES.—The Secretary shall make available to appropriate owners and operators of surface transportation assets, and to any other person that the Secretary determines appropriate to foster greater sharing of classified information relating to threats of terrorism and other threats, including targeted violence, to surface transportation assets, the process of application for security clearances under Executive Order No. 13549 (Aug. 18, 2010, 75 Fed. Reg. 51609) or any successor Executive order.

(5) REPORTS TO CONGRESS.—

(A) SECRETARY.—Not later than December 27, 2022, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes a detailed description of the measures used to ensure privacy rights, civil rights, and civil liberties protections in carrying out this subsection.

(B) COMPTROLLER GENERAL.—Not later than December 27, 2023, the Comptroller General shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a review of the implementation of this subsection, including an assessment of the measures used to ensure privacy rights, civil rights, and civil liberties protections, and any recommendations to improve this implementation, together with any recommendations to improve information sharing with State, local, Tribal, territorial, and private sector entities to prevent, identify, and respond to threats of terrorism and other threats, including targeted violence, to surface transportation assets.

§ 10513. Homeland Security Information Sharing Fellows Program

(a) ESTABLISHMENT.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, and in consultation with the Chief

Human Capital Officer, shall establish the Homeland Security Information Sharing Fellows Program for the purpose of—

(1) detailing State, local, and tribal law enforcement officers and intelligence analysts to the Department in accordance with subchapter VI of chapter 33 of title 5, to participate in the work of the Office of Intelligence and Analysis in order to become familiar with—

(A) the relevant missions and capabilities of the Department and other Federal agencies; and

(B) the role, programs, products, and personnel of the Office of Intelligence and Analysis; and

(2) promoting information sharing between the Department and State, local, and tribal law enforcement officers and intelligence analysts by assigning the officers and analysts to—

(A) serve as a point of contact in the Department to assist in the representation of State, local, and tribal information requirements;

(B) identify information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is of interest to State, local, and tribal law enforcement officers, intelligence analysts, and other emergency response providers;

(C) assist Department analysts in preparing and disseminating products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that are tailored to State, local, and tribal law enforcement officers and intelligence analysts and designed to prepare for and thwart acts of terrorism; and

(D) assist Department analysts in preparing products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that are tailored to State, local, and tribal emergency response providers and assist in the dissemination of the products through appropriate Department channels.

(b) ELIGIBILITY.—To be eligible for selection as an Information Sharing Fellow under the Homeland Security Information Sharing Fellows Program, an individual shall—

(1) have homeland security-related responsibilities;

(2) be eligible for an appropriate security clearance;

(3) possess a valid need for access to classified information, as determined by the Under Secretary for Intelligence and Analysis;

(4) be an employee of—

(A) a State, local, or regional fusion center;

(B) a State or local law enforcement or other government entity that serves a major metropolitan area, suburban area, or rural area, as determined by the Secretary;

(C) a State or local law enforcement or other government entity with port, border, or agricultural responsibilities, as determined by the Secretary;

(D) a tribal law enforcement or other authority; or

(E) another entity the Secretary determines is appropriate; and

(5) have undergone appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer and the Officer for Civil Rights and Civil Liberties, in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee).

(c) OPTIONAL PARTICIPATION.—A State, local, or tribal law enforcement or other government entity shall not be required to participate in the Homeland Security Information Sharing Fellows Program.

(d) PROCEDURES FOR NOMINATION AND SELECTION.—

(1) IN GENERAL.—The Under Secretary for Intelligence and Analysis shall establish procedures to provide for the nomination and selection of individuals to participate in the Homeland Security Information Sharing Fellows Program.

(2) LIMITATIONS.—The Under Secretary for Intelligence and Analysis shall—

(A) select law enforcement officers and intelligence analysts representing a broad cross-section of State, local, and tribal agencies; and

(B) ensure that the number of Information Sharing Fellows selected does not impede the activities of the Office of Intelligence and Analysis.

§ 10514. Rural Policing Institute

(a) DEFINITION OF RURAL.—In this section, the term ''rural'' means an area—

(1) that is not located in a metropolitan statistical area, as defined by the Office of Management and Budget; or

(2) that is located in a metropolitan statistical area and a county, borough, parish, or area under the jurisdiction of an Indian tribe with a population of not more than 50,000.

(b) IN GENERAL.—The Secretary shall establish a Rural Policing Institute, which shall be administered by the Federal Law Enforcement Training Center, to target training to law enforcement agencies and other emergency response providers located in rural areas. The Secretary, through the Rural Policing Institute, shall—

(1) evaluate the needs of law enforcement agencies and other emergency response providers in rural areas;

(2) develop expert training programs designed to address the needs of law enforcement agencies and other emergency response providers in rural areas as identified in the evaluation conducted under paragraph (1), including training programs about intelligence-led policing and protections for privacy, civil rights, and civil liberties;

(3) provide the training programs developed under paragraph (2) to law enforcement agencies and other emergency response providers in rural areas; and

(4) conduct outreach efforts to ensure that local and tribal governments in rural areas are aware of the training programs developed under paragraph (2) so they can avail themselves of the programs.

(c) CURRICULA.—The training at the Rural Policing Institute established under subsection (b) shall—

(1) be configured in a manner so as not to duplicate or displace a law enforcement or emergency response program of the Federal Law Enforcement Training Center or a local or tribal government entity in existence on August 3, 2007; and

(2) to the maximum extent practicable, be delivered in a cost-effective manner at facilities of the Department, on closed military installations with adequate training facilities, or at facilities operated by the participants.

§ 10515. Interagency Threat Assessment and Coordination Group

(a) IN GENERAL.—To improve the sharing of information within the scope of the information sharing environment established under section 11908 of this title with State, local, tribal, and private-sector officials, the Director of National Intelligence, through the program manager for the information sharing environment, in coordination with the Secretary, shall coordinate and oversee the creation of an Interagency Threat Assessment and Coordination Group (in this section referred to as ''ITACG'').

(b) COMPOSITION OF ITACG.—The ITACG shall consist of—

(1) an ITACG Advisory Council to set policy and develop processes for the integration, analysis, and dissemination of federally coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information; and

(2) an ITACG Detail comprised of State, local, and tribal homeland security and law enforcement officers and intelligence analysts detailed to work in the National Counterterrorism Center with Federal intelligence analysts for the purpose of integrating, analyzing, and assisting in the dissemination of federally coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, through appropriate channels identified by the ITACG Advisory Council.

(c) RESPONSIBILITIES OF SECRETARY.—The Secretary, or the Secretary's designee, in coordination with the Director of the National Counterterrorism Center and the ITACG Advisory Council, shall—

(1) create policies and standards for the creation of information products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that are suitable for dissemination to State, local, and tribal governments and the private sector;

(2) evaluate and develop processes for the timely dissemination of federally coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to State, local, and tribal governments and the private sector;

(3) establish criteria and a methodology for indicating to State, local, and tribal governments and the private sector the reliability of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, disseminated to them;

(4) educate the intelligence community about the requirements of State, local, and tribal homeland security, law enforcement, and other emergency response providers regarding information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(5) establish and maintain the ITACG Detail, which shall assign an appropriate number of State, local, and tribal homeland security and

law enforcement officers and intelligence analysts to work in the National Counterterrorism Center who shall—

(A) educate and advise National Counterterrorism Center intelligence analysts about the requirements of the State, local, and tribal homeland security and law enforcement officers, and other emergency response providers regarding information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(B) assist National Counterterrorism Center intelligence analysts in integrating, analyzing, and otherwise preparing versions of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information that are unclassified or classified at the lowest possible level and suitable for dissemination to State, local, and tribal homeland security and law enforcement agencies in order to help deter and prevent terrorist attacks;

(C) implement, in coordination with National Counterterrorism Center intelligence analysts, the policies, processes, procedures, standards, and guidelines developed by the ITACG Advisory Council;

(D) assist in the dissemination of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to State, local, and tribal jurisdictions only through appropriate channels identified by the ITACG Advisory Council;

(E) make recommendations, as appropriate, to the Secretary or the Secretary's designee, for the further dissemination of intelligence products that could likely inform or improve the security of a State, local, or tribal government (including a State, local, or tribal law enforcement agency), or a private-sector entity; and

(F) report directly to the senior intelligence official from the Department under paragraph (6);

(6) detail a senior intelligence official from the Department to the National Counterterrorism Center, who shall—

(A) manage the day-to-day operations of the ITACG Detail;

(B) report directly to the Director of the National Counterterrorism Center or the Director's designee; and

(C) in coordination with the Director of the Federal Bureau of Investigation, and subject to the approval of the Director of the National Counterterrorism Center, select a deputy from the pool of available detailees from the Federal Bureau of Investigation in the National Counterterrorism Center;

(7) establish, in the ITACG Advisory Council, a mechanism to select law enforcement officers and intelligence analysts for placement in the National Counterterrorism Center consistent with paragraph (5), using criteria developed by the ITACG Advisory Council that shall encourage participation from a broadly representative group of State, local, and tribal homeland security and law enforcement agencies; and

(8) compile an annual assessment of the ITACG Detail's performance, including summaries of customer feedback, in preparing, disseminating, and requesting the dissemination of intelligence products intended for State, local and tribal government (including State, local, and tribal law enforcement agencies), and private-sector entities.

(d) MEMBERSHIP.—The Secretary, or the Secretary's designee, shall serve as the chair of the ITACG Advisory Council, which shall include—

(1) representatives of—

(A) the Department;

(B) the Federal Bureau of Investigation;

(C) the National Counterterrorism Center;

(D) the Department of Defense;

(E) the Department of Energy;

(F) the Department of State; and

(G) other Federal entities as appropriate;

(2) the program manager of the information sharing environment, designated under section 11908(d) of this title, or the program manager's designee; and

(3) executive level law enforcement and intelligence officials from State, local, and tribal governments.

(e) CRITERIA.—The Secretary, in consultation with the Director of National Intelligence, the Attorney General, and the program manager of the information sharing environment established under section 11908 of this title, shall—

(1) establish procedures for selecting members of the ITACG Advisory Council and for the proper handling and safeguarding of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by those members; and

(2) ensure that at least 50 percent of the members of the ITACG Advisory Council are from State, local, and tribal governments.

(f) OPERATIONS.—

(1) IN GENERAL.—The ITACG Advisory Council shall meet regularly, but not less than quarterly, at the facilities of the National Counterterrorism Center of the Office of the Director of National Intelligence.

(2) MANAGEMENT.—Pursuant to section 119(f)(1)(E) of the National Security Act of 1947 (50 U.S.C. 3056(f)(1)(E)), the Director of the National Counterterrorism Center, acting through the senior intelligence official from the Department of Homeland Security detailed pursuant to subsection (c)(6), shall ensure that—

(A) the products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, prepared by the National Counterterrorism Center and the ITACG Detail for distribution to State, local, and tribal homeland security and law enforcement agencies, reflect the requirements of the agencies and are produced consistently with the policies, processes, procedures, standards, and guidelines established by the ITACG Advisory Council;

(B) in consultation with the ITACG Advisory Council and consistent with sections 102A(f)(1)(B)(iii) and 119(f)(1)(E) of the National Security Act of 1947 (50 U.S.C. 3024(f)(1)(B)(iii), 3056(f)(1)(E)), all products described in subparagraph (A) are disseminated through existing channels of the Department and the Department of Justice and other appropriate channels to State, local, and tribal government officials and other entities;

(C) all detailees under subsection (c)(5) have appropriate access to all relevant information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, available at the National Counterterrorism Center in order to accomplish the objectives under subsection (c)(5);

(D) all detailees under subsection (c)(5) have the appropriate security clearances and are trained in the procedures for handling, processing, storing, and disseminating classified products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information; and

(E) all detailees under subsection (c)(5) complete appropriate privacy and civil liberties training.

(g) INAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of title 5 shall not apply to the ITACG or any subsidiary groups of the ITACG.

§ 10516. Classified Information Advisory Officer

(a) DESIGNATION.—The Secretary shall identify and designate in the Department a Classified Information Advisory Officer.

(b) RESPONSIBILITIES.—The responsibilities of the Classified Information Advisory Officer are as follows:

(1) To develop and disseminate educational materials and to develop and administer training programs to assist State, local, and tribal governments (including State, local, and tribal law enforcement agencies), and private-sector entities—

(A) in developing plans and policies to respond to requests related to classified information without communicating the information to individuals who lack appropriate security clearances;

(B) regarding the appropriate procedures for challenging classification designations of information received by personnel of the entities; and

(C) on the means by which the personnel may apply for security clearances.

(2) To inform the Under Secretary for Intelligence and Analysis on policies and procedures that could facilitate the sharing of classified information with the personnel, as appropriate.

§ 10517. Annual report and briefing on intelligence activities of the Department

(a) IN GENERAL.—For each fiscal year and along with the budget materials submitted in support of the budget of the Department pursuant to section 1105(a) of title 31, the Under Secretary for Intelligence and Analysis shall submit to the congressional intelligence committees a report for that fiscal year on each intelligence activity of each intelligence component of the Department, as designated by the Under Secretary, that includes the following:

(1) The amount of funding requested for each intelligence activity.

(2) The number of full-time employees funded to perform each intelligence activity.

(3) The number of full-time contractor employees (or the equivalent of full-time in the case of part-time contractor employees) funded to perform, or in support of, each intelligence activity.

(4) A determination as to whether each intelligence activity is predominantly in support of national intelligence or departmental mission.

(5) The total number of analysts of the Intelligence Enterprise of the Department who perform—

(A) strategic analysis; or

(B) operational analysis.

(b) BRIEFING ON DEPARTMENT INTELLIGENCE ACTIVITIES

(1) DEFINITIONS.—In this subsection:

(A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(i) the congressional intelligence committees;

(ii) the Committee on Homeland Security and Government Affairs and the Committee on Appropriations of the Senate; and

(iii) the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

(B) COMPONENT OF THE DEPARTMENT.—The term ''component of the department'' means the following components of the Department:

(i) The Cybersecurity and Infrastructure Security Agency Threat Management Division.

(ii) The Federal Emergency Management Agency Protection and National Preparedness Office of Counterterrorism and Security Preparedness.

(iii) The Transportation Security Administration Office of Intelligence and Analysis.

(iv) The United States Citizenship and Immigration Services Fraud Detection and National Security Directorate, Field Operations Directorate, and Collateral Duty Intellience.

(v) The United States Customs and Border Protection Office of Intelligence.

(vi) The United States Immigration and Customs Enforcement Homeland Security Investigations, Office of Intelligence, and Special Agent in Charge Intelligence Program.

(C) INTELLIGENCE ACTIVITY.—The term ''intelligence activity'' shall be interpreted consistent with how the term is used in section 502 of the National Security Act of 1947 (50 U.S.C. 3092).

(2) BRIEFING.—

(A) WHEN PROVIDED.—Not less frequently than once each year thereafter, the Chief Intelligence Officer of the Department shall provide the appropriate congressional committees a briefing on new intelligence activities commenced by any component of the Department and any that have been terminated.

(B) CONTENTS.—Each briefing shall include the following:

(i) A comprehensive description of all intelligence activities conducted during the period by any component of the Department that conducts intelligence activities.

(ii) With respect to each intelligence activity, a description of the activity, including at a minimum—

(I) the nature of the activity;

(II) the component undertaking the activity;

(III) the legal authority for the activity; and

(IV) the source of funding for the activity.

(iii) A description and the quantity of any types of finished intelligence products or intelligence information reports produced or contributed to by a component of the Department that conducts intelligence activities during the period specified in the briefing.

(iv) An identification of any external or internal guidelines, policies, processes, practices, or programs governing the collection, retention, analysis, or dissemination by the component of information regarding United States citizens, lawful permanent residents of the United States, or individuals located in the United States.

(C) FORM.—The briefing may be provided in classified form.

§ 10518. Data framework

(a) DEFINITIONS.—In this section:

(1) HOMELAND SECURITY INFORMATION.—The term ''homeland security information'' has the meaning given the term in section 11907 of this title.

(2) NATIONAL INTELLIGENCE.—The term ''national intelligence'' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(3) TERRORISM INFORMATION.—The term ''terrorism information'' has the meaning given the term in section 11908 of this title.

(b) DEVELOPMENT.—

(1) IN GENERAL.—The Secretary shall develop a data framework to integrate existing Department datasets and systems, as appropriate, for access by authorized personnel in a manner consistent with relevant legal authorities and privacy, civil rights, and civil liberties policies and protections.

(2) REQUIREMENTS.—In developing the framework, the Secretary shall ensure, in accordance with all applicable statutory and regulatory requirements, that the following information is included:

(A) All information acquired, held, or obtained by an office or component of the Department that falls within the scope of the information sharing environment, including homeland security information, terrorism information, weapons of mass destruction information, and national intelligence.

(B) Information or intelligence relevant to priority mission needs and capability requirements of the Homeland Security Enterprise, as determined appropriate by the Secretary.

(c) ACCESS.—

(1) IN GENERAL.—The Secretary shall ensure that the data framework required under this section is accessible to employees of the Department who the Secretary determines—

(A) have an appropriate security clearance;

(B) are assigned to perform a function that requires access to information in the framework; and

(C) are trained in applicable standards for safeguarding and using the information.

(2) GUIDANCE.—The Secretary shall—

(A) issue guidance for Department employees authorized to access and contribute to the data framework pursuant to paragraph (1); and

(B) ensure that the guidance enforces a duty to share between offices and components of the Department when accessing or contributing to the framework for mission needs.

(3) EFFICIENCY.—The Secretary shall promulgate data standards and instruct components of the Department to make available information through the data framework required under this section in a machine-readable standard format, to the greatest extent practicable.

(d) EXCLUSION OF INFORMATION.—The Secretary may exclude information from the data framework required under this section if the Secretary determines inclusion of the information may—

(1) jeopardize the protection of sources, methods, or activities;

(2) compromise a criminal or national security investigation;

(3) be inconsistent with other Federal laws or regulations; or

(4) be duplicative or not serve an operational purpose if included in the framework.

(e) SAFEGUARDS.—The Secretary shall incorporate into the data framework required under this section systems capabilities for auditing and ensuring the security of information included in the framework. The capabilities shall include the following:

(1) Mechanisms for identifying insider threats.

(2) Mechanisms for identifying security risks.

(3) Safeguards for privacy, civil rights, and civil liberties.

(f) DEADLINE FOR IMPLEMENTATION.—Not later than 2 years after December 19, 2018, the Secretary shall ensure the data framework required under this section has the ability to include appropriate information in existence in the Department to meet the critical mission operations of the Department.

(g) NOTICE TO CONGRESS.—

(1) STATUS UPDATES.—The Secretary shall submit to the appropriate congressional committees regular updates on the status of the data framework until the framework is fully operational.

(2) OPERATIONAL NOTIFICATION.—Not later than 60 days after the date on which the data framework required under this section is fully operational, the Secretary shall provide notice to the appropriate congressional committees that the data framework is fully operational.

(3) VALUE ADDED.—The Secretary shall annually brief Congress on component use of the data framework required under this section to support operations that disrupt terrorist activities and incidents in the homeland.

§ 10519. Procedures for sharing information

The Secretary shall establish procedures on the use of information shared under this chapter that—

(1) limit the re-dissemination of the information to ensure that it is not used for an unauthorized purpose;

(2) ensure the security and confidentiality of the information;

(3) protect the constitutional and statutory rights of individuals who are subjects of the information; and

(4) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

§ 10520. Privacy Officer

(a) APPOINTMENT AND RESPONSIBILITIES.—The Secretary shall appoint a senior official in the Department, who shall report directly to the Secretary, to assume primary responsibility for privacy policy, including—

(1) ensuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(2) ensuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in section 552a of title 5 (known as the Privacy Act of 1974);

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;

(5) coordinating with the Officer for Civil Rights and Civil Liberties to ensure that—

(A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and

(B) Congress receives appropriate reports on the programs, policies, and procedures; and

(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of section 552a of title 5 (known as the Privacy Act of 1974), internal controls, and other matters.

(b) AUTHORITY TO INVESTIGATE.—

(1) IN GENERAL.—The senior official appointed under subsection (a) may—

(A) have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to programs and operations with respect to the responsibilities of the senior official under this section;

(B) make investigations and reports relating to the administration of the programs and operations of the Department that are, in the senior official's judgment, necessary or desirable;

(C) subject to the approval of the Secretary, require by subpoena the production, by any person other than a Federal agency, of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary to the performance of the responsibilities of the senior official under this section; and

(D) administer to, or take from, a person an oath, affirmation, or affidavit, whenever necessary to the performance of the responsibilities of the senior official under this section.

(2) ENFORCEMENT OF SUBPOENAS.—A subpoena issued under paragraph (1)(C) shall, in the case of contumacy or refusal to obey, be enforceable by order of an appropriate United States district court.

(3) EFFECT OF OATHS.—An oath, affirmation, or affidavit administered or taken under paragraph (1)(D) by or before an employee of the

Privacy Office designated for that purpose by the senior official appointed under subsection (a) shall have the same force and effect as if administered or taken by or before an officer having a seal of office.

(c) SUPERVISION AND COORDINATION.—

(1) IN GENERAL.—The senior official appointed under subsection (a) shall—

(A) report to, and be under the general supervision of, the Secretary; and

(B) coordinate activities with the Inspector General of the Department in order to avoid duplication of effort.

(2) COORDINATION WITH INSPECTOR GENERAL.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the senior official appointed under subsection (a) may investigate a matter relating to possible violations or abuse concerning the administration of a program or operation of the Department relevant to the purposes under this section.

(B) COORDINATION.—

(i) REFERRAL TO INSPECTOR GENERAL.—Before initiating an investigation described under subparagraph (A), the senior official shall refer the matter and all related complaints, allegations, and information to the Inspector General of the Department.

(ii) DETERMINATION.—Not later than 30 days after the receipt of a matter referred under clause (i), the Inspector General shall—

(I) make a determination regarding whether the Inspector General intends to initiate an audit or investigation of the matter referred under clause (i); and

(II) notify the senior official of that determination.

(iii) NOTIFICATION THAT AUDIT NOT INITIATED.—If the Inspector General notifies the senior official that the Inspector General intends to initiate an audit or investigation, but does not initiate that audit or investigation within 90 days after providing that notification, the Inspector General shall further notify the senior official that an audit or investigation was not initiated. The further notification under this clause shall be made not later than 3 days after the end of that 90-day period.

(iv) INVESTIGATION BY SENIOR OFFICIAL.—The senior official may investigate a matter referred under clause (i) if—

(I) the Inspector General notifies the senior official under clause (ii) that the Inspector General does not intend to initiate an audit or investigation relating to that matter; or

(II) the Inspector General provides a further notification under clause (iii) relating to that matter.

(v) TRAINING.—An employee of the Office of Inspector General who audits or investigates a matter referred under clause (i) shall be required to receive adequate training on privacy laws, rules, and regulations, to be provided by an entity approved by the Inspector General in consultation with the senior official appointed under subsection (a).

(d) NOTIFICATION TO CONGRESS ON REMOVAL.—If the Secretary removes the senior official appointed under subsection (a) or transfers that senior official to another position or location within the Department, the Secretary shall—

(1) promptly submit a written notification of the removal or transfer to both Houses of Congress; and

(2) include in the notification the reasons for the removal or transfer.

(e) REPORTS BY SENIOR OFFICIAL TO CONGRESS.—The senior official appointed under subsection (a) shall—

(1) submit reports directly to Congress regarding performance of the responsibilities of the senior official under this section, without prior comment or amendment by the Secretary, Deputy Secretary of Homeland Security, or any other officer or employee of the Department or the Office of Management and Budget; and

(2) inform the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives not later than—

(A) 30 days after the Secretary disapproves the senior official's request for a subpoena under subsection (b)(1)(C) or the Secretary substantively modifies the requested subpoena; or

(B) 45 days after the senior official's request for a subpoena under subsection (b)(1)(C), if that subpoena has neither been approved nor disapproved by the Secretary.

Chapter 107—Cybersecurity and Infrastructure Security

Subchapter I—General

Subchapter I—General

§ 10701. Definitions

In this subchapter, subchapters II and III, and sections 10761 through 10767 of this title:

(1) AGENCY.—The term ''Agency'' means the Cybersecurity and Infrastructure Security Agency.

(2) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term ''appropriate congressional committee'' means—

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

(B) the Committee on Homeland Security of the House of Representatives.

(3) CLOUD SERVICE PROVIDER.—The term ''cloud service provider'' means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating to that publication.

(4) CRITICAL INFRASTRUCTURE INFORMATION.—The term ''critical infrastructure information'' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of critical infrastructure or a protected system to resist interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk management planning, or risk audit; and

(C) a planned or past operational problem or solution regarding critical infrastructure or a protected system, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to interference, compromise, or incapacitation.

(5) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communication that appear to be transmitted for the purpose of gathering technical information relating to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of the attribute is not otherwise prohibited by law; or

(H) any combination of subparagraphs (A) through (G).

(6) 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.

(7) CYBERSECURITY RISK.—The term ''cybersecurity risk''—

(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of the information or information systems, including related consequences caused by an act of terrorism; and

(B) does not include an action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(8) 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.

(9) DEFENSIVE MEASURE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''defensive measure'' means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) EXCLUSION.—The term ''defensive measure'' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting the information system not owned by—

(i) the private entity (as defined in section 1501 of this title) operating the measure; or

(ii) another entity or Federal entity that may provide consent and has provided consent to that private entity for operation of the measure.

(10) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(11) HOMELAND SECURITY ENTERPRISE.—In this section, the term ''Homeland Security Enterprise'' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private-sector representatives, academics, and other policy experts.

(12) INCIDENT.—The term ''incident'' means an occurrence that actually or imminently jeopardizes, without lawful authority —

(A) the integrity, confidentiality, or availability of information on an information system; or

(B) an information system.

(13) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ''Information Sharing and Analysis Organization'' means a formal or informal entity or collaboration created or employed by public- or private-sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information, including information relating to cybersecurity risks and incidents, to better understand security problems and interdependencies relating to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability of the infrastructure and systems;

(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem relating to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, the Federal Government, State and local governments, or other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(14) INFORMATION SYSTEM.—The term ''information system''—

(A) has the meaning given the term in section 3502 of title 44; and

(B) includes industrial control systems such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(15) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(16) MALICIOUS CYBER COMMAND AND CONTROL.—The term ''malicious cyber command and control'' means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(17) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if the method is associated with a known or suspected cybersecurity threat.

(18) MANAGED SERVICE PROVIDER.—The term ''managed service provider'' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

(19) MONITOR.—The term ''monitor'' means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

(20) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term ''national cybersecurity asset response activities'' means—

(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities referred to in subparagraph (A);

(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate the risks;

(D) facilitating information sharing and operational coordination with threat response; and

(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

(21) NATIONAL SECURITY SYSTEM.—The term ''national security system'' had the meaning given the term in section 11103 of title 40.

(22) RANSOMEWARE ATTACK.—The term ''ransomware attack''—

(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial

of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

(B) does not include an event in which the demand for payment is—

(i) not genuine; or

(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.

(23) SECTOR RISK MANAGEMENT AGENCY.—The term ''Sector Risk Management Agency'' means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all-hazards environment in coordination with the Department.

(24) SECURITY CONTROL.—The term ''security control'' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(25) SECURITY VULNERABILITY.–The term ''security vulnerability'' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(26) SHARING.—The term ''sharing'' means providing, receiving, and disseminating.

(27) SLTT ENTITY.—The term ''SLTT entity'' means a domestic government entity that is a State government, local government, Tribal government, territorial government, or any subdivision of any of those governments.

(28) SUPPLY CHAIN COMPROMISE.—The term ''supply chain compromise'' means an incident in the supply chain of an information system that an adversary can leverage or does leverage to compromise the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits and can occur at any point during the life cycle.

§ 10702. Responsibilities

(a) DIRECTOR.—

(1) IN GENERAL.—The Director shall—

(A) lead cybersecurity and critical infrastructure security programs, operations, and associated policy for the Agency, including national cybersecurity asset response activities;

(B) coordinate with Federal entities, including Sector Risk Management Agencies, and non-Federal entities, including international entities, to carry out the cybersecurity and critical infrastructure activities of the Agency, as appropriate;

(C) carry out the responsibilities of the Secretary to secure Federal information and information systems consistent with law, including subchapter II of chapter 35 of title 44 and subchapter IV of this chapter,including by carrying out a periodic strategic assessment of the related programs and activities of the Agency to ensure the programs and activities contemplate the innovation of information systems and changes in cybersecurity risks and cybersecurity threats;

(D) coordinate a national effort to secure and protect against critical infrastructure risks, consistent with subsection (b)(1)(E);

(E) on request, provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and, where appropriate, provide those analyses, expertise, and other technical assistance in coordination with Sector Risk Management Agencies and other Federal departments and agencies;

(F) develop and utilize mechanisms for active and frequent collaboration between the Agency and Sector Risk Management Agencies to ensure appropriate coordination, situational awareness, and communications with Sector Risk Management Agencies;

(G) maintain and utilize mechanisms for the regular and ongoing consultation and collaboration among the divisions of the Agency to further operational coordination, integrated situational awareness, and improved integration across the Agency in accordance with this title;

(H) develop, coordinate, and implement—

(i) comprehensive strategic plans for the activities of the Agency; and

(ii) risk assessments by and for the Agency;

(I) carry out emergency communications responsibilities, in accordance with chapter 123 of this title;

(J) carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate that outreach and engagement with critical infrastructure Sector Risk Management Agencies, as appropriate;

(K) provide education, training, and capacity development to Federal and non-Federal entities to enhance the security and resiliency of domestic and global cybersecurity and infrastructure security;

(L) appoint a Cybersecurity State Coordinator in each State, as described in section 10883 of this title;

(M) carry out the duties and authorities relating to the .gov internet domain, as described in section 10881 of this title; and

(N) carry out other duties and powers prescribed by law or delegated by the Secretary.

(2) CENTRAL LOCATIONS AND CO-LOCATION.—

(A) CENTRAL LOCATIONS.—To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence.

(B) CO-LOCATION.—When establishing the central locations described in subparagraph (A), the Director shall coordinate with component heads and the Under Secretary for Management to co-locate or partner on new real property leases, renew occupancy agreements for existing leases, or agree to extend or newly occupy Federal space or new construction.

(b) SECRETARY.—

(1) IN GENERAL.—The responsibilities of the Secretary relating to cybersecurity and infrastructure security shall include the following:

(A) Accessing, receiving, and analyzing law enforcement information, intelligence information, and other information from Federal Government agencies, State, local, tribal, and territorial government agencies, including law enforcement agencies, and private-sector entities, and integrating that information, in support of the mission responsibilities of the Department, to—

(i) identify and assess the nature and scope of terrorist threats to the homeland;

(ii) detect and identify threats of terrorism against the United States; and

(iii) understand those threats in light of actual and potential vulnerabilities of the homeland.

(B) Carrying out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks in the United States, including an assessment of the probability of success of those attacks and the feasibility and potential

efficacy of various countermeasures to those attacks. At the discretion of the Secretary, the assessments may be carried out in coordination with Sector Risk Management Agencies.

(C) Integrating relevant information, analysis, and vulnerability assessments, regardless of whether the information, analysis, or assessments are provided or produced by the Department, in order to make recommendations, including prioritization, for protective and support measures by the Department, other Federal Government agencies, State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities regarding terrorist and other threats to homeland security.

(D) Ensuring, pursuant to section 10502 of this title, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this chapter, including obtaining that information from other Federal Government agencies.

(E) Developing, in coordination with the Sector Risk Management Agencies with available expertise, a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency communications systems, and the physical and technological assets that support such systems.

(F) Recommending measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government agencies, including Sector Risk Management Agencies, and in cooperation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities.

(G) Reviewing, analyzing, and making recommendations for improvements to the policies and procedures governing the sharing of information relating to homeland security in the Federal Government and between Federal Government agencies and State, local, tribal, and territorial government agencies and authorities.

(H) Disseminating, as appropriate, information analyzed by the Department in the Department to other Federal Government agencies with responsibilities relating to homeland security, and to State, local, tribal, and territorial government agencies and private-sector entities with those responsibilities, to assist in the de-

terrence, prevention, or preemption of, or response to, terrorist attacks against the United States.

(I) Consulting with State, local, tribal, and territorial government agencies and private-sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(J) Ensuring that material received pursuant to this subtitle (except subchapters III through V of this chapter) is protected from unauthorized disclosure and handled and used only for the performance of official duties.

(K) Requesting additional information from other Federal Government agencies, State, local, tribal, and territorial government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain the information.

(L) Establishing and utilizing, in conjunction with the Chief Information Officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(M) Coordinating training and other support to the elements and personnel of the Department, other Federal Government agencies, and State, local, tribal, and territorial government agencies that provide information to the Department, or are consumers of information provided by the Department, to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

(N) Coordinating with Federal, State, local, tribal, and territorial law enforcement agencies, and the private sector, as appropriate.

(O) Exercising the authorities and oversight of the functions, personnel, assets, and liabilities of those components transferred to the Department pursuant to section 10501(e) of this title.

(P) Carrying out the functions of the National Cybersecurity and Communications Integration Center under section 10706 of this title.

(Q) Carrying out the requirements of the Chemical Facility Anti-Terrorism Standards Program established under subchapter VII of this chapter and the secure handling of ammonium nitrate program established under subchapter VI of this chapter, or any successor programs.

(R) Encouraging and building cybersecurity awareness and competency across the United States and developing, attracting, and retaining the cybersecurity workforce necessary for the cybersecurity related missions of the Department, including by—

(i) overseeing elementary and secondary cybersecurity education and awareness related programs at the Agency;

(ii) leading efforts to develop, attract, and retain the cybersecurity workforce necessary for the cybersecurity related missions of the Department;

(iii) encouraging and building cybersecurity awareness and competency across the United States; and

(iv) carrying out cybersecurity related workforce development activities, including through—

(I) increasing the pipeline of future cybersecurity professionals through programs focused on elementary and secondary education, postsecondary education, and workforce development; and

(II) building awareness of and competency in cybersecurity across the civilian Federal Government workforce.

(2) REALLOCATION.—The Secretary may reallocate within the Agency the functions specified in subsections (d) and (e), consistent with the responsibilities provided in paragraph (1), on certifying to and briefing the appropriate congressional committees, and making known to the public, at least 60 days prior to the reallocation, that the reallocation is necessary for carrying out the activities of the Agency.

(3) STAFF.—

(A) IN GENERAL.—The Secretary shall provide the Agency with a staff of analysts having appropriate expertise and experience to assist the Agency in discharging the responsibilities of the Agency under this section.

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

(C) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(4) DETAIL OF PERSONNEL.—

(A) IN GENERAL.—To assist the Agency in discharging the responsibilities of the Agency under this section, personnel of the Federal agencies described in subparagraph (B) may be detailed to the Agency for the performance of analytic functions and related duties.

(B) AGENCIES.—The Federal agencies referred to in subparagraph (A) are—

(i) the Department of State;

(ii) the Central Intelligence Agency;

(iii) the Federal Bureau of Investigation;

(iv) the National Security Agency;

(v) the National Geospatial-Intelligence Agency;

(vi) the Defense Intelligence Agency;

(vii) Sector Risk Managmenet Agencies; and

(viii) any other agency of the Federal Government the President considers appropriate.

(C) INTERAGENCY AGREEMENTS.—The Secretary and the head of a Federal agency described in subparagraph (B) may enter into agreements for the purpose of detailing personnel under this paragraph.

(D) REIMBURSABLE OR NON-REIMBURSABLE BASIS.—The detail of personnel under this paragraph may be on a reimbursable or non-reimbursable basis.

(c) PRIVACY OFFICER.—The responsibilities of the Privacy Officer of the Agency include—

(1) ensuring that the use of technologies by the Agency sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(2) ensuring that personal information contained in systems of records of the Agency is handled in full compliance as specified in section 552 of title 5;

(3) evaluating legislation and regulatory proposals involving collection, use, and disclosure of personal information by the Agency; and

(4) conducting a privacy impact assessment of proposed rules of the Agency on the privacy of personal information, including the type of personal information collected and the number of people affected.

(d) EXECUTIVE ASSISTANT DIRECTOR FOR CYBERSECURITY.—The Executive Assistant Director for Cybersecurity shall—

(1) direct the cybersecurity efforts of the Agency;

(2) carry out activities, at the direction of the Director, relating to the security of Federal information and Federal information systems

consistent with law, including subchapter II of chapter 35 of title 44 and subchapter IV of this chapter;

(3) fully participate in the mechanisms required under subsection (a)(1)(G); and

(4) carry out such other duties and powers as prescribed by the Director.

(e) EXECUTIVE ASSISTANT DIRECTOR FOR INFRASTRUCTURE SECURITY.—The Executive Assistant Director for Infrastructure Security shall—

(1) direct the critical infrastructure security efforts of the Agency;

(2) carry out, at the direction of the Director, subchapters V and VI of this chapter;

(3) fully participate in the mechanisms required under subsection (a)(1)(G); and

(4) carry out such other duties and powers as prescribed by the Director.

§ 10703. Authority not affected

Nothing in this chapter may be construed as affecting in any manner the authority, existing on November 15, 2018, of another component of the Department or another Federal department or agency, including the authority provided to the Sector Risk Management Agency specified in section 61003(c) of division F of the Fixing America's Surface Transportation Act (Public Law 114–94, 129 Stat. 1778).

§ 10704. Enhancement of Federal and non-Federal cybersecurity

In carrying out the responsibilities under section 10702 of this title, the Director shall—

(1) as appropriate, provide to State and local government entities, and on request to private entities that own or operate critical information systems—

(A) analysis and warnings related to threats to, and vulnerabilities of, critical information systems; and

(B) crisis management support in response to threats to, or attacks on, critical information systems;

(2) as appropriate, provide technical assistance, on request, to the private sector and other government entities, with respect to emergency recovery plans to respond to major failures of critical information systems; and

(3) fulfill the responsibilities of the Secretary to protect Federal information systems under subchapter II of chapter 35 of title 44.

§ 10705. Recruitment and retention

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

(2) COLLECTIVE BARGAINING AGREEMENT.—The term ''collective bargaining agreement'' has the same meaning given that term in section 7103(a)(8) of title 5.

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

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

(5) QUALIFIED POSITION.—The term ''qualified position'' means a position, designated by the Secretary for the purpose of this section, in which the incumbent performs, manages, or supervises functions that execute the responsibilities of the Department relating to cybersecurity.

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

(b) GENERAL AUTHORITY OF SECRETARY.—

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

(A) IN GENERAL.—The Secretary may—

(i) establish, as positions in the excepted service, such qualified positions in the Department as the Secretary determines necessary to carry out the responsibilities of the Department relating to cybersecurity, including positions formerly identified as—

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

(II) positions in the Senior Executive Service;

(ii) appoint an individual to a qualified position (after taking into consideration the availability of preference eligibles for appointment to the position); and

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

(B) CONSTRUCTION WITH OTHER LAWS.—The authority of the Secretary under this subsection applies without regard to any

other law relating to the appointment, number, classification, or compensation of employees.

(2) BASIC PAY.—

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

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

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

(A) ADDITIONAL COMPENSATION BASED ON TITLE 5 AUTHORIZATION.—The Secretary may provide employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by title 5.

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

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

(5) COLLECTIVE BARGAINING AGREEMENTS.—Nothing in paragraph (1) may be construed to impair the continued effectiveness of a collective bargaining agreement with respect to an office, component, subcomponent, or equivalent of the Department that is a successor to an office, component, subcomponent, or equivalent of the Department covered by the agreement before the succession.

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

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

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

(2) describes—

(A) how the Secretary plans to fulfill the critical need of the Department to recruit and retain employees in qualified positions;

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

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

(3) discusses how the planning and actions taken under paragraph (2) are integrated into the strategic workforce planning of the Department;

(4) provides metrics on actions occurring during the reporting period, including—

(A) the number of employees in qualified positions hired by occupation and grade and level or pay band;

(B) the placement of employees in qualified positions by directorate and office in the Department;

(C) the total number of veterans hired;

(D) the number of separations of employees in qualified positions by occupation and grade and level or pay band;

(E) the number of retirements of employees in qualified positions by occupation and grade and level or pay band; and

(F) the number and amounts of recruitment, relocation, and retention incentives paid to employees in qualified positions by occupation and grade and level or pay band; and

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

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

(e) INCUMBENTS OF EXISTING COMPETITIVE SERVICE POSITIONS.—

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

(2) SUBSEQUENT CONVERSION.—After the date on which an individual who refuses a conversion under paragraph (1) stops serving in the position selected to be converted, the position may be converted to a position in the excepted service.

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

(1) the Subcommittee on Homeland Security of the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

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

§ 10706. National Cybersecurity and Communications Integration Center

(a) DEFINITIONS OF CYBERSECURITY VULNERABILITY.—In this section, the term ''cybersecurity vulnerability'' has the meaning given the term ''security vulnerability'' in section 10701 of this title.

(b) FUNCTIONS.—The cybersecurity functions of the Center shall include—

(1) being a Federal civilian interface for the multi-directional and cross-sector sharing of information relating to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including the implementation of subchapter V of this chapter;

(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

(3) coordinating the sharing of information relating to cyber threat indicators, defensive measures, cybersecurity risks, and incidents across the Federal Government;

(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related to or could have consequential impacts across multiple sectors;

(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cyber threat indicators, defensive measures, cybersecurity risks, and incidents;

(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (m), as appropriate; and

(C) sharing the analysis conducted under subparagraph (A) and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B), as appropriate, with Federal and non-Federal entities;

(6) on request, providing operational and timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may include attribution, mitigation, and remediation,which may take the form of continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions;

(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

(A) facilitate information security;

(B) strengthen information systems against cybersecurity risks and incidents; and

(C) share cyber threat indicators and defensive measures;

(8) engaging with international partners, in consultation with other appropriate agencies, to—

(A) collaborate on cyber threat indicators, defensive measures, and information relating to cybersecurity risks and incidents; and

(B) enhance the security and resilience of global cybersecurity;

(9) sharing cyber threat indicators, defensive measures, mitigation protocols to counter cybersecurity vulnerabilities, as appropriate, and other information relating to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure, and with State and major urban area fusion centers, as appropriate;

(10) participating, as appropriate, in national exercises run by the Department;

(11) in coordination with the Emergency Communications Division, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of the communications;

(12) detecting, identifying, and receiving information for a cybersecurity purpose about security vulnerabilities relating to critical infrastructure in information systems and devices; and

(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined insection 10761 of this title) submitted by covered entities (as defined insection 10761 of this title) and reports related to ransom payments (as defined insection 10761 of this title) submitted by covered entities (as defined insection 10761 of this title) in furtherance of the activities specified insections subsections (b) and (d) of section 10702 and 10762 of this title, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.

(c) COMPOSITION.—

(1) IN GENERAL.—The Center is composed of—

(A) appropriate representatives of Federal entities, such as—

(i) Sector Risk Management Agencies;

(ii) civilian and law enforcement agencies; and

(iii) elements of the intelligence community;

(B) appropriate representatives of non-Federal entities, such as—

(i) State, local, and tribal governments;

(ii) Information Sharing and Analysis Organizations, including information sharing and analysis centers;

(iii) owners and operators of critical information systems; and

(iv) private entities, including cybersecurity specialists;

(C) components in the Center that carry out cybersecurity and communications activities;

(D) a designated Federal official for operational coordination with and across each sector;

(E) an entity that collaborates with State and local governments, including an entity that collaborates with election officials, on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center; and

(F) other appropriate representatives or entities, as determined by the Secretary.

(2) INCIDENTS.—In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.

(d) PRINCIPLES.—In carrying out the functions under subsection (b), the Center shall ensure—

(1) to the extent practicable, that—

(A) timely, actionable, and relevant cyber threat indicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is shared;

(B) when appropriate, cyber threat indicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;

(C) activities are prioritized and conducted based on the level of risk;

(D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;

(E) continuous, collaborative, and inclusive coordination occurs—

(i) across sectors; and

(ii) with—

(I) sector coordinating councils;

(II) Information Sharing and Analysis Organizations; and

(III) other appropriate non-Federal partners;

(F) as appropriate, the Center works to develop and use mechanisms for sharing information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient;

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents;

(H) the Center designates an agency contact for non-Federal entities; and

(I) activities of the Center address the security of both information technology and operational technology, including industrial control systems;

(2) that information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents is appropriately safeguarded against unauthorized access or disclosure; and

(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons, including by working with the Privacy Officer appointed under section 10520 of this title to ensure that the Center

follows the policies and procedures specified in subsections (c) and (e)(5)(C) of section 10784 of this title.

(e) CYBER HUNT AND INCIDENT RESPONSE TEAMS.—

(1) IN GENERAL.—The Center shall maintain cyber hunt and incident response teams for the purpose of leading Federal asset response activities and providing timely technical assistance to Federal and non-Federal entities, including across all critical infrastructure sectors, regarding actual or potential security incidents, as appropriate and on request, including—

(A) assistance to asset owners and operators in restoring services following a cyber incident;

(B) identification and analysis of cybersecurity risk and unauthorized cyber activity;

(C) mitigation strategies to prevent, deter, and protect against cybersecurity risks;

(D) recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as appropriate; and

(E) such other capabilities as the Secretary determines appropriate.

(2) ASSOCIATED METRICS.—The Center shall—

(A) define the goals and desired outcomes for each cyber hunt and incident response team; and

(B) develop metrics—

(i) to measure the effectiveness and efficiency of each cyber hunt and incident response team in achieving the goals and desired outcomes defined under subparagraph (A); and

(ii) that—

(I) are quantifiable and actionable; and

(II) the Center shall use to improve the effectiveness and accountability of, and service delivery by, cyber hunt and incident response teams.

(3) CYBERSECURITY SPECIALISTS.—After notice to, and with the approval of, the entity requesting action by or technical assistance from the Center, the Secretary may include cybersecurity specialists from the private sector on a cyber hunt and incident response team.

(f) NO RIGHT OR BENEFIT.—

(1) IN GENERAL.—The provision of assistance or information to, and inclusion in the Center, or any team or activity of the Center, of, governmental or private entities under this section shall be at the sole and

unreviewable discretion of the Director of the Cybersecurity and Infrastructure Security Agency.

(2) CERTAIN ASSISTANCE OR INFORMATION.—Providing a governmental or private entity certain assistance or information or including the entity in the Center or a team or activity of the Center, pursuant to this section, shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

(g) AUTOMATED INFORMATION SHARING.—

(1) IN GENERAL.—The Director, in coordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the sharing of cyber threat indicators and defensive measures in accordance with subchapter V of this chapter.

(2) ANNUAL REPORT.—The Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives an annual report on the status and progress of the development of the capabilities described in paragraph (1). The reports shall be required until the capabilities are fully implemented.

(h) VOLUNTARY INFORMATION SHARING PROCEDURES AND RELATIONSHIPS.—

(1) PROCEDURES.—

(A) IN GENERAL.—The Center may enter into a voluntary information sharing relationship with any consenting non-Federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes in accordance with this section. Nothing in this subsection may be construed to require any non-Federal entity to enter into an information sharing relationship with the Center or any other entity. The Center may terminate a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Director, for any reason, including if the Center determines that the non-Federal entity with which the Center has entered into the relationship has violated the terms of this subsection.

(B) NATIONAL SECURITY.—The Secretary may decline to enter into a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary,

acting through the Director, for any reason, including if the Secretary determines that declining to enter into the relationship is appropriate for national security.

(2) RELATIONSHIPS.—A voluntary information sharing relationship under this subsection may be characterized as an agreement described as follows:

(A) For the use of a non-Federal entity, the Center shall make available a standard agreement, consistent with this section, on the Department's website.

(B) At the request of a non-Federal entity, and if determined appropriate by the Center, at the sole and unreviewable discretion of the Secretary, acting through the Director, the Department shall negotiate a non-standard agreement, consistent with this section.

(C) An agreement between the Center and a non-Federal entity that was entered into, or that was in effect, before December 18, 2015, shall be deemed in compliance with the requirements of this subsection. An agreement under this subsection shall include the relevant privacy protections as in effect under the Cooperative Research and Development Agreement for Cybersecurity Information Sharing and Collaboration, as of December 31, 2014. Nothing in this subsection may be construed to require a non-Federal entity to enter into either a standard or negotiated agreement to be in compliance with this subsection.

(i) DIRECT REPORTING.—The Secretary shall develop policies and procedures for direct reporting to the Secretary by the Director of the Center regarding significant cybersecurity risks and incidents.

(j) REPORTS ON INTERNATIONAL COOPERATION.—The Secretary periodically shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners in accordance with subsection (b)(8).

(k) OUTREACH.—The Secretary, acting through the Director, shall—

(1) disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the Center; and

(2) enhance outreach to critical infrastructure owners and operators for purposes of sharing cyber threat indicators and defensive measures with the Center.

(l) CYBERSECURITY OUTREACH.—

(1) DEFINITIONS.—For purposes of this subsection, the terms ''small business concern'' and ''small business development center'' have the meanings given the terms in section 3 of the Small Business Act (15 U.S.C. 632).

(2) PROVIDE ASSISTANCE.—The Secretary may leverage small business development centers to provide assistance to small business concerns by disseminating information on cyber threat indicators, defense measures, cybersecurity risks, incidents, analyses, and warnings to help small business concerns in developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees.

(m) COORDINATED VULNERABILITY DISCLOSURE.—The Secretary, in coordination with industry and other stakeholders, may develop and adhere to Department policies and procedures for coordinating vulnerability disclosures.

(n) PROTOCOLS TO COUNTER CERTAIN CYBERSECURITY VULNERABILITIES.—The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, including in circumstances in which the vulnerabilities exist because software or hardware is no longer supported by a vendor.

(o) SUBPOENA AUTHORITY.—

(1) DEFINITION OF COVERED DEVICE OR SYSTEM.—In this subsection, the term ''covered device or system''—

(A) means a device or system commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers; but

(B) does not include personal devices and systems, such as consumer mobile devices, home computers, residential wireless routers, or residential internet enabled consumer devices.

(2) AUTHORITY.—

(A) IN GENERAL.—If the Director identifies a system connected to the internet with a specific security vulnerability and has reason to believe the security vulnerability relates to critical infrastructure and affects a covered device or system, and the Director is unable to identify the entity at risk that owns or operates the covered device or system, the Director may issue a subpoena for the production of information necessary to identify and notify the entity at risk, to carry out a function authorized under subsection (b)(12).

(B) LIMIT ON INFORMATION.—A subpoena issued pursuant to subparagraph (A) may seek information—

(i) only in the categories set forth in subparagraphs (A), (B), (D), and (E) of section 2703(c)(2) of title 18; and

(ii) for not more than 20 covered devices.

(C) LIABILITY PROTECTIONS FOR DISCLOSING PROVIDERS.—The provisions of section 2703(e) of title 18, shall apply to a subpoena issued pursuant to subparagraph (A).

(3) COORDINATION.—

(A) IN GENERAL.—If the Director exercises the subpoena authority under this subsection, and in the interest of avoiding interference with ongoing law enforcement investigations, the Director shall coordinate the issuance of a subpoena with the Department of Justice, including the Federal Bureau of Investigation, pursuant to interagency procedures that the Director, in coordination with the Attorney General, shall develop.

(B) CONTENTS.—The inter-agency procedures developed under this paragraph shall provide that a subpoena issued by the Director under this subsection shall be—

(i) issued to carry out a function described in subsection (b)(12); and

(ii) subject to the limitations described in this subsection.

(4) NONCOMPLIANCE.—If a person, partnership, corporation, association, or entity fails to comply with a duly served subpoena issued pursuant to this subsection, the Director may request that the Attorney General seek enforcement of the subpoena in any judicial district in which the person, partnership, corporation, association, or entity resides, is found, or transacts business.

(5) NOTICE.—Not later than 7 days after the date on which the Director receives information obtained through a subpoena issued pursuant to this subsection, the Director shall notify any entity identified by information obtained pursuant to the subpoena regarding the subpoena and the identified vulnerability.

(6) AUTHENTICATION.—

(A) IN GENERAL.—A subpoena issued pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that the subpoena was issued by the Agency and has not been altered or modified since the issuance.

(B) INVALIDATED IF NOT AUTHENTICATED.—A subpoena issued pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of the subpoena.

(7) PROCEDURES.—The Director shall establish internal procedures and associated training, applicable to employees and operations of the Agency, regarding subpoenas issued pursuant to this subsection, which shall address the following:

(A) The protection of and restriction on dissemination of nonpublic information obtained through the subpoena, including a requirement that the Agency not disseminate nonpublic information obtained through the subpoena that identifies the party that is subject to the subpoena or the entity at risk identified by information obtained, except that the Agency may share the nonpublic information with the Department of Justice for the purpose of enforcing the subpoena in accordance with paragraph (4), and may share with a Federal agency the nonpublic information of the entity at risk if—

(i) the Agency identifies or is notified of a cybersecurity incident involving the entity that relates to the vulnerability that led to the issuance of the subpoena;

(ii) the Director determines that sharing the nonpublic information with another Federal department or agency is necessary to allow the department or agency to take a law enforcement or national security action, consistent with the interagency procedures under paragraph (3)(A), or actions related to mitigating or otherwise resolving the incident;

(iii) the entity to which the information pertains is notified of the Director's determination, to the extent practicable consistent with national security or law enforcement interests, consistent with the interagency procedures; and

(iv) the entity consents, except that the entity's consent shall not be required if another Federal department or agency identifies the entity to the Agency in connection with a suspected cybersecurity incident.

(B) The restriction on the use of information obtained through the subpoena for a cybersecurity purpose.

(C) The retention and destruction of nonpublic information obtained through the subpoena, including—

(i) destruction of information that the Director determines is unrelated to critical infrastructure immediately on providing notice to the entity pursuant to paragraph (5); and

(ii) destruction of any personally identifiable information not later than 6 months after the date on which the Director receives information obtained through the subpoena, unless otherwise agreed to by the individual identified by the subpoena respondent.

(D) The processes for providing notice to each party that is subject to the subpoena and each entity identified by information obtained under the subpoena.

(E) The processes and criteria for conducting critical infrastructure security risk assessments to determine whether a subpoena is necessary prior to being issued pursuant to this subsection.

(F) The information to be provided to an entity at risk at the time of the notice of the vulnerability, which shall include—

(i) a discussion or statement that responding to, or subsequent engagement with, the Agency, is voluntary; and

(ii) to the extent practicable, information regarding the process through which the Director identifies security vulnerabilities.

(8) LIMITATION ON PROCEDURES.—The internal procedures established pursuant to paragraph (7) may not require an owner or operator of critical infrastructure to take any action as a result of a notice of vulnerability made pursuant to this chapter.

(9) REVIEW OF PROCEDURES.—Not later than 1 year after January 1, 2021, the Privacy Officer of the Agency shall—

(A) review the internal procedures established pursuant to paragraph (7) to ensure that—

(i) the procedures are consistent with fair information practices; and

(ii) the operations of the Agency comply with the procedures; and

(B) notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of the results of the review under subparagraph (A).

(10) PUBLICATION OF INFORMATION.—Not later than 120 days after establishing the internal procedures under paragraph (7), the Director shall publish information on the website of the Agency regarding

the subpoena process under this subsection, including information regarding the following:

(A) The internal procedures.

(B) The purpose for subpoenas issued pursuant to this subsection.

(C) The subpoena process.

(D) The criteria for the critical infrastructure security risk assessment conducted prior to issuing a subpoena.

(E) Policies and procedures on retention and sharing of data obtained by subpoenas.

(F) Guidelines on how entities contacted by the Director may respond to notice of a subpoena.

(11) ANNUAL REPORTS.—The Director shall annually submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report (which may include a classified annex but with the presumption of declassification) on the use of subpoenas issued pursuant to this subsection, which shall include the following:

(A) A discussion of the following:

(i) The effectiveness of the use of the subpoenas to mitigate critical infrastructure security vulnerabilities.

(ii) The critical infrastructure security risk assessment process conducted for subpoenas issued under this subsection.

(iii) The number of subpoenas issued during the preceding year.

(iv) To the extent practicable, the number of vulnerable covered devices or systems mitigated under this subsection by the Agency during the preceding year.

(v) The number of entities notified by the Director under this subsection, and their responses, during the preceding year.

(B) For each subpoena issued under this subsection, the following:

(i) Information relating to the source of the security vulnerability detected, identified, or received by the Director.

(ii) Information relating to the steps taken to identify the entity at risk prior to issuing the subpoena.

(iii) A description of the outcome of the subpoena, including discussion on the resolution or mitigation of the critical infrastructure security vulnerability.

(12) PUBLICATION OF ANNUAL REPORTS.—The Director shall publish a version of the annual report required under paragraph (11) on the website of the Agency, which shall, at a minimum, include the findings described in clauses (iii), (iv), and (v) of subparagraph (A) of paragraph (11).

(13) PROHIBITION ON USE OF INFORMATION FOR UNAUTHORIZED PURPOSES.—Any information obtained pursuant to a subpoena issued under this subsection may not be provided to another Federal department or agency for a purpose other than a cybersecurity purpose or for the purpose of enforcing a subpoena issued pursuant to this subsection.

(p) INDUSTRIAL CONTROL SYSTEMS.—The Director shall maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. In carrying out this subsection, the Director shall—

(1) lead Federal Government efforts, in consultation with Sector Risk Management Agencies, as appropriate, to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;

(2) maintain threat hunting and incident response capabilities to respond to industrial control system cybersecurity risks and incidents;

(3) provide cybersecurity technical assistance to industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control system stakeholders to identify, evaluate, assess, and mitigate vulnerabilities;

(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control systems stakeholders; and

(5) conduct such other efforts and assistance as the Secretary determines appropriate.

(q) COORDINATION ON CYBERSECURITY FOR SLTT ENTITIES.— The Center shall, on request and to the extent practicable, and in coordination as appropriate with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center—

(1) conduct exercises with SLTT entities;

(2) provide operational and technical cybersecurity training to SLTT entities to address cybersecurity risks or incidents, with or without reimbursement, related to—

(A) cyber threat indicators;

(B) defensive measures;

(C) cybersecurity risks;

(D) vulnerabilities; and

(E) incident response and management;

(3) to increase situational awareness and help prevent incidents, assist SLTT entities in sharing, in real time, with the Federal Government as well as among SLTT entities, actionable—

(A) cyber threat indicators;

(B) defensive measures;

(C) information about cybersecurity risks; and

(D) information about incidents;

(4) provide SLTT entities notifications containing specific incident and malware information that may affect them or their residents;

(5) provide to, and periodically update, SLTT entities via an easily accessible platform and other means—-

(A) information about tools;

(B) information about products;

(C) resources;

(D) policies;

(E) guidelines;

(F) controls; and

(G) other cybersecurity standards and best practices and procedures related to information security, including, as appropriate, information produced by other Federal agencies;

(6) work with senior SLTT entity officials, including chief information officers and senior election officials and through national associations, to coordinate the effective implementation by SLTT entities of tools, products, resources, policies, guidelines, controls, and procedures related to information security to secure the information systems, including election systems, of SLTT entities;

(7) provide operational and technical assistance to SLTT entities to implement tools, products, resources, policies, guidelines, controls, and procedures on information security;

(8) assist SLTT entities in developing policies and procedures for coordinating vulnerability disclosures consistent with international and national standards in the information technology industry; and

(9) promote cybersecurity education and awareness through engagements with Federal agencies and non-Federal entities.

(r) REPORTS.—Not later than 1 year after June 21, 2022, and every 2 years thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on

Homeland Security of the House of Representatives a report on the services and capabilities that the Agency directly and indirectly provides to SLTT entities.

§ 10707. Plans

(a) DEFINITION OF AGENCY INFORMATION SYSTEM.—In this section, the term ''agency information system'' means an information system used or operated by an agency or by another entity on behalf of an agency.

(b) INTRUSION ASSESSMENT PLAN.—

(1) REQUIREMENT.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall—

(A) develop and implement an intrusion assessment plan to proactively detect, identify, and remove intruders in agency information systems on a routine basis; and

(B) update the plan as necessary.

(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(c) CYBER INCIDENT RESPONSE PLANS.—The Director shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, Information Sharing and Analysis Organizations, owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, update not less often than biennially, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks to critical infrastructure. The Director, in consultation with relevant Sector Risk Management Agencies and the National Cyber Director, shall develop mechanisms to engage with stakeholders to educate the stakeholders regarding Federal Government cybersecurity roles and responsibilities for cyber incident response.

(d) NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (c), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

(e) HOMELAND SECURITY STRATEGY TO IMPROVE THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS

(1) IN GENERAL

(A) DEVELOPMENT AND AVAILABILITY.—Not later than December 27, 2022, the Secretary, acting through the Director, shall, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, and other stake-

holders, as appropriate, develop and make publicly available a Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments.

(B) RECOMMENDATIONS AND REQUIREMENTS.—The strategy required under subparagraph (A) shall provide recommendations relating to the ways in which the Federal Government should support and promote the ability of State, local, Tribal, and territorial governments to identify, mitigate against, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents.

(2) CONTENTS.—The strategy required under paragraph (1) shall—

(A) identify capability gaps in the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(B) identify Federal resources and capabilities that are available or could be made available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(C) identify and assess the limitations of Federal resources and capabilities available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents and make recommendations to address such limitations;

(D) identify opportunities to improve the coordination of the Agency with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center, to improve—

(i) incident exercises, information sharing and incident notification procedures;

(ii) the ability for State, local, Tribal, and territorial governments to voluntarily adapt and implement guidance in Federal binding operational directives; and

(iii) opportunities to leverage Federal schedules for cybersecurity investments undersection 502 of title 40;

(E) recommend new initiatives the Federal Government should undertake to improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(F) set short-term and long-term goals that will improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents; and

(G) set dates, including interim benchmarks, as appropriate for State, local, Tribal, and territorial governments to establish baseline capabilities to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents.

(3) CONSIDERATIONS.—In developing the strategy required under paragraph (1), the Director, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, and other stakeholders, as appropriate, shall consider—-

(A) lessons learned from incidents that have affected State, local, Tribal, and territorial governments, and exercises with Federal and non-Federal entities;

(B) the impact of incidents that have affected State, local, Tribal, and territorial governments, including the resulting costs to the governments;

(C) the information related to the interest and ability of state and non-state threat actors to compromise information systems owned or operated by State, local, Tribal, and territorial governments; and

(D) emerging cybersecurity risks and cybersecurity threats to State, local, Tribal, and territorial governments resulting from the deployment of new technologies.

(4) EXEMPTION.—Chapter 35 of title 44shall not apply to any action to implement this subsection.

(f) NATIONAL CYBER EXERCISE PROGRAM.—

(1) DEFINITIONS.—In this subsection:

(A) PRIVATE ENTITY.—The term ''private entity'' has the meaning given that term insection 10801 of this title.

(B) STATE.—The term ''State'' means a State, the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, the Northern Mariana Islands, and any other territory (including a possession) of the United States.

(2) IN GENERAL.—

(A) ESTABLISHMENT.—There is in the Agency the National Cyber Exercise Program (referred to in this subsection as the

"Exercise Program") to evaluate the National Cyber Incident Response Plan, and other related plans and strategies.

(B) REQUIREMENTS.—

(i) IN GENERAL.—The Exercise Program shall be—

(I) based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(II) designed, to the extent practicable, to simulate the partial or complete incapacitation of a government or critical infrastructure network resulting from a cyber incident;

(III) designed to provide for the systematic evaluation of cyber readiness and enhance operational understanding of the cyber incident response system and relevant information sharing agreements; and

(IV) designed to promptly develop after-action reports and plans that can quickly incorporate lessons learned into future operations.

(ii) MODEL EXERCISE SELECTION.—The Exercise Program shall—-

(I) include a selection of model exercises that government and private entities can readily adapt for use; and

(II) aid the governments and private entities with the design, implementation, and evaluation of exercises that—-

(aa) conform to the requirements described in clause (i);

(bb) are consistent with any applicable national, State, local, or Tribal strategy or plan; and

(cc) provide for systematic evaluation of readiness.

(C) CONSULTATION.—In carrying out the Exercise Program, the Director may consult with appropriate representatives from Sector Risk Management Agencies, the Office of the National Cyber Director, cybersecurity research stakeholders, and Sector Coordinating Councils.

(3) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to affect the authorities or responsibilities of the Administrator of the Federal Emergency Management Agency pursuant to subsections (a) and (b) of section 20508 of this title.

§ 10708. Strategy

(a) DEVELOPMENT OF STRATEGY.—The Secretary shall develop a departmental strategy to carry out cybersecurity responsibilities as set forth by law.

(b) CONTENTS.—The strategy required under subsection (a) shall include the following:

(1) Strategic and operational goals and priorities to successfully execute the full range of the Secretary's cybersecurity responsibilities.

(2) Information on the programs, policies, and activities that are required to successfully execute the full range of the Secretary's cybersecurity responsibilities, including programs, policies, and activities in furtherance of the following:

(A) Cybersecurity functions set forth in section 10706 of this title.

(B) Cybersecurity investigation capabilities.

(C) Cybersecurity research and development.

(D) Engagement with international cybersecurity partners.

(d) CONSIDERATIONS.—In developing the strategy required under subsection (a), the Secretary shall—

(1) consider—

(A) the cybersecurity strategy for the Homeland Security Enterprise published by the Secretary in November 2011;

(B) the Department of Homeland Security Fiscal Years 2014–2018 Strategic Plan; and

(C) the most recent quadrennial homeland security review issued pursuant to section 11706 of this title; and

(2) include information on the roles and responsibilities of components and offices of the Department, to the extent practicable, to carry out the strategy.

(d) IMPLEMENTATION PLAN.—Not later than 90 days after the development of the strategy required under subsection (a), the Secretary shall issue an implementation plan for the strategy that includes the following:

(1) Strategic objectives and corresponding tasks.

(2) Projected timelines and costs for the tasks.

(3) Metrics to evaluate performance of the tasks.

(e) CONGRESSIONAL OVERSIGHT.—The Secretary shall submit to Congress for assessment the following:

(1) A copy of the strategy required under subsection (a), on issuance.

(2) A copy of the implementation plan required under subsection (d), on issuance, together with detailed information on any associated legislative or budgetary proposals.

(f) CLASSIFIED INFORMATION.—The strategy required under subsection (a) shall be in an unclassified form but may contain a classified annex.

(g) RULE OF CONSTRUCTION.—Nothing in this section may be construed as permitting the Department to engage in monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

§ 10709. NET Guard

The Director may establish a national technology guard, to be known as ''NET Guard'', comprised of local teams of volunteers with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks.

§ 10710. Clearances

The Secretary shall make available the process of application for security clearances under Executive Order 13549 (50 U.S.C. 3161 note) or any successor Executive order to appropriate representatives of sector coordinating councils, sector Information Sharing and Analysis Organizations, owners and operators of critical infrastructure, and any other person the Secretary determines appropriate.

§ 10711. Federal intrusion detection and prevention system

(a) DEFINITIONS.—In subsections (a) through (f) of this section:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44.

(2) AGENCY INFORMATION.—The term ''agency information'' means information collected or maintained by or on behalf of an agency.

(3) AGENCY INFORMATION SYSTEM.—The term ''agency information system'' has the meaning given the term in section 10707 of this title.

(b) DEPLOYMENT, OPERATION, AND MAINTENANCE OF CAPABILITIES.—

(1) IN GENERAL.—The Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

(B) a capability to—

(i) prevent network traffic associated with those cybersecurity risks from transiting or traveling to or from an agency information system; or

(ii) modify the network traffic to remove the cybersecurity risk.

(2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

(c) ACTIVITIES.—In carrying out subsection (b), the Secretary—

(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses the information, notwithstanding another law that would otherwise restrict or prevent the head of an agency from disclosing the information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with subsection (b);

(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

(4) shall regularly assess, through operational test and evaluation in real world or simulated environments, available advanced protective technologies to improve detection and prevention capabilities, including commercial and noncommercial technologies and detection technologies beyond signature-based detection, and acquire, test, and deploy the technologies when appropriate;

(5) shall establish a pilot through which the Secretary may acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4); and

(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note).

(d) PRINCIPLES.—In carrying out subsection (b), the Secretary shall ensure that—

(1) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(2) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(3) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

(4) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

(e) PRIVATE ENTITIES.—

(1) CONDITIONS.—A private entity described in subsection (c)(2) may not—

(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity other than the Department or the agency that disclosed the information under subsection (c)(1), including personal information of a specific individual or information that identifies a specific individual not directly related to a cybersecurity risk; or

(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

(2) LIMITATION ON LIABILITY.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

(3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

(f) PRIVACY OFFICER REVIEW.—The Privacy Officer appointed under section 10520 of this title, in consultation with the Attorney General, shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable privacy laws, including those governing the acquisition, interception, retention, use, and disclosure of communications.

(g) AGENCY RESPONSIBILITIES.—

(1) DEFINITION OF AGENCY INFORMATION SYSTEM.—In this subsection, the term ''agency information system'' means an information system owned or operated by an agency.

(2) IN GENERAL.—Except as provided in paragraph (3)—

(A) the head of each agency shall apply and continue to utilize the intrusion detection and prevention capabilities to all information traveling between an agency information system and another information system; and

(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to subsection (b)(2), the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

(3) EXCEPTION.—The requirements under paragraph (2) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit an agency from applying the intrusion detection and prevention capabilities to an information system other than an agency information system under subsection (b)(1) at the discretion of the head of the agency or as provided in relevant policies, directives, and guidelines.

(h) RULE OF CONSTRUCTION.—Nothing in subsection (i) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under subsection (c)(2) if the assistance was rendered before the termination date under subsection (i) or otherwise during a period in which the assistance was authorized.

(i) TERMINATION.—The requirements under subsections (a) through (f) terminate on September 30, 2023.

§ 10712. National asset database

(a) ESTABLISHMENT.—

(1) NATIONAL ASSET DATABASE.—The Secretary shall establish and maintain a national database of each system or asset that—

(A) the Secretary, in consultation with appropriate homeland security officials of the States, determines to be vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States, a State, or a local government; or

(B) the Secretary determines is appropriate for inclusion in the database.

(2) PRIORITIZED CRITICAL INFRASTRUCTURE LIST.—In accordance with Homeland Security Presidential Directive–7, as in effect on January 1, 2007, the Secretary shall establish and maintain a single classified prioritized list of systems and assets included in the database under paragraph (1) that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects.

(b) USE OF DATABASE.—The Secretary shall use the database established under subsection (a)(1) in the development and implementation of Department plans and programs as appropriate.

(c) MAINTENANCE OF DATABASE.—

(1) IN GENERAL.—The Secretary shall maintain and annually update the database established under subsection (a)(1) and the list established under subsection (a)(2), including—

(A) establishing data collection guidelines and providing the guidelines to the appropriate homeland security official of each State;

(B) regularly reviewing the guidelines established under subparagraph (A), including by consulting with the appropriate homeland security officials of States, to solicit feedback about the guidelines, as appropriate;

(C) after providing the homeland security official of a State with the guidelines under subparagraph (A), allowing the official a reasonable amount of time to submit to the Secretary data recommended by the official for inclusion in the database established under subsection (a)(1);

(D) examining the contents and identifying submissions made by the official that are described incorrectly or that do not meet the guidelines established under subparagraph (A); and

(E) providing to the appropriate homeland security official of each relevant State a list of submissions identified under subparagraph (D) for review and possible correction before the Secretary finalizes the decision of which submissions will be included in the database established under subsection (a)(1).

(2) ORGANIZATION OF INFORMATION IN DATABASE.—The Secretary shall organize the contents of the database established under subsection (a)(1) and the list established under subsection (a)(2) as the Secretary determines is appropriate. Any organizational structure of the contents shall include the categorization of the contents—

(A) according to the sectors listed in the National Infrastructure Protection Plan developed pursuant to Homeland Security Presidential Directive–7; and

(B) by the State and county of their location.

(3) PRIVATE-SECTOR INTEGRATION.—The Secretary shall identify and evaluate methods, including the Department's Protected Critical Infrastructure Information Program, to acquire relevant private-sector information for the purpose of using that information to generate a database or list, including the database established under subsection (a)(1) and the list established under subsection (a)(2).

(4) RETENTION OF CLASSIFICATION.—The classification of information required to be provided to Congress, the Department, or another department or agency under this section by a Sector Risk Management Agency, including the assignment of a level of classification of the information, shall be binding on Congress, the Department, and that other Federal agency.

(d) REPORTS.—

(1) ANNUAL REPORT REQUIRED.—The Secretary shall submit annually to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the database established under subsection (a)(1) and the list established under subsection (a)(2).

(2) CONTENTS.—Each report shall include the following:

(A) The name, location, and sector classification of each of the systems and assets on the list established under subsection (a)(2).

(B) The name, location, and sector classification of each of the systems and assets on the list that are determined by the Secretary to be most at risk to terrorism.

(C) Any significant challenges in compiling the list of the systems and assets included on the list or in the database established under subsection (a)(1).

(D) Any significant changes from the preceding report in the systems and assets included on the list or in the database.

(E) If appropriate, the extent to which the database and the list have been used, individually or jointly, for allocating funds by the Federal Government to prevent, reduce, mitigate, or respond to acts of terrorism.

(F) The amount of coordination between the Department and the private sector, through an entity of the Department that meets with representatives of private-sector industries for purposes of coordination, for the purpose of ensuring the accuracy of the database and list.

(G) Other information the Secretary deems relevant.

(3) CLASSIFIED INFORMATION.—The report shall be submitted in unclassified form but may contain a classified annex.

(e) NATIONAL INFRASTRUCTURE PROTECTION CONSORTIUM.—The Secretary may establish the National Infrastructure Protection Consortium. The National Infrastructure Protection Consortium may advise the Secretary on the best way to identify, generate, organize, and maintain a database or list of systems and assets established by the Secretary, including the database established under subsection (a)(1) and the list established under subsection (a)(2). If the Secretary establishes the National Infrastructure Protection Consortium, the Consortium may—

(1) be composed of national laboratories, Federal agencies, State and local homeland security organizations, academic institutions, or national Centers of Excellence that have demonstrated experience working with and identifying critical infrastructure and key resources; and

(2) provide input to the Secretary on any request pertaining to the contents of the database or the list.

§ 10713. Prohibition on new regulatory authority

(a) NATIONAL CYBERSECURITY PROTECTION ACT OF 2014.—Nothing in the National Cybersecurity Protection Act of 2014 (Public Law 113–282, 128 Stat. 3066) or the amendments made by the Act shall be construed—

(1) to grant the Secretary any authority to promulgate regulations or set standards relating to the cybersecurity of private-sector critical infrastructure that was not in effect on December 17, 2014; or

(2) to require any private entity—

(A) to request assistance from the Secretary; or

(B) that requested assistance from the Secretary to implement any measure or recommendation suggested by the Secretary.

(b) SECTION 1716(B) OF THE WILLIAM. M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2021.—Nothing in section 1716 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–263, div. A, title XVII, 134 Stat. 4094) or the amendments made by that section shall be construed—

(1) to grant the Secretary or the head of any other Federal agency or department any authority to promulgate regulations or set standards relating to the cybersecurity of private-sector critical infrastructure that was not in effect on December 31, 2020; or

(2) to require any private entity—

(A) to request assistance from the Director; or

(B) to implement any measure or recommendation suggested by the Director.

Subchapter II—Critical Infrastructure Information

§ 10731. Definitions

In this subchapter:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 551 of title 5.

(2) COVERED FEDERAL AGENCY.—The term ''covered Federal agency'' means the Department.

(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term ''critical infrastructure information'' has the meaning given the term in section 10701 of this title.

(4) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.—The term ''critical infrastructure protection program'' means a component or bureau of a covered Federal agency that has been designated by the President or an agency head to receive critical infrastructure information.

(5) PROTECTED SYSTEM.—The term ''protected system''—

(A) means a service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes a physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(6) VOLUNTARY.—

(A) IN GENERAL.—The term ''voluntary'', in the case of a submittal of critical infrastructure information to a covered Federal agency, means the submittal of the information in the absence of the agency's exercise of legal authority to compel access to, or submission of, the information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) EXCLUSIONS.—The term ''voluntary''—

(i) in the case of an action brought under the securities laws as is defined in section 3(a) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a))—

(I) does not include information or statements contained in documents or materials filed with the Securities

and Exchange Commission, or with Federal banking regulators, under section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 78l(i)); and

(II) with respect to the submittal of critical infrastructure information, does not include a disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and

(ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

§ 10732. Designation of critical infrastructure protection program

A critical infrastructure protection program may be designated as such by one of the following:

(1) The President.

(2) The Secretary.

§ 10733. Protection of voluntarily shared critical infrastructure information

(a) PROTECTION.—

(1) DEFINITION OF EXPRESS STATEMENT.—For purposes of paragraph (2), the term ''express statement'', with respect to information or records, means—

(A) in the case of written information or records, a written marking on the information or records substantially similar to the following: ''This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the Critical Infrastructure Information Act of 2002.''; or

(B) in the case of oral information, a similar written statement submitted within a reasonable period following the oral communication.

(2) IN GENERAL.—Notwithstanding another law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (1)—

(A) shall be exempt from disclosure under section 552 of title 5 (known as the Freedom of Information Act);

(B) shall not be subject to agency rules or judicial doctrine regarding ex parte communications with a decision-making official;

(C) shall not, without the written consent of the person or entity submitting the information, be used directly by the agency, another Federal, State, or local authority, or a third party, in a civil action arising under Federal or State law if the information is submitted in good faith;

(D) shall not, without the written consent of the person or entity submitting the information, be used or disclosed by an officer or employee of the United States for purposes other than the purposes of this subchapter, except—

(i) in furtherance of an investigation or the prosecution of a criminal act; or

(ii) when disclosure of the information would be—

(I) to either House of Congress, or to the extent of matter within its jurisdiction, a committee or subcommittee of Congress (including a joint committee or subcommittee); or

(II) to the Comptroller General, or an authorized representative of the Comptroller General, in the course of the performance of the duties of the Government Accountability Office;

(E) shall not, if provided to a State or local government or government agency—

(i) be made available pursuant to State or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to a party by the State or local government or government agency without the written consent of the person or entity submitting the information; or

(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act; and

(F) does not constitute a waiver of an applicable privilege or protection provided under law, such as trade secret protection.

(b) LIMITATION.—A communication of critical infrastructure information to a covered Federal agency made pursuant to this subchapter shall not be considered to be an action subject to the requirements of chapter 10 of title 5.

(c) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local,

or Federal Government entity, agency, or authority, or a third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including information lawfully and properly disclosed generally or broadly to the public and to use the information in any manner permitted by law. For purposes of this section, a permissible use of independently obtained information includes the disclosure of the information under section 2302(b)(8) of title 5.

(d) TREATMENT OF VOLUNTARY SUBMITTAL OF INFORMATION.—The voluntary submittal to the Government of information or records that are protected from disclosure by this subchapter shall not be construed to constitute compliance with a requirement to submit the information to a Federal agency under any other provision of law.

(e) PROCEDURES.—

(1) IN GENERAL.—The Secretary shall, in consultation with appropriate representatives of the National Security Council and the Office of Science and Technology Policy, establish uniform procedures for the receipt, care, and storage by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government.

(2) ELEMENTS.—The procedures established under paragraph (1) shall include mechanisms regarding—

(A) the acknowledgement of receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government;

(B) the maintenance of the identification of the information as voluntarily submitted to the Government for purposes of, and subject to, this subchapter;

(C) the care and storage of the information; and

(D) the protection and maintenance of the confidentiality of the information so as to permit the sharing of the information within the Federal Government and with State and local governments, and the issuance of notices and warnings related to the protection of critical infrastructure and protected systems, in a manner to protect from public disclosure the identity of the submitting person or entity, or information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(f) PENALTIES.—Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this subchapter coming to him or her in the course of this em-

ployment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, the department or agency or officer or employee thereof, shall be fined under title 18, imprisoned not more than 1 year, or both, and shall be removed from office or employment.

(g) AUTHORITY TO ISSUE WARNINGS.—The Federal Government may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the Federal Government shall take appropriate actions to protect from disclosure—

(1) the source of voluntarily submitted critical infrastructure information that forms the basis for the warning; or

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(h) AUTHORITY TO DELEGATE.—The President may delegate authority to a critical infrastructure protection program, designated under section 10732 of this title, to enter into a voluntary agreement to promote critical infrastructure security, including with an Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 708 of the Defense Production Act of 1950 (50 U.S.C. 4558).

§ 10734. No private right of action

Nothing in this subchapter may be construed to create a private right of action for enforcement of a provision of this subtitle (except chapter 129).

Subchapter III—Cyber Response and Recovery

§ 10741. Definitions

For the purposes of this subchapter:

(1) ASSET RESPONSE ACTIVITY.—The term ''asset response activity'' means an activity to support an entity impacted by an incident with the response to, remediation of, or recovery from, the incident, including—

(A) furnishing technical and advisory assistance to the entity to protect the assets of the entity, mitigate vulnerabilities, and reduce the related impacts;

(B) assessing potential risks to the critical infrastructure sector or geographic region impacted by the incident, including potential cascading effects of the incident on other critical infrastructure sectors or geographic regions;

(C) developing courses of action to mitigate the risks assessed under subparagraph (B);

(D) facilitating information sharing and operational coordination with entities performing threat response activities; and

(E) providing guidance on how best to use Federal resources and capabilities in a timely, effective manner to speed recovery from the incident.

(2) DECLARATION.—The term ''declaration'' means a declaration of the Secretary under section 10742(a)(1) of this title.

(3) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(4) FEDERAL AGENCY.—The term ''Federal agency'' has the meaning given the term ''agency'' in section 3502 of title 44.

(5) FUND.—The term ''Fund'' means the Cyber Response and Recovery Fund under section 10743(a) of this title.

(6) INCIDENT.—The term ''incident'' has the meaning given the term ''agency'' in section 3552 of title 44.

(7) RENEWAL.—The term ''renewal'' means a renewal of a declaration under section 10742(d) of this title.

(8) SIGNIFICANT INCIDENT.—The term ''significant incident''—

(A) means an incident or a group of related incidents that results, or is likely to result, in demonstrable harm to—

(i) the national security interests, foreign relations, or economy of the United States; or

(ii) the public confidence, civil liberties, or public health and safety of the people of the United States; and

(B) does not include an incident or a portion of a group of related incidents that occurs on—

(i) a national security system (as defined in section 3552 of title 44); or

(ii) an information system described in paragraph (2) or (3) of section 3553(e) of title 44.

§ 10742. Declaration

(a) IN GENERAL.—

(1) DECLARATION.—The Secretary, in consultation with the National Cyber Director, may make a declaration of a significant incident in accordance with this section for the purpose of enabling the activities described in this subchapter if the Secretary determines—

(A) a specific significant incident—

(i) has occurred; or

(ii) is likely to occur imminently; and

(B) otherwise available resources, other than the Fund, are likely insufficient to respond effectively to, or to mitigate effectively, the specific significant incident described in subparagraph (A).

(2) PROHIBITION ON DELEGATION.—The Secretary may not delegate the authority provided to the Secretary under paragraph (1).

(b) ASSET RESPONSE ACTIVITIES.—On a declaration, the Director shall coordinate—

(1) the asset response activities of each Federal agency in response to the specific significant incident associated with the declaration; and

(2) with appropriate entities, which may include—

(A) public and private entities and State and local governments with respect to the asset response activities of those entities and governments; and

(B) Federal, State, local, and Tribal law enforcement agencies with respect to investigations and threat response activities of those law enforcement agencies; and

(3) Federal, State, local, and Tribal emergency management and response agencies.

(c) DURATION.—Subject to subsection (d), a declaration shall terminate on the earlier of—

(1) a determination by the Secretary that the declaration is no longer necessary; or

(2) the expiration of the 120-day period beginning on the date on which the Secretary makes the declaration.

(d) RENEWAL.—The Secretary, without delegation, may renew a declaration as necessary.

(e) PUBLICATION.—

(1) WHEN AND WHERE DECLARATION OR RENEWAL MUST BE PUBLISHED.—Not later than 72 hours after a declaration or a renewal, the Secretary shall publish the declaration or renewal in the Federal Register.

(2) WHAT MAY NOT BE INCLUDED.—A declaration or renewal published under paragraph (1) may not include the name of any affected individual or private company.

(f) ADVANCE ACTIONS.—

(1) IN GENERAL.—The Secretary—

(A) shall assess the resources available to respond to a potential declaration; and

(B) may take actions before and while a declaration is in effect to arrange or procure additional resources for asset response activities or technical assistance the Secretary determines necessary,

which may include entering into standby contracts with private entities for cybersecurity services or incident responders in the event of a declaration.

(2) EXPENDITURE OF FUNDS.—An expenditure from the Fund for the purpose of paragraph (1)(B) shall be made from amounts available in the Fund. Amounts available in the Fund shall be in addition to any other appropriations available to the Cybersecurity and Infrastructure Security Agency for that purpose.

§ 10743. Cyber Response and Recovery Fund

(a) IN GENERAL.—There is a Cyber Response and Recovery Fund, which shall be available for—

(1) the coordination of activities described in section 10742(b) of this title;

(2) response and recovery support for the specific significant incident associated with a declaration to Federal, State, local, and Tribal entities and public and private entities on a reimbursable or non-reimbursable basis, including through asset response activities and technical assistance, such as—

(A) vulnerability assessments and mitigation;

(B) technical incident mitigation;

(C) malware analysis;

(D) analytic support;

(E) threat detection and hunting; and

(F) network protections;

(3) as the Director determines appropriate, grants for, or cooperative agreements with, Federal, State, local, and Tribal entities and public and private entities to respond to, and recover from, the specific significant incident associated with a declaration, such as—

(A) hardware or software to replace, update, improve, harden, or enhance the functionality of existing hardware, software, or systems; and

(B) technical contract personnel support; and

(4) advance actions taken by the Secretary under section 10742(f)(1)(B) of this title.

(b) DEPOSITS AND EXPENDITURES.—

(1) IN GENERAL.—Amounts shall be deposited in the Fund from—

(A) appropriations to the Fund for activities of the Fund; and

(B) reimbursement from Federal agencies for the activities described in paragraphs (1), (2) and (4) of subsection (a), which shall only be from amounts made available in advance in appropriations Acts for the reimbursement.

(2) EXPENDITURES.—An expenditure from the Fund for the purposes of this subchapter shall be made from amounts available in the Fund from a deposit described in paragraph (1). Amounts available in the Fund shall be in addition to any other appropriations available to the Cybersecurity and Infrastructure Security Agency for those purposes.

(c) AMOUNTS SUPPLEMENT, NOT SUPPLANT, OTHER FUNDING.—Amounts in the Fund shall be used to supplement, not supplant, other Federal, State, local, or Tribal funding for activities in response to a declaration.

(d) REPORTING.—The Secretary shall require an entity that receives amounts from the Fund to submit a report to the Secretary that details the specific use of the amounts.

§ 10744. Notification and reporting

(a) NOTIFICATION.—On a declaration or renewal, the Secretary shall immediately notify the National Cyber Director and appropriate congressional committees and include in the notification—

(1) an estimation of the planned duration of the declaration;

(2) with respect to a notification of a declaration, the reason for the declaration, including information relating to the specific significant incident or imminent specific significant incident, including—

(A) the operational or mission impact or anticipated impact of the specific significant incident on Federal and non-Federal entities;

(B) if known, the perpetrator of the specific significant incident; and

(C) the scope of the Federal and non-Federal entities impacted or anticipated to be impacted by the specific significant incident malware analysis;

(3) with respect to a notification of a renewal, the reason for the renewal;

(4) justification as to why available resources, other than the Fund, are insufficient to respond to or mitigate the specific significant incident; and

(5) a description of the coordination activities described in section 10742(b) of this title that the Secretary anticipates the Director will perform.

(b) REPORT TO CONGRESS.—Not later than 180 days after the date of a declaration or renewal, the Secretary shall submit to the appropriate congressional committees a report that includes—

(1) the reason for the declaration or renewal, including information and intelligence relating to the specific significant incident that led to the declaration or renewal;

(2) the use of any funds from the Fund for the purpose of responding to the incident or threat described in paragraph (1);

(3) a description of the actions, initiatives, and projects undertaken by the Department and State and local governments and public and private entities in responding to and recovering from the specific significant incident described in paragraph (1);

(4) an accounting of the specific obligations and outlays of the Fund; and

(5) an analysis of—

(A) the impact of the specific significant incident described in paragraph (1) on Federal and non-Federal entities;

(B) the impact of the declaration or renewal on the response to, and recovery from, the specific significant incident described in paragraph (1); and

(C) the impact of the funds made available from the Fund as a result of the declaration or renewal on the recovery from, and response to, the specific significant incident described in paragraph (1).

(c) CLASSIFICATION.— Each notification made under subsection (a) and each report submitted under subsection (b)—

(1) shall be in an unclassified form with appropriate markings to indicate information that is exempt from disclosure under section 552 of title 5 (known as the Freedom of Information Act); and

(2) may include a classified annex.

(d) CONSOLIDATED REPORT.—The Secretary shall not be required to submit multiple reports under subsection (b) for multiple declarations or renewals if the Secretary determines that the declarations or renewals substantively relate to the same specific significant incident.

(e) EXEMPTION.—The requirements of subchapter I of chapter 35 of title 44 shall not apply to the voluntary collection of information by the Department during an investigation of, a response to, or an immediate post-response review of, the specific significant incident leading to a declaration or renewal.

§ 10745. Rule of construction

Nothing in this subchapter shall be construed to impair or limit the ability of the Director to carry out the authorized activities of the Cybersecurity and Infrastructure Security Agency.

§ 10746. Authorization of appropriations

There is authorized to be appropriated to the Fund $20,000,000 for fiscal year 2022 and each fiscal year thereafter until September 30, 2028, which shall remain available until September 30, 2028.

§ 10747. Sunset

The authorities granted to the Secretary or the Director under this subchapter shall expire on November 15, 2028.

Subchapter IV—Cyber Incident Reporting

§ 10761. Definitions

In this subchapter:

(1) CENTER.—The term ''Center'' means the center established under section 10706 of this title.

(2) COUNCIL.—The term ''Council'' means the Cyber Incident Reporting Council described insection 10767 of this title.

(3) COVERED CYBER INCIDENT.—The term ''covered cyber incident'' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant tosection 10763(b) of this title.

(4) COVERED ENTITY.—The term ''covered entity'' means an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant tosection 10763(b) of this title.

(5) CYBER INCIDENT.—The term ''cyber incident''—

(A) has the meaning given the term ''incident'' insection 10701 of this title; and

(B) does not include an occurrence that imminently, but not actually, jeopardizes—

(i) information on information systems; or

(ii) information systems.

(6) CYBER THREAT.—The term ''cyber threat'' has the meaning given the term ''cybersecurity threat'' in section 10701 of this title.

(7) FEDERAL ENTITY.—The term ''Federal entity'' has the meaning given the term in section 10781 of this title.

(8) RANSOM PAYMENT.—The term ''ransom payment'' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

(9) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the

United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

(10) VIRTUAL CURRENCY.—The term ''virtual currency'' means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

(11) VIRTUAL CURRENT ADDRESS.—The term ''virtual currency address'' means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.

§ 10762. Cyber incident review

(a) CENTER ACTIVITIES.—The Center shall—

(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to subchapter V and sections 10801 through 10804 and 10821 of this title, reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, to identify tactics, techniques, and procedures adversaries use to overcome those controls, and for other cybersecurity purposes, including to assess potential impact of cyber incidents on public health and safety and to enhance situational awareness of cyber threats across critical infrastructure sectors;

(2) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

(3) leverage information gathered about cyber incidents to—

(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, critical infrastructure owners and operators, cybersecurity and cyber incident response firms, and security researchers; and

(B) provide appropriate entities, including sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, cybersecurity and cyber incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant tosection 10766 of this title;

(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident re-

ports, ransom payment reports, and other voluntarily provided information, and how the Agency can most effectively support private sector cybersecurity;

(5) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities, and identify and disseminate ways to prevent or mitigate similar cyber incidents in the future;

(6) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy that definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

(7) with respect to covered cyber incident reports under sections10763(a) and 10764 of this title involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions in the Agency, as appropriate;

(8) publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations based on covered cyber incident reports, which may be based on the unclassified information contained in the briefings required under subsection (c);

(9) proactively identify opportunities, consistent with the protections insection 10766 of this title, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable; and

(10) in accordance withsection 10766 of this titleand subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, voluntarily submitted information pursuant tosection 10764 of this title, or information received pursuant to a request for information or subpoena undersection 10765 of this title, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

(b) INFORMATION SHARING.—The President or a designee of the President—

(1) may establish a specific time requirement for sharing information under subsection (a)(10); and

(2) shall determine the appropriate Federal agencies under subsection (a)(10).

(c) PERIODIC BRIEFINGS.—Not later than 60 days after the effective date of the final rule required undersection 10763(b) of this title, and on the 1st day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

(1) include the total number of reports submitted undersections 10763 and 10764 of this titleduring the preceding month, including a breakdown of required and voluntary reports;

(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted undersections 10763 and 10764 of this title, including—

(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

(3) include a summary of the known uses of the information in reports submitted undersections 10763 and 10764 of this title; and

(4) include an unclassified portion, but may include a classified component.

§ 10763. Required reporting of certain cyber incidents

(a) IN GENERAL.—

(1) Covered cyber incident reports.—

(A) IN GENERAL.—A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

(B) LIMITATION.—The Director may not require reporting under subparagraph (A) any earlier than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred.

(2) RANSOM PAYMENT REPORTS.—

(A) IN GENERAL.—A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours after the ransom payment has been made.

(B) APPLICATION.—The requirements under subparagraph (A) shall apply even if the ransomware attack is not a covered cyber incident subject to the reporting requirements under paragraph (1).

(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Agency an update or supplement to a previously submitted covered cyber incident report if substantial new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1), until the date that the covered entity notifies the Agency that the covered cyber incident at issue has concluded and has been fully mitigated and resolved.

(4) PRESERVATION OF INFORMATION.—Any covered entity subject to the requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b).

(5) EXCEPTIONS.—

(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered entity is the victim of a covered cyber incident and makes a ransom payment prior to the 72 hour requirement under paragraph (1), such that the reporting requirements under paragraphs (1) and (2) both apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b).

(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—

(i) IN GENERAL.—Subject to the limitation described in clause (ii), where the Agency has an agreement in place that satisfies the requirements ofsection 10768(b) of this title, the requirements under paragraphs (1), (2), and (3) shall not apply to a covered entity required by law, regulation, or con-

tract to report substantially similar information to another Federal agency within a substantially similar timeframe.

(ii) LIMITATION.—The exemption in clause (i) shall take effect with respect to a covered entity once an agency agreement and sharing mechanism is in place between the Agency and the respective Federal agency, pursuant tosection 10768(b) of this title.

(iii) RULES OF CONSTRUCTION.—Nothing in this paragraph shall be construed to—

(I) exempt a covered entity from the reporting requirements under paragraph (3) unless the supplemental report also meets the requirements of clauses (i) and (ii) of this subparagraph;

(II) prevent the Agency from contacting an entity submitting information to another Federal agency that is provided to the Agency pursuant tosection 10768 of this title; or

(III) prevent an entity from communicating with the Agency.

(C) DOMAIN NAME SYSTEM.—The requirements under paragraphs (1), (2) and (3) shall not apply to a covered entity or the functions of a covered entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority.

(6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

(7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect on the dates prescribed in the final rule issued pursuant to subsection (b).

(b) RULEMAKING.—

(1) NOTICE OF PROPOSED RULEMAKING.—Not later than March 15, 2024, the Director, in consultation with Sector Risk Management Agencies, the Department of Justice, and other Federal agencies, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

(2) FINAL RULE.—Not later than 18 months after publication of the notice of proposed rulemaking under paragraph (1), the Director shall issue a final rule to implement subsection (a).

(3) SUBSEQUENT RULEMAKINGS.—

(A) IN GENERAL.—The Director may issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

(B) PROCEDURES.—Any subsequent rules issued under subparagraph (A) shall comply with the requirements underchapter 5 of title 5, including the issuance of a notice of proposed rulemaking under section 553 of title 5.

(c) ELEMENTS.—The final rule issued pursuant to subsection (b) shall be composed of the following elements:

(1) A clear description of the types of entities that constitute covered entities, based on—

(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

(A) at a minimum, require the occurrence of—

(i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of the information system or network, or a serious impact on the safety and resiliency of operational systems and processes;

(ii) a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability, against—

(I) an information system or network; or

(II) an operational technology system or process; or

(iii) unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

(B) consider—

(i) the sophistication or novelty of the tactics used to perpetrate the cyber incident, as well as the type, volume, and sensitivity of the data at issue;

(ii) the number of individuals directly or indirectly affected or potentially affected by the cyber incident; and

(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

(C) exclude—

(i) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; and

(ii) the threat of disruption as extortion, as described insection 10701 of this title.

(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the covered entity shall comply with the requirements in this subchapter in reporting the covered cyber incident or ransom payment.

(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident:

(A) A description of the covered cyber incident, including—

(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by the cyber incident;

(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

(iii) the estimated date range of the incident; and

(iv) the impact to the operations of the covered entity.

(B) Where applicable, a description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident.

(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for the cyber incident.

(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.

(E) The name and other information that clearly identifies the covered entity impacted by the covered cyber incident, including, as applicable, the State of incorporation or formation of the covered entity, trade names, legal names, or other identifiers.

(F) Contact information, such as telephone number or electronic mail address, that the Agency may use to contact the covered entity or an authorized agent of the covered entity, or, where applicable, the service provider of the covered entity acting with the express permission of, and at the direction of, the covered entity to assist with compliance with the requirements of this subchapter.

(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

(A) A description of the ransomware attack, including the estimated date range of the attack.

(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack.

(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

(D) The name and other information that clearly identifies the covered entity that made the ransom payment or on whose behalf the payment was made.

(E) Contact information, such as telephone number or electronic mail address, that the Agency may use to contact the covered entity that made the ransom payment or an authorized agent of the covered entity, or, where applicable, the service provider of the covered entity acting with the express permission of, and at the direction of, the covered entity to assist with compliance with the requirements of this subchapter.

(F) The date of the ransom payment.

(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency

address or physical address the funds were requested to be sent to, if applicable.

(I) The amount of the ransom payment.

(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4), the period of time for which the data is required to be preserved, and allowable uses, processes, and procedures.

(7) Deadlines and criteria for submitting supplemental reports to the Agency required under subsection (a)(3), which shall—

(A) be established by the Director in consultation with the Council;

(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which the covered entity may also be subject, and make efforts to harmonize the timing and contents of the reports to the maximum extent practicable;

(C) balance the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations; and

(D) provide a clear description of what constitutes substantial new or different information.

(8) Procedures for—

(A) entities, including third parties pursuant to subsection (d)(1), to submit reports required by paragraphs (1), (2), and (3) of subsection (a), including the manner and form of the reports, which shall include, at a minimum, a concise, user-friendly web-based form;

(B) the Agency to carry out—

(i) the enforcement provisions ofsection 10765 of this title, including with respect to the issuance, service, withdrawal, referral process, and enforcement of subpoenas, appeals, and due process procedures;

(ii) other available enforcement mechanisms, including acquisition, suspension, and debarment procedures; and

(iii) other aspects of noncompliance;

(C) implementing the exceptions provided in subsection (a)(5); and

(D) protecting privacy and civil liberties consistent with processes adopted pursuant tosection 10784(c) of this titleand anonymizing and safeguarding, or no longer retaining, information received and disclosed through covered cyber incident reports and

ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

(9) Other procedural measures directly necessary to implement subsection (a).

(d) THIRD PARTY REPORT SUBMISSION AND RANSOM PAYMENT.—

(1) REPORT SUBMISSION.—A covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a).

(2) RANSOM PAYMENT.—If a covered entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

(3) DUTY TO REPORT.—Third-party reporting under this subparagraph does not relieve a covered entity from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

(4) RESPONSIBILITY TO ADVISE.—Any third party used by a covered entity that knowingly makes a ransom payment on behalf of a covered entity impacted by a ransomware attack shall advise the impacted covered entity of the responsibilities of the impacted covered entity regarding reporting ransom payments under this section.

(e) OUTREACH TO COVERED ENTITIES.—

(1) IN GENERAL.—The Agency shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of covered entities impacted by ransomware attacks, and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

(2) ELEMENTS.—The outreach and education campaign under paragraph (1) shall include the following:

(A) An overview of the final rule issued pursuant to subsection (b).

(B) An overview of mechanisms to submit to the Agency covered cyber incident reports, ransom payment reports, and information relating to the disclosure, retention, and use of covered cyber incident reports and ransom payment reports under this section.

(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

(D) An overview of the steps taken undersection 10765 of this titlewhen a covered entity is not in compliance with the reporting requirements under subsection (a).

(E) Specific outreach to cybersecurity vendors, cyber incident response providers, cybersecurity insurance entities, and other entities that may support covered entities.

(F) An overview of the privacy and civil liberties requirements in this subchapter.

(3) COORDINATION.—In conducting the outreach and education campaign required under paragraph (1), the Agency may coordinate with—

(A) the Critical Infrastructure Partnership Advisory Council established undersection 10391 of this title;

(B) Information Sharing and Analysis Organizations;

(C) trade associations;

(D) information sharing and analysis centers;

(E) sector coordinating councils; and

(F) any other entity as determined appropriate by the Director.

(f) EXEMPTION.—Sections 3506(c), 3507, 3508, and 3509 of title 44shall not apply to any action to carry out this section.

(g) RULE OF CONSTRUCTION.—Nothing in this section shall affect the authorities of the Federal Government to implement the requirements of Executive Order 14028 (86 Fed. Reg. 26633), including changes to the Federal Acquisition Regulations and remedies to include suspension and debarment.

(h) SAVINGS PROVISION.—Nothing in this section shall be construed to supersede or to abrogate, modify, or otherwise limit the authority that is vested in any officer or any agency of the United States Government to regulate or take action with respect to the cybersecurity of an entity.

§ 10764. Voluntary reporting of other cyber incidents

(a) IN GENERAL.—Entities may voluntarily report cyber incidents or ransom payments to the Agency that are not required under paragraph (1), (2), or (3) ofsection 10763(a) of this title, but may enhance the situational awareness of cyber threats.

(b) VOLUNTARY PROVISION OF ADDITIONAL INFORMATION IN REQUIRED REPORTS.—Covered entities may voluntarily include in reports required under paragraph (1), (2), or (3) ofsection 10763(a) of this titleinformation that is not required to be included but may enhance the situational awareness of cyber threats.

(c) APPLICATION OF SECTION 10766.—Section 10766 of this title shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b) as it applies to reports and information submitted under section 10763 of this title.

§ 10765. Noncompliance with required reporting

(a) PURPOSE.—In the event that a covered entity that is required to submit a report undersection 10763(a) of this titlefails to comply with the requirement to report, the Director may obtain information about the cyber incident or ransom payment by engaging the covered entity directly to request information about the cyber incident or ransom payment, and if the Director is unable to obtain information through the engagement, by issuing a subpoena to the covered entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred.

(b) INITIAL REQUEST FOR INFORMATION.—

(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) ofsection 10762(a) of this title, that a covered entity has experienced a covered cyber incident or made a ransom payment but failed to report the cyber incident or payment to the Agency in accordance withsection 10763(a) of this title, the Director may request additional information from the covered entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

(2) TREATMENT.—Information provided to the Agency in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established insection 10763 of this title including that section 10766 of this title shall apply to the information in the same manner and to the same extent to information submitted in response to requests under paragraph (1) as it applies to information submitted under section 10763 of this title.

(c) ENFORCEMENT.—

(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the covered entity from which the information was requested, or received an inadequate response, the Director may—

(A) issue—

(i) to the covered entity a subpoena to compel disclosure of information the Director considers necessary to determine whether a covered cyber incident or ransom payment has oc-

curred and obtain the information required to be reported pursuant tosection 10763 of this title;and

(ii) any implementing regulations; and

(B) assess potential impacts to national security, economic security, or public health and safety.

(2) CIVIL ACTION.—

(A) IN GENERAL.—If a covered entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce the subpoena.

(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the covered entity against which the action is brought resides, is found, or does business.

(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this subsection as contempt of court.

(3) NON-DELEGATION.—The authority of the Director to issue a subpoena under this subsection may not be delegated.

(4) AUTHENTICATION.—

(A) IN GENERAL.—Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that the subpoena was issued by the Agency and has not been altered or modified since issuance.

(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of the subpoena.

(d) PROVISION OF CERTAIN INFORMATION TO ATTORNEY GENERAL.—

(1) IN GENERAL.—Notwithstandingparagraph (b)(2) and section 10766(a)(5) of this title, if the Director determines, based on the information provided in response to a subpoena issued pursuant to subsection (c), that the facts relating to the cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Director may provide the information to the Attorney General or the head of the appropriate Federal regulatory agency, who may use the information for a regulatory enforcement action or criminal prosecution.

(2) CONSULTATION.—The Director may consult with the Attorney General or the head of the appropriate Federal regulatory agency when making the determination under paragraph (1).

(e) CONSIDERATIONS.—When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

(1) the complexity in determining if a covered cyber incident has occurred; and

(2) prior interaction with the Agency or awareness of the covered entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

(f) EXCLUSIONS.—This section shall not apply to a State, local, Tribal, or territorial government entity.

(g) REPORT TO CONGRESS.—The Director shall submit to Congress an annual report on the number of times the Director—

(1) issued an initial request for information pursuant to subsection (b);

(2) issued a subpoena pursuant to subsection (c); or

(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

(h) PUBLICATION OF ANNUAL REPORT.—The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

(1) issued an initial request for information pursuant to subsection (b); or

(2) issued a subpoena pursuant to subsection (c).

(i) ANONYMIZATION OF REPORTS.—The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

§ 10766. Information shared with or provided to the Federal Government

(a) DISCLOSURE, RETENTION, AND USE.—

(1) AUTHORIZED ACTIVITIES.—Information provided to the Agency pursuant tosection 10763 or 10764 of this titlemay be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(A) a cybersecurity purpose;

(B) the purpose of identifying—

(i) a cyber threat, including the source of the cyber threat; or

(ii) a security vulnerability;

(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;

(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident reported pursuant tosection 10763 or 10764 of this titleor any of the offenses listed insection 10784(e)(5)(A)(v) of this title.

(2) AGENCY ACTIONS AFTER RECEIPT.—

(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—On receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the Agency shall immediately review the report to determine whether the cyber incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use the report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

(B) PRINCIPLES FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in covered cyber incident and ransom payment reports submitted to the Agency pursuant tosection 10763 of this titleshall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant tosection 10784 of this titleand in a manner that protects personal information from unauthorized use or unauthorized disclosure.

(4) DIGITAL SECURITY.—The Agency shall ensure that reports submitted to the Agency pursuant tosection 10763 of this title, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—

(A) IN GENERAL.—A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Agency in accordance with this subchapter to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment unless the government entity expressly allows entities to submit reports to the Agency to meet regulatory reporting obligations of the entity.

(B) ALLOWANCE FOR REGULATIONS.—A report submitted to the Agency pursuant tosection 10763 or 10764 of this titlemay, consistent with Federal or State regulatory authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to those systems.

(b) PROTECTIONS FOR REPORTING ENTITIES AND INFORMATION.—Reports describing covered cyber incidents or ransom payments submitted to the Agency by entities in accordance withsection 10763 of this title, as well as voluntarily-submitted cyber incident reports submitted to the Agency pursuant tosection 10764 of this title, shall—

(1) be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity;

(2) be exempt from disclosure undersection 552(b)(3) of title 5, as well as any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records;

(3) be considered not to constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection; and

(4) not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(c) LIABILITY PROTECTIONS.—

(1) IN GENERAL.—No cause of action for the submission of a report pursuant tosection 10763(a) of this titlethat is submitted in conformance with this subchapter and the rule promulgated undersection 10763(b) of this title shall lie or be maintained in any court by any person or entity and the action shall be promptly dismissed, except that this subsection shall not apply with regard to an action by the Federal Government pursuant tosection 10765(c)(2) of this title.

(2) SCOPE.—The liability protections provided in this subsection shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Agency.

(3) RESTRICTIONS.—Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this subchapter or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting the report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision of a State, provided that nothing in this subchapter shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting the report.

(d) SHARING WITH NON-FEDERAL ENTITIES.—The Agency shall anonymize the victim who reported the information when making information provided in reports received undersection 10763 of this titleavailable to critical infrastructure owners and operators and the general public.

(e) RELATIONSHIP TO CHAPTER 121 OF TITLE 18.—Nothing in this subchapter shall be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed underchapter 121 of title 18.

§ 10767. Cyber Incident Reporting Council

(a) RESPONSIBILITY OF THE SECRETARY.—The Secretary shall lead an intergovernmental Cyber Incident Reporting Council, in consultation with the Director of the Office of Management and Budget, the Attorney General, the National Cyber Director, Sector Risk Management Agencies, and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations.

(b) RULE OF CONSTRUCTION.—Nothing in subsection (a) shall be construed to provide any additional regulatory authority to any Federal entity.

§ 10768. Federal sharing of incident reports

(a) DEFINITIONS.—In this section:

(1) SECTION 10701 DEFINITIONS.—The terms ''Agency'', ''Director'', ''information system'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 10701 of this title.

(2) SECTION 10761 DEFINITIONS—The terms ''covered cyber incident'', ''covered entity'', ''cyber incident'', and ''ransom payment'' have the meanings given those terms in section 10761 of this title.

(b) CYBER INCIDENT REPORTING SHARING

(1) IN GENERAL.—Notwithstanding any other provision of law or regulation, any Federal agency, including any independent establishment (as defined insection 104 of title 5), that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Agency as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Department (including the Agency) and the recipient Federal agency. The Director shall share and coordinate each report pursuant tosection 10762(b) of this title.

(2) RULE OF CONSTRUCTION.—The requirements described in paragraph (1) andsection 10766(d) of this title may not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure or provision of information within the executive branch.

(3) PROTECTION OF INFORMATION.—The Director shall comply with any obligations of the recipient Federal agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would impose greater protection requirements than this subchapter or the amendments made by the Cyber Incident Reporting for Critical Instructure Act of 2022 (Public Law 117–103, div. Y, 136 Stat. 1038).

(4) EFFECTIVE DATE.—This subsection shall take effect on the effective date of the final rule issued pursuant tosection 10763(b) of this title.

(5) AGENCY AGREEMENTS.—

(A) IN GENERAL.—The Agency and any Federal agency, including any independent establishment (as defined insection 104 of title 5), that receives incident reports from entities, including due to ransomware attacks, shall, as appropriate, enter into a documented agreement to establish policies, processes, procedures, and

mechanisms to ensure reports are shared with the Agency pursuant to paragraph (1).

(B) AVAILABILITY.—To the maximum extent practicable, each documented agreement required under subparagraph (A) shall be made publicly available.

(C) REQUIREMENT.—The documented agreements required by subparagraph (A) shall require reports be shared from Federal agencies with the Agency in such time as to meet the overall timeline for covered entity reporting of covered cyber incidents and ransom payments established insection 10763 of this title.

(c) HARMONIZING REPORTING REQUIREMENTS.—The Secretary, acting through the Director, shall, in consultation with the Cyber Incident Reporting Council described insection 10767 of this title, to the maximum extent practicable—

(1) periodically review existing regulatory requirements, including the information required in the reports, to report incidents and ensure that any reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with appropriate Federal partners and regulatory authorities that receive reports relating to incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agreements between the authorities to permit the sharing of the reports, consistent with applicable law and policy, without impacting the ability of the Agency to gain timely situational awareness of a covered cyber incident or ransom payment.

Subchapter V—Cybersecurity Information Sharing

§ 10781. Definitions

In this subchapter:

(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) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' has the meaning given the term in section 10701 of this title.

(5) CYBERSECURITY PURPOSE.—The term ''cybersecurity purpose'' has the meaning given the term in section 10701 of this title.

(6) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given the term in section 10701 of this title.

(7) DEFENSIVE MEASURE.—The term ''defensive measure'' has the meaning given the term in section 10701 of this title.

(8) FEDERAL ENTITY.—The term ''Federal entity'' means a department or agency of the United States or any component of the department or agency.

(9) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 10701 of this title.

(10) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village or other political subdivision of a State.

(11) MALICIOUS CYBER COMMAND AND CONTROL.—The term ''malicious cyber command and control'' has the meaning given the term in section 10701 of this title.

(12) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' has the meaning given the term in section 10701 of this title.

(13) MONITOR.—The term ''monitor'' has the meaning given the term in section 10701 of this title.

(14) NON-FEDERAL ENTITY.—

(A) IN GENERAL.—Except as provided in this paragraph, the term ''non-Federal entity'' means any private entity, non-Federal Government agency or department, or State, tribal, or local government (including a political subdivision, department, or component of the government).

(B) INCLUSIONS.—The term ''non-Federal entity'' includes a government agency or department of the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the

Northern Mariana Islands, and any other territory or possession of the United States.

(C) EXCLUSIONS.—The term ''non-Federal entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(15) PRIVATE ENTITY.—

(A) IN GENERAL.—Except as provided in this paragraph, the term ''private entity'' means any person or private group, organization, proprietorship, partnership, trust, cooperative organization, or other commercial or nonprofit entity, including an officer, employee, or agent.

(B) INCLUSION.—The term ''private entity'' includes a State, tribal, or local government performing utility services, such as electric, natural gas, or water services.

(C) EXCLUSION.—The term ''private entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(16) SECURITY CONTROL.—The term ''security control'' has the meaning given the term in section 10701 of this title.

(17) SECURITY VULNERABILITY.—The term ''security vulnerability'' has the meaning given the term in section 10701 of this title.

(18) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304).

§ 10782. Procedures for sharing information by Federal Government

(a) IN GENERAL.—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall jointly develop and issue procedures to facilitate and promote—

(1) timely sharing of classified cyber threat indicators and defensive measures the Federal Government possesses with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances;

(2) timely sharing with relevant Federal entities and non-Federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this subchapter, in the possession of the Federal Government, that may be declassified and shared at an unclassified level;

(3) timely sharing with relevant Federal entities and non-Federal entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators and defensive measures the Federal Government possesses;

(4) timely sharing with Federal entities and non-Federal entities, if appropriate, of information relating to cybersecurity threats or authorized uses under this subchapter that the Federal Government possesses about cybersecurity threats to those entities to prevent or mitigate adverse effects from the threats; and

(5) periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this subchapter, in the possession of the Federal Government with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).

(b) CONTENT.—The procedures developed under subsection (a) shall—

(1) ensure the Federal Government has and maintains the capability to share cyber threat indicators and defensive measures in real time consistent with the protection of classified information;

(2) incorporate to the greatest extent practicable existing processes and existing roles and responsibilities of Federal entities and non-Federal entities for information sharing by the Federal Government, including sector-specific information sharing and analysis centers;

(3) include procedures for notifying, in a timely manner, Federal entities and non-Federal entities that have received a cyber threat indicator or defensive measure from a Federal entity under this subchapter that is known or determined to be in error or in contravention of the requirements of this subchapter or another provision of Federal law or policy of the error or contravention;

(4) include requirements for Federal entities sharing cyber threat indicators or defensive measures to implement and utilize security controls to protect against unauthorized access to, or acquisition of, the indicators or measures;

(5) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—

(A) to—

(i) review the indicator to assess whether the indicator contains any information not directly related to a cybersecurity threat that the Federal entity knows at the time of sharing

to be personal information of a specific individual or information that identifies a specific individual; and

(ii) remove the information; or

(B) to implement and utilize a technical capability configured to remove information not directly related to a cybersecurity threat that the Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual; and

(6) include procedures for notifying, in a timely manner, any United States person whose personal information is known or determined to have been shared by a Federal entity in violation of this subchapter.

(c) CONSULTATION.—In developing the procedures required under this section, the Director of National Intelligence, the Secretary, the Secretary of Defense, and the Attorney General shall consult with appropriate Federal entities, including the Small Business Administration and the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

(d) SUBMITTAL TO CONGRESS.—The Director of National Intelligence, in consultation with the heads of the appropriate Federal entities, shall submit to Congress a report on the procedures required by subsection (a).

§ 10783. Authorization for preventing, detecting, analyzing, and mitigating cybersecurity threats

(a) AUTHORIZATION FOR MONITORING.—

(1) IN GENERAL.—Notwithstanding another law, a private entity may, for cybersecurity purposes, monitor—

(A) an information system of the private entity;

(B) an information system of another non-Federal entity, on the authorization and written consent of the other entity;

(C) an information system of a Federal entity, on the authorization and written consent of an authorized representative of the Federal entity; and

(D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

(2) CONSTRUCTION.—Nothing in paragraph (1) shall be construed to—

(A) authorize the monitoring of an information system, or the use of information obtained through the monitoring, other than as provided in this subchapter; or

(B) limit otherwise lawful activity.

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

(1) IN GENERAL.—Notwithstanding another law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

(A) an information system of the private entity to protect the rights or property of the entity;

(B) an information system of another non-Federal entity, on written consent of the other entity for operation of the defensive measure to protect the rights or property of the entity;

(C) an information system of a Federal entity on written consent of an authorized representative of the Federal entity for operation of the defensive measure to protect the rights or property of the Federal Government.

(2) CONSTRUCTION.—Nothing in paragraph (1) shall be construed to—

(A) authorize the use of a defensive measure other than as provided in paragraph (1); or

(B) limit otherwise lawful activity.

(c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding another law, a non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive, from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure.

(2) COMPLIANCE WITH LAWFUL RESTRICTION.—A non-Federal entity receiving a cyber threat indicator or defensive measure from another non-Federal entity or a Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of the indicator or defensive measure by the sharing non-Federal entity or Federal entity.

(3) CONSTRUCTION.—Nothing in paragraph (1) shall be construed to—

(A) authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in paragraph (1); or

(B) limit otherwise lawful activity.

(d) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—A non-Federal entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this sec-

tion shall implement and utilize a security control to protect against unauthorized access to or acquisition of the cyber threat indicator or defensive measure.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—A non-Federal entity sharing a cyber threat indicator pursuant to this subchapter shall, prior to sharing—

(A) review the cyber threat indicator to assess whether the indicator contains any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove the information; or

(B) implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

(3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY NON-FEDERAL ENTITIES.—

(A) IN GENERAL.—Consistent with this subchapter, a cyber threat indicator or defensive measure shared or received under this section may, for cybersecurity purposes—

(i) be used by a non-Federal entity to monitor or operate a defensive measure that is applied to—

(I) an information system of the non-Federal entity; or

(II) an information system of another non-Federal entity or a Federal entity on the written consent of the other non-Federal entity or that Federal entity; and

(ii) be otherwise used, retained, and further shared by a non-Federal entity subject to—

(I) an otherwise lawful restriction placed by the sharing non-Federal entity or Federal entity on the cyber threat indicator or defensive measure; or

(II) an otherwise applicable provision of law.

(B) CONSTRUCTION.—Nothing in subparagraph (A) shall be construed to authorize the use of a cyber threat indicator or defensive measure other than as provided in this section.

(4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL GOVERNMENT.—

(A) LAW ENFORCEMENT USE.—A State, tribal, or local government that receives a cyber threat indicator or defensive measure under this subchapter may use the cyber threat indicator or defensive measure for the purposes described in section 10784(e)(5)(A) of this title.

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator or defensive measure shared by or with a State, tribal, or local government, including a component of a State, tribal, or local government that is a private entity, under this section shall be—

(i) considered voluntarily shared information; and

(ii) exempt from disclosure under any provision of State, tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records.

(C) STATE, TRIBAL, AND LOCAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), a cyber threat indicator or defensive measure shared with a State, tribal, or local government under this subchapter shall not be used by any State, tribal, or local government to regulate, including an enforcement action, the lawful activity of any non-Federal entity or any activity taken by a non-Federal entity pursuant to mandatory standards, including an activity relating to monitoring, operating a defensive measure, or sharing a cyber threat indicator.

(ii) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—A cyber threat indicator or defensive measure shared as described in clause (i) may, consistent with a State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to the information systems.

(e) ANTITRUST EXEMPTION.—

(1) IN GENERAL.—Except as provided in section 10789(e) of this title, it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator or defensive measure, or assistance, relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this subchapter.

(2) APPLICABILITY.—Paragraph (1) shall apply only to information that is exchanged or assistance provided to assist with—

(A) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or

(B) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.

(f) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator or defensive measure with a non-Federal entity under this subchapter shall not create a right or benefit to similar information by the non-Federal entity or any other non-Federal entity.

§ 10784. Sharing of cyber threat indicators and defensive measures with Federal Government

(a) DEVELOPMENT OF POLICIES AND PROCEDURES.—The Attorney General and the Secretary shall, in consultation with the heads of the appropriate Federal entities, jointly issue and make publicly available policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government. Consistent with the guidelines required by subsection (e), the policies and procedures shall ensure—

(1) that cyber threat indicators shared with the Federal Government by any non-Federal entity pursuant to section 10783(c) of this title through the real-time process described in subsection (d)—

(A) are shared in an automated manner with all appropriate Federal entities;

(B) are only subject to a delay, modification, or other action due to controls established for the real-time process that could impede real-time receipt by all appropriate Federal entities when the delay, modification, or other action is due to controls—

(i) agreed on unanimously by all of the heads of the appropriate Federal entities;

(ii) carried out before any appropriate Federal entity retains or uses the cyber threat indicators or defensive measures; and

(iii) uniformly applied so that each appropriate Federal entity is subject to the same delay, modification, or other action; and

(C) may be provided to other Federal entities;

(2) that cyber threat indicators shared with the Federal Government by any non-Federal entity pursuant to section 10783 of this title in a manner other than the real-time process described in subsection (d)—

(A) are shared as quickly as operationally practicable with all appropriate Federal entities;

(B) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all appropriate Federal entities; and

(C) may be provided to other Federal entities; and

(3) there are—

(A) audit capabilities; and

(B) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this subchapter in an unauthorized manner.

(b) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT.—The Attorney General and the Secretary jointly shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this subchapter. The guidelines shall include guidance on the following:

(1) Identification of types of information that would qualify as a cyber threat indicator under this subchapter that would be unlikely to include information that—

(A) is not directly related to a cybersecurity threat; and

(B) is personal information of a specific individual or information that identifies a specific individual.

(2) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

(3) Such other matters as the Attorney General and the Secretary consider appropriate for entities sharing cyber threat indicators with Federal entities under this subchapter.

(c) PRIVACY AND CIVIL LIBERTIES.—

(1) ISSUANCE AND AVAILABILITY OF GUIDELINES.—The Attorney General and the Secretary shall, in coordination with the heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with industry expertise as the Attorney General and the Secretary consider relevant, jointly issue and make publicly available final guidelines relating to privacy and civil liberties that shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this subchapter.

(2) CONTENT.—The guidelines shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the effect on privacy and civil liberties of activities by the Federal Government under this subchapter;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals, including by establishing—

(i) a process for the timely destruction of the information that is known not to be directly related to uses authorized under this subchapter; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of the guidelines;

(D) consistent with this subchapter, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled ''National Strategy for Trusted Identities in Cyberspace'' and published by the President in April 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this subchapter, including the extent to which the cyber threat indicators may be used by the Federal Government;

(E) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving the information not to constitute a cyber threat indicator;

(F) protect the confidentiality of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals to the greatest extent practicable and require recipients to be informed that the indicators may only be used for purposes authorized under this subchapter; and

(G) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

(3) PERIODIC REVIEW.—The Attorney General and the Secretary shall, in coordination with the heads of the appropriate Federal entities and in consultation with officers and private entities described in paragraph (1), periodically, but not less frequently than once every 2 years, jointly review the guidelines issued under paragraph (1).

(d) CAPABILITY AND PROCESS IN THE DEPARTMENT.—

(1) IN GENERAL.—The Secretary, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process in the Department that—

(A) shall accept from any non-Federal entity in real time cyber threat indicators and defensive measures, pursuant to this section;

(B) on submittal of the certification under paragraph (2) that the capability and process fully and effectively operates as described in paragraph (2), shall be the process by which the Federal Government receives cyber threat indicators and defensive measures under this subchapter that are shared by a non-Federal entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems, except—

(i) consistent with section 10733 of this title, communications between a Federal entity and a non-Federal entity regarding a previously shared cyber threat indicator to—

(I) describe the relevant cybersecurity threat; or

(II) develop a defensive measure based on the cyber threat indicator; and

(ii) communications by a regulated non-Federal entity with the entity's Federal regulatory authority regarding a cybersecurity threat;

(C) ensures that all of the appropriate Federal entities receive in an automated manner cyber threat indicators and defensive measures shared through the real-time process in the Department;

(D) is in compliance with the policies, procedures, and guidelines required by this section; and

(E) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—

(i) the reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or a Federal entity, including cyber threat indicators or defensive measures shared with a Federal entity in furtherance of opening a Federal law enforcement investigation;

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) the provision of cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

(2) CERTIFICATION AND DESIGNATION.—

(A) CERTIFICATION OF CAPABILITY AND PROCESS.—The Secretary shall, in consultation with the heads of the appropriate Federal entities, submit to Congress a certification as to whether the capability and process required by paragraph (1) fully and effectively operates—

(i) as the process by which the Federal Government receives from any non-Federal entity a cyber threat indicator or defensive measure under this subchapter; and

(ii) in accordance with the interim policies, procedures, and guidelines developed under this subchapter.

(B) DESIGNATION.—

(i) IN GENERAL.—At any time after certification is submitted under subparagraph (A), the President may designate an appropriate Federal entity, other than the Department of Defense (including the National Security Agency), to develop and implement a capability and process as described in paragraph (1) in addition to the capability and process developed under paragraph (1) by the Secretary, if, not fewer than 30 days before making the designation, the President submits to Congress a certification and explanation that—

(I) the designation is necessary to ensure full, effective, and secure operation of a capability and process for the Federal Government to receive from any non-Federal entity cyber threat indicators or defensive measures under this subchapter;

(II) the designated appropriate Federal entity will receive and share cyber threat indicators and defensive measures in accordance with the policies, procedures, and guidelines developed under this subchapter, including subsection (a)(1); and

(III) the designation is consistent with the mission of the appropriate Federal entity and improves the ability of the Federal Government to receive, share, and use cyber threat indicators and defensive measures as authorized under this subchapter.

(ii) APPLICATION TO ADDITIONAL CAPABILITY AND PROCESS.—If the President designates an appropriate Federal entity to develop and implement a capability and process under clause (i), this subchapter that apply to the capability and process required by paragraph (1) apply to the capability and process developed and implemented under clause (i).

(3) PUBLIC NOTICE AND ACCESS.—The Secretary shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—

(A) any non-Federal entity may share cyber threat indicators and defensive measures through the process with the Federal Government; and

(B) all of the appropriate Federal entities receive the cyber threat indicators and defensive measures in real time with receipt through the process in the Department consistent with the policies and procedures issued under subsection (a).

(4) OTHER FEDERAL ENTITIES.—The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive in a timely manner any cyber threat indicators and defensive measures shared with the Federal Government through the process.

(e) INFORMATION SHARED WITH OR PROVIDED TO FEDERAL GOVERNMENT.—

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of cyber threat indicators and defensive measures to the Federal Government under this subchapter shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with section 10783(c)(2) of this title and any other applicable provision of law, a cyber threat indicator or defensive measure provided by a non-Federal entity to the Federal Government under this subchapter shall be considered the commercial, financial, and proprietary information of the non-Federal entity when so designated by the originating non-Federal entity or a third party acting in accordance with the written authorization of the originating non-Federal entity.

(3) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator or defensive measure shared with the Federal Government under this subchapter shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5 and any State, tribal, or local provision of law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5 and any State, tribal, or local provision of law requiring disclosure of information or records.

(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this subchapter shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) AUTHORIZED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter may, consistent with otherwise applicable provisions of Federal law, be disclosed to, retained by, and used by any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of identifying—

(I) a cybersecurity threat, including the source of the cybersecurity threat; or

(II) a security vulnerability;

(iii) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(iv) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(v) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iii) or any of the offenses listed in sections 1028 through 1030 and chapters 37 and 90 of title 18.

(B) PROHIBITED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subparagraph (A).

(C) PRIVACY AND CIVIL LIBERTIES.—Cyber threat indicators and defensive measures provided to the Federal Government under

this subchapter shall be retained, used, and disseminated by the Federal Government—

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) through (c);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain—

(I) personal information of a specific individual; or

(II) information that identifies a specific individual; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing—

(I) personal information of a specific individual; or

(II) information that identifies a specific individual.

(D) FEDERAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this subchapter shall not be used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity or any activities taken by a non-Federal entity pursuant to mandatory standards, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators.

(ii) EXCEPTIONS.—

(I) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to the information systems.

(II) PROCEDURES DEVELOPED AND IMPLEMENTED UNDER THIS SUBCHAPTER.—Clause (i) shall not apply to procedures developed and implemented under this subchapter.

§ 10785. Protection from liability

(a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall be brought in any court against any private entity, and the action shall be promptly dismissed, for the monitoring of an information system and infor-

mation under section 10783(a) of this title that is conducted in accordance with this subchapter.

(b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of action shall be brought in any court against any private entity, and the action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 10783(c) of this title if—

(1) the sharing or receipt is conducted in accordance with this subchapter; and

(2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with section 10784(d)(1)(B) of this title.

(c) CONSTRUCTION.—Nothing in this subchapter shall be construed—

(1) to create—

(A) a duty to share a cyber threat indicator or defensive measure; or

(B) a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure; or

(2) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

§ 10786. Oversight of Government activities

(a) REPORT ON IMPLEMENTATION.—Not later than December 18, 2016, the heads of the appropriate Federal entities shall jointly submit to Congress a detailed report concerning the implementation of this subchapter. The report may include such recommendations as the heads of the appropriate Federal entities may have for improvements or modifications to the authorities, policies, procedures, and guidelines under this subchapter and shall include the following:

(1) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 10784(d) of this title, including any impediments to real-time sharing.

(2) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for sharing cyber threat indicators or defensive measures with the private sector.

(3) The number of cyber threat indicators or defensive measures received through the capability and process developed under section 10784(d) of this title.

(4) A list of Federal entities that have received cyber threat indicators or defensive measures under this subchapter.

(b) BIENNIAL REPORT ON COMPLIANCE.—

(1) WHEN REPORT SHALL BE SUBMITTED.—Not later than December 18, 2017, and not less frequently than once every 2 years thereafter, the inspectors general of the appropriate Federal entities, in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress an interagency report on the actions of the executive branch of the Federal Government to carry out this subchapter during the most recent 2-year period.

(2) CONTENTS.—Each report shall include, for the period covered by the report, the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines relating to the sharing of cyber threat indicators in the Federal Government, including those policies, procedures, and guidelines relating to the removal of information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) A review of the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government under this subchapter, including a review of the following:

(i) The appropriateness of subsequent uses and dissemination of cyber threat indicators or defensive measures.

(ii) Whether cyber threat indicators or defensive measures were shared in a timely and adequate manner with appropriate entities, or, if appropriate, were made publicly available.

(D) An assessment of the cyber threat indicators or defensive measures shared with the appropriate Federal entities under this subchapter, including the following:

(i) The number of cyber threat indicators or defensive measures shared through the capability and process developed under section 10784(d) of this title.

(ii) An assessment of any information not directly related to a cybersecurity threat that is personal information of a

specific individual or information identifying a specific individual and was shared by a non-Federal government entity with the Federal Government in contravention of this subchapter, or was shared in the Federal Government in contravention of the guidelines required by this subchapter, including a description of any significant violation of this subchapter.

(iii) The number of times, according to the Attorney General, that information shared under this subchapter was used by a Federal entity to prosecute an offense listed in section 10784(e)(5)(A) of this title.

(iv) A quantitative and qualitative assessment of the effect of the sharing of cyber threat indicators or defensive measures with the Federal Government on the privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that was personal information of a specific individual or information that identified a specific individual in accordance with the procedures required by section 10784(c)(2)(E) of this title.

(v) The adequacy of any steps taken by the Federal Government to reduce any adverse effect from activities carried out under this subchapter on the privacy and civil liberties of United States persons.

(E) An assessment of the sharing of cyber threat indicators or defensive measures among Federal entities to identify inappropriate barriers to sharing information.

(3) RECOMMENDATIONS.—Each report may include such recommendations as the inspectors general may have for improvements or modifications to the authorities and processes under this subchapter.

(c) INDEPENDENT REPORT ON REMOVAL OF PERSONAL INFORMATION.—Not later than December 18, 2018, the Comptroller General shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures pursuant to this subchapter. The report shall include an assessment of the sufficiency of the policies, procedures, and guidelines established under this subchapter in addressing concerns relating to privacy and civil liberties.

(d) FORM OF REPORTS.—Each report required under this section shall be submitted in an unclassified form, but may include a classified annex.

(e) PUBLIC AVAILABILITY OF REPORTS.—The unclassified portions of the reports required under this section shall be made available to the public.

§ 10787. Report on cybersecurity threats

(a) DEFINITION OF INTELLIGENCE COMMUNITY.—In this section, the term ''intelligence community'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(b) WHEN REPORT SHALL BE SUBMITTED.—Not later than 180 days after December 18, 2015, the Director of National Intelligence, in coordination with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyberattacks, theft, and data breaches.

(c) CONTENTS.—The report shall include the following:

(1) An assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats, including cyberattacks, theft, and data breaches, directed against the United States that threaten the United States' national security interests, economy, and intellectual property, specifically identifying the relative utility of the relationships, which elements of the intelligence community participate in the relationships, and whether and how the relationships could be improved.

(2) A list and an assessment of the countries and nonstate actors that are the primary threats to carry out a cybersecurity threat, including a cyberattack, theft, or data breach, against the United States that threatens the United States' national security, economy, and intellectual property.

(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats, including cyberattacks, theft, or data breaches, directed against the United States private sector are degraded by a delay in the prompt notification by private entities of those threats or cyberattacks, theft, and data breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats, including cyberattacks, theft, and data breaches.

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(d) FORM OF REPORT.—The report required by subsection (b) shall be made available in classified and unclassified forms.

§ 10788. Exception to limitation on authority of Secretary of Defense to disseminate information

Notwithstanding section 393(c)(3) of title 10, the Secretary of Defense may authorize the sharing of cyber threat indicators and defensive measures pursuant to the policies, procedures, and guidelines developed or issued under this subchapter.

§ 10789. Construction and preemption

(a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this subchapter shall be construed—

(1) to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or the Federal Government under this subchapter; or

(2) to limit or prohibit otherwise lawful use of the disclosures by any Federal entity, even when the otherwise lawful disclosures duplicate or replicate disclosures made under this subchapter.

(b) WHISTLE BLOWER PROTECTIONS.—Nothing in this subchapter shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) or 7211 of title 5, section 1034 of title 10, section 1104 of the National Security Act of 1947 (50 U.S.C. 3234), or any similar provision of Federal or State law.

(c) PROTECTION OF SOURCES AND METHODS.—Nothing in this subchapter shall be construed—

(1) to create any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or department of the Government, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

(d) RELATIONSHIP TO OTHER LAWS.—Nothing in this subchapter shall be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to the Federal Government.

(e) PROHIBITED CONDUCT.—Nothing in this subchapter shall be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanging

price or cost information, customer lists, or information regarding future competitive planning.

(f) INFORMATION SHARING RELATIONSHIPS.—Nothing in this subchapter shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any non-Federal entity and a Federal entity or another non-Federal entity; or

(4) to require the use of the capability and process in the Department developed under section 10784(d) of this title.

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this subchapter shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between non-Federal entities, or between a non-Federal entity and a Federal entity; or

(2) to abrogate trade secret or intellectual property rights of a non-Federal entity or Federal entity.

(h) ANTI-TASKING RESTRICTION.—Nothing in this subchapter shall be construed to permit a Federal entity—

(1) to require a non-Federal entity to provide information to a Federal entity or another non-Federal entity;

(2) to condition the sharing of cyber threat indicators with a non-Federal entity on the entity's provision of cyber threat indicators to a Federal entity or another non-Federal entity; or

(3) to condition the award of a Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity or another non-Federal entity.

(i) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this subchapter shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this subchapter.

(j) USE AND RETENTION OF INFORMATION.—Nothing in this subchapter shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this subchapter for any use other than permitted in this subchapter.

(k) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This subchapter supersedes any statute or other provision of law of a State or political subdivision of a State that re-

stricts or otherwise expressly regulates an activity authorized under this subchapter.

(2) STATE LAW ENFORCEMENT.—Nothing in this subchapter shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

(l) REGULATORY AUTHORITY.—Nothing in this subchapter shall be construed—

(1) to authorize the prescribing of any regulations not specifically authorized to be issued under this subchapter;

(2) to establish or limit any regulatory authority not specifically established or limited under this subchapter; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

(m) AUTHORITY OF SECRETARY OF DEFENSE TO RESPOND TO MALICIOUS CYBER ACTIVITY CARRIED OUT BY FOREIGN POWERS.—Nothing in this subchapter shall be construed to limit the authority of the Secretary of Defense under section 394 of title 10.

(n) DISCLOSURE IN CRIMINAL PROSECUTION.—Nothing in this subchapter shall be construed to prevent the disclosure of a cyber threat indicator or defensive measure shared under this subchapter in a criminal prosecution when an applicable provision of Federal, State, tribal, or local law requires disclosure in the case.

§ 10790. Effective period

(a) IN GENERAL.—Except as provided in subsection (b), this subchapter and the amendments made by the Cybersecurity Information Sharing Act of 2015 (Public Law 114–113, div. N, title I, 129 Stat. 2936) are effective during the period ending on September 30, 2025.

(b) EXCEPTION.—With respect to any action authorized by this subchapter or information obtained pursuant to an action authorized by this subchapter that occurs before the date on which the provisions referred to in subsection (a) cease to have effect, this subchapter shall continue in effect.

Subchapter VI—Cybersecurity Enhancement

Part A—Federal Cybersecurity Enhancement

§ 10801. Definitions

In this part:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44.

(2) AGENCY INFORMATION SYSTEM.—The term ''agency information system'' has the meaning given the term in section 10707 of this title.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

(B) the Committee on Homeland Security of the House of Representatives.

(4) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given the term in section 10701 of this title.

(5) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

(6) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 10706 of this title.

(7) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(8) NATIONAL SECURITY SYSTEM.—The term ''national security system'' has the meaning given the term in section 11103 of title 40.

§ 10802. Advanced internal defenses

(a) ADVANCED NETWORK SECURITY TOOLS.—

(1) IN GENERAL.—The Secretary shall include, in the efforts of the Department to continuously diagnose and mitigate cybersecurity risks, advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, and to detect and mitigate intrusions and anomalous activity.

(2) DEVELOPMENT OF PLAN.—The Director shall develop, and the Secretary shall implement, a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

(b) PRIORITIZING ADVANCED SECURITY TOOLS.—The Director and the Secretary, in consultation with appropriate agencies, shall—

(1) review and update Government-wide policies and programs to ensure appropriate prioritization and use of network security monitoring tools in agency networks; and

(2) brief appropriate congressional committees on the prioritization and use.

(c) IMPROVED METRICS.—The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under sec-

tion 3554 of title 44 to include measures of intrusion and incident detection and response times.

(d) TRANSPARENCY AND ACCOUNTABILITY.—The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, by displaying metrics for department components, small agencies, and micro-agencies.

(e) EXCEPTION.—The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

§ 10803. Federal cybersecurity requirements

(a) IMPLEMENTATION OF FEDERAL CYBERSECURITY STANDARDS.—Consistent with section 3553 of title 44, the Secretary, in consultation with the Director, shall exercise the authority to issue binding operational directives to assist the Director in ensuring timely agency adoption of, and compliance with, policies and standards promulgated under section 11331 of title 40 for securing agency information systems.

(b) CYBERSECURITY REQUIREMENTS AT AGENCIES.—

(1) IN GENERAL.—Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44 and the standards and guidelines promulgated under section 11331 of title 40 and except as provided in paragraph (2), not later than December 18, 2016, the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44;

(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data;

(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement identity management consistent with section 504 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7464), including multi-factor authentication, for—

(i) remote access to an agency information system; and

(ii) each user account with elevated privileges on an agency information system.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to an agency information system for which—

(A) the head of the agency has personally certified to the Director with particularity that—

(i) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the cybersecurity requirement;

(ii) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and

(iii) the agency has taken all necessary steps to secure the agency information system and agency information stored on or transiting it; and

(B) the head of the agency or the designee of the head of the agency has submitted the certification described in subparagraph (A) to the appropriate congressional committees and the agency's authorizing committees.

(3) CONSTRUCTION.—

(A) AUTHORITY OF OFFICIALS NOT ALTERED.—Nothing in this section shall be construed to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44.

(B) DEVELOPMENT OF TECHNOLOGY, STANDARDS, POLICIES, AND GUIDELINES NOT AFFECTED.—Nothing in this section shall be construed to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of title 44 or to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

(c) EXCEPTION.—The requirements under this section do not apply to the Department of Defense, a national security system, or an element of the intelligence community.

§ 10804. Assessment; reports

(a) DEFINITIONS.—In this section:

(1) AGENCY INFORMATION.—The term ''agency information'' has the meaning given the term in section 10711 of this title.

(2) CYBER THREAT INDICATOR; DEFENSIVE MEASURE.—The terms ''cyber threat indicator'' and ''defensive measure'' have the meanings given the terms in section 10701 of this title.

(3) INTRUSION ASSESSMENTS.—The term ''intrusion assessments'' means actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems.

(4) INTRUSION ASSESSMENT PLAN.—The term ''intrusion assessment plan'' means the plan required under section 10707(b) of this title.

(5) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—The term ''intrusion detection and prevention capabilities'' means the capabilities required under section 10711(b) of this title.

(b) THIRD PARTY ASSESSMENT.—Not later than December 18, 2018, the Comptroller General shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.

(c) REPORTS TO CONGRESS.—

(1) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—

(A) SECRETARY.—The Secretary not later than June 18 each year shall submit to the appropriate congressional committees a report on the status of the implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and noncommercial technologies;

(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and noncommercial technologies;

(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency information sys-

tems on each iteration of the intrusion detection and prevention capabilities, and the number of each type of indicator, identifier, and technique;

(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention capabilities blocked network traffic associated with cybersecurity risk; and

(vi) a description of the pilot established under section 10711(c)(5) of this title, including the number of new technologies tested and the number of participating agencies.

(B) DIRECTOR.—Not later than June 18, 2017, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, an analysis of agency application of the intrusion detection and prevention capabilities, including—

(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and

(ii) a list by agency of—

(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect the cybersecurity risks; and

(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect the agency information systems.

(C) CHIEF INFORMATION OFFICER.—Not earlier than June 18, 2017, and not later than December 18, 2017, the Federal Chief Information Officer shall review and submit to the appropriate congressional committees a report assessing the intrusion detection and intrusion prevention capabilities, including—

(i) the effectiveness of the system in detecting, disrupting, and preventing cyber-threat actors, including advanced per-

sistent threats, from accessing agency information and agency information systems;

(ii) whether the intrusion detection and prevention capabilities, continuous diagnostics and mitigation, and other systems deployed under subtitle C of title II of the Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2155) are effective in securing Federal information systems;

(iii) the costs and benefits of the intrusion detection and prevention capabilities, including as compared to commercial technologies and tools and including the value of classified cyber threat indicators; and

(iv) the capability of agencies to protect sensitive cyber threat indicators and defensive measures if they were shared through unclassified mechanisms for use in commercial technologies and tools.

(2) DEVELOPMENT AND IMPLEMENTATION OF INTRUSION ASSESSMENT PLAN, ADVANCED INTERNAL DEFENSES, AND FEDERAL CYBERSECURITY REQUIREMENTS.—The Director—

(A) 30 days after any update to the intrusion assessment plan, shall submit the intrusion assessment plan to the appropriate congressional committees;

(B) not later than December 18, 2016, and annually thereafter, shall submit to Congress, as part of the report required under section 3553(c) of title 44—

(i) a description of the implementation of the intrusion assessment plan;

(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;

(iii) a description of the advanced network security tools included in the efforts to continuously diagnose and mitigate cybersecurity risks pursuant to section 10802(a)(1) of this title; and

(iv) a list by agency of compliance with the requirements of section 10803(b) of this title; and

(C) not later than December 18, 2016, shall submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 10802(a)(2) of this title; and

(ii) the improved metrics developed pursuant to section 10802(c) of this title.

(3) TERMINATION.—The requirements under this subsection terminate on September 30, 2023.

(d) FORM.—Each report required under this section shall be submitted in unclassified form, but may include a classified annex.

§ 10805. Report of security vulnerabilities on appropriate information systems

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security, the Committee on Armed Services, the Committee on Energy and Commerce, and the Permanent Select Committee on Intelligence of the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs, the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, and the Select Committee on Intelligence of the Senate.

(2) APPROPRIATE INFORMATION SYSTEM.—The term '' appropriate information system'' means an information system that the Secretary selects for inclusion under the vulnerability disclosure policy required by subsection (b).

(3) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term by section 3502 of title 44.

(4) SECURITY VULNERABILITY.—The term ''security vulnerability'' has the meaning given the term in section 10801 of this title.

(b) VULNERABILITY DISCLOSURE POLICY.—The Secretary shall establish a policy applicable to individuals, organizations, and companies that report security vulnerabilities on appropriate information systems of the Department. The policy shall include the following:

(1) The appropriate information systems of the Department that individuals, organizations, and companies may use to discover and report security vulnerabilities on appropriate information systems.

(2) The conditions and criteria under which individuals, organizations, and companies may operate to discover and report security vulnerabilities.

(3) How individuals, organizations, and companies may disclose to the Department security vulnerabilities discovered on appropriate information systems of the Department.

(4) The ways in which the Department may communicate with individuals, organizations, and companies that report security vulnerabilities.

(5) The process the Department shall use for public disclosure of reported security vulnerabilities.

(c) MITIGATION OR REMEDIATION PROCESS.—The Secretary shall develop a process for the Department to address the mitigation or remediation of the security vulnerabilities reported through the policy developed in subsection (b).

(d) CONSULTATION.—

(1) IN GENERAL.—In developing the security vulnerability disclosure policy under subsection (b), the Secretary shall consult with the following:

(A) The Attorney General regarding how to ensure that individuals, organizations, and companies that comply with the requirements of the policy developed under subsection (b) are protected from prosecution under section 1030 of title 18, civil lawsuits, and similar provisions of law with respect to specific activities authorized under the policy.

(B) The Secretary of Defense and the Administrator of General Services regarding lessons that may be applied from existing vulnerability disclosure policies.

(C) Non-governmental security researchers.

(2) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of title 5 shall not apply to any consultation under this subsection.

(e) PUBLIC AVAILABILITY.—The Secretary shall make the policy developed under subsection (b) publicly available.

(f) SUBMISSION TO CONGRESS.—

(1) DISCLOSURE POLICY AND MITIGATION OR REMEDIATION PROCESS.—Not later than 90 days after December 21, 2018, the Secretary shall submit to the appropriate congressional committees a copy of the policy required under subsection (b) and the process required under subsection (c).

(2) REPORT AND BRIEFING.—

(A) REPORT.—Not later than 1 year after establishing the policy required under subsection (b), the Secretary shall submit to the appropriate congressional committees a report on the policy and the process required under subsection (c).

(B) ANNUAL BRIEFING.—One year after the date of the submission of the report under subparagraph (A) and annually thereafter for each of the next 3 years, the Secretary shall provide to the appropriate congressional committees a briefing on the policy required under subsection (b) and the process required under subsection (c).

(C) MATTERS FOR INCLUSION.—The report required under subparagraph (A) and the briefings required under subparagraph (B) shall include the following with respect to the policy required under subsection (b) and the process required under subsection (c) for the period covered:

(i) The number of unique vulnerabilities reported.

(ii) The number of previously unknown security vulnerabilities mitigated or remediated.

(iii) The number of unique individuals, organizations, and companies that reported security vulnerabilities.

(iv) The average length of time between the reporting of security vulnerabilities and mitigation or remediation of the vulnerabilities.

§ 10806. Bug bounty pilot program

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate.

(B) the Select Committee on Intelligence of the Senate.

(C) the Committee on Homeland Security of the House of Representatives; and

(D) the Permanent Select Committee on Intelligence of the House of Representatives.

(2) BUG BOUNTY PROGRAM.—The term ''bug bounty program'' means a program under which—

(A) individuals, organizations, and companies are temporarily authorized to identify and report vulnerabilities of appropriate information systems of the Department; and

(B) eligible individuals, organizations, and companies receive compensation in exchange for the reports.

(3) ELIGIBLE INDIVIDUAL, ORGANIZATION, OR COMPANY.—The term ''eligible individual, organization, or company'' means an individual, organization, or company that meets such criteria as the Secretary determines in order to receive compensation in compliance with Federal laws.

(4) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44.

(5) PILOT PROGRAM.—The term ''pilot program'' means the bug bounty program required to be established under subsection (b).

(b) ESTABLISHMENT.—

(1) IN GENERAL.—Not later than 180 days after December 21, 2018, the Secretary shall establish, in the Office of the Chief Information Officer, a bug bounty pilot program to minimize vulnerabilities of appropriate information systems of the Department.

(2) AUTHORITY TO AWARD CONTRACT TO MANAGE PROGRAM.—In establishing the pilot program, the Secretary, subject to the availability of appropriations, may award 1 or more competitive contracts to an entity, as necessary, to manage the pilot program.

(c) RESPONSIBILITIES OF SECRETARY.—In establishing and conducting the pilot program, the Secretary shall—

(1) designate appropriate information systems to be included in the pilot program;

(2) provide compensation to eligible individuals, organizations, and companies for reports of previously unidentified security vulnerabilities in the information systems designated under paragraph (1);

(3) establish criteria for individuals, organizations, and companies to be considered eligible for compensation under the pilot program in compliance with Federal laws;

(4) consult with the Attorney General on how to ensure that approved individuals, organizations, and companies that comply with the requirements of the pilot program are protected from prosecution under section 1030 of title 18 and similar provisions of law, and from civil lawsuits, for specific activities authorized under the pilot program;

(5) consult with the Secretary of Defense and the heads of other departments and agencies that have implemented programs to provide compensation for reports of previously undisclosed vulnerabilities in information systems, regarding lessons that may be applied from the programs;

(6) develop an expeditious process by which an individual, organization, or company can register with the Department, submit to a background check as determined by the Department, and receive a determination as to eligibility; and

(7) engage, as constructive and to the extent practicable, qualified interested persons, including non-government sector representatives, about the structure of the pilot program.

(d) REPORT TO CONGRESS.—Not later than 180 days after the date on which the pilot program is completed, the Secretary shall submit to the appropriate congressional committees a report on the pilot program, which shall include—

(1) the number of individuals, the number of organizations, and the number of companies that participated in the pilot program, broken down by the number of individuals, organizations, or companies that—

(A) registered;

(B) were determined eligible;

(C) submitted security vulnerabilities; and

(D) received compensation;

(2) the number and severity of vulnerabilities reported as part of the pilot program;

(3) the number of previously unidentified security vulnerabilities remediated as a result of the pilot program;

(4) the current number of outstanding previously unidentified vulnerabilities and Department remediation plans;

(5) the average length of time between the reporting of security vulnerabilities and remediation of the vulnerabilities;

(6) the type of compensation provided under the pilot program; and

(7) the lessons learned from the pilot program.

§ 10807. Pilot program on public-private partnerships with internet ecosystem companies to detect and disrupt adversary cyber operations

(a) DEFINITIONS.—In this section:

(1)APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services of the Senate; and

(B) the Committee on Homeland Security and the Committee on Armed Services of the House of Representatives.

(2)INTERNET ECOSYSTEM COMPANY.—The term ''internet ecosystem company'' means a business incorporated in the United States that provides cybersecurity services, internet service, content delivery services, Domain Name Service, cloud services, mobile telecommunications services, email and messaging services, internet browser services, or such other services as the Secretary determines appropriate for the purposes of the pilot program under subsection (b).

(b)IN GENERAL.—Not later than December 27, 2022, the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency and in coordination with the Secretary of Defense and the National Cyber Director, shall commence a pilot program to assess the feasibility and advisability of entering into public-private partnerships with internet ecosystem companies to facilitate, within the bounds of applicable provisions of law and those companies' terms of service, policies, procedures, contracts,

and other agreements, actions by those companies to discover and disrupt use by malicious cyber actors of the platforms, systems, services, and infrastructure of those companies.

(c)PUBLIC-PRIVATE PARTNERSHIPS.—-

(1)IN GENERAL.—-In carrying out the pilot program under subsection (b), the Secretary shall seek to enter into one or more public-private partnerships with internet ecosystem companies.

(2)VOLUNTARY PARTICIPATION.—

(A)IN GENERAL.—Participation by an internet ecosystem company in a public-private partnership under the pilot program, including in any activity described in subsection (d), shall be voluntary.

(B)PROHIBITION.—No funds appropriated by any Act may be used to direct, pressure, coerce, or otherwise require that any internet ecosystem company take any action on their platforms, systems, services, or infrastructure as part of the pilot program.

(d)Authorized Activities.—In carrying out the pilot program under subsection (b), the Secretary may—-

(1) provide assistance to a participating internet ecosystem company to develop effective know-your-customer processes and requirements;

(2) provide information, analytics, and technical assistance to improve the ability of participating companies to detect and prevent illicit or suspicious procurement, payment, and account creation on their own platforms, systems, services, or infrastructure;

(3) develop and socialize best practices for the collection, retention, and sharing of data by participating internet ecosystem companies to support discovery of malicious cyber activity, investigations, and attribution on the platforms, systems, services, or infrastructure of those companies;

(4) provide to participating internet ecosystem companies actionable, timely, and relevant information, such as information about ongoing operations and infrastructure, threats, tactics, and procedures, and indicators of compromise, to enable those companies to detect and disrupt the use by malicious cyber actors of the platforms, systems, services, or infrastructure of the companies;

(5) provide recommendations for (but not design, develop, install, operate, or maintain) operational workflows, assessment and compliance practices, and training that participating internet ecosystem companies can implement to reliably detect and disrupt the use by malicious cyber actors of the platforms, systems, services, or infrastructure of the companies;

(6) provide recommendations for accelerating, to the greatest extent practicable, the automation of existing or implemented operational workflows to operate at line-rate to enable real-time mitigation without the need for manual review or action;

(7) provide recommendations for (but not design, develop, install, operate, or maintain) technical capabilities to enable participating internet ecosystem companies to collect and analyze data on malicious activities occurring on the platforms, systems, services, or infrastructure of those companies to detect and disrupt operations of malicious cyber actors; and

(8) provide recommendations regarding relevant mitigations for suspected or discovered malicious cyber activity and thresholds for action.

(e)COMPETITION CONCERNS.Consistent withsection 1905 of title 18, the Secretary shall ensure that any trade secret or proprietary information of a participating internet ecosystem company made known to the Federal Government pursuant to a public-private partnership under the pilot program remains private and protected unless explicitly authorized by the company.

(f)IMPARTIALITY.—-In carrying out the pilot program under subsection (b), the Secretary may not take any action that is intended primarily to advance the particular business interests of an internet ecosystem company but may take actions that advance the interests of the United States, notwithstanding differential impact or benefit to a given company's or given companies' business interests.

(g)RESPONSIBILITIES.—

(1)SECRETARY.—The Secretary shall exercise primary responsibility for the pilot program under subsection (b), including organizing and directing authorized activities with participating Federal Government organizations and internet ecosystem companies to achieve the objectives of the pilot program.

(2)NATIONAL CYBER DIRECTOR.—The National Cyber Director shall support prioritization and cross-agency coordination for the pilot program, including ensuring appropriate participation by participating agencies and the identification and prioritization of key private sector entities and initiatives for the pilot program.

(3)SECRETARY OF DEFENSE.—The Secretary of Defense shall provide support and resources to the pilot program, including the provision of technical and operational expertise drawn from appropriate and relevant officials and components of the Department of Defense, including the National Security Agency, United States Cyber Command, the Chief Information Officer, the Office of the Secretary of Defense, mili-

tary department Principal Cyber Advisors, and the Defense Advanced Research Projects Agency.

(h)PARTICIPATION OF OTHER FEDERAL GOVERNMENT COMPONENTS.—The Secretary may invite to participate in the pilot program required under subsection (b) the heads of such departments or agencies as the Secretary considers appropriate.

(i)Integration With Other Efforts.—THE SECRETARY SHALL ENSURE THAT THE PILOT PROGRAM REQUIRED UNDER SUBSECTION (B) MAKES USE OF, BUILDS ON, AND, AS APPROPRIATE, INTEGRATES WITH AND DOES NOT DUPLICATE OTHER EFFORTS OF THE DEPARTMENT AND THE DEPARTMENT OF DEFENSE RELATING TO CYBERSECURITY, INCLUDING THE FOLLOWING:

(1) The Joint Cyber Defense Collaborative of the Cybersecurity and Infrastructure Security Agency.

(2) The Cybersecurity Collaboration Center and Enduring Security Framework of the National Security Agency.

(j)RULES OF CONSTRUCTION.—

(1)LIMITATION ON GOVERNMENT ACCESS TO DATA.—Nothing in this section authorizes sharing of information, including information relating to customers of internet ecosystem companies or private individuals, from an internet ecosystem company to an agency, officer, or employee of the Federal Government unless otherwise authorized by another provision of law.

(2)STORED COMMUNICATIONS ACT.—Nothing in this section may be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed underchapter 121 of title 18(commonly known as the ''Stored Communications Act'').

(3)THIRD PARTY CUSTOMERS.–Nothing in this section may be construed to require a third party, such as a customer or managed service provider of an internet ecosystem company, to participate in the pilot program under subsection (b).

(k)ANNUAL BRIEFINGS.—

(1) IN GENERAL.—Not later than two years after December 27, 2023 and annually thereafter for 3 years, the Secretary, in coordination with the Secretary of Defense and the National Cyber Director, shall brief the appropriate committees of Congress on the progress of the pilot program required under subsection (b).

(2)ELEMENTS.—Each briefing required under paragraph (1) shall include the following:

(A) Recommendations for addressing relevant policy, budgetary, and legislative gaps to increase the effectiveness of the pilot program.

(B) Recommendations, such as providing liability protection, for increasing private sector participation in the pilot program.

(C) A description of the challenges encountered in carrying out the pilot program, including any concerns expressed by internet ecosystem companies regarding participation in the pilot program.

(D) The findings of the Secretary with respect to the feasibility and advisability of extending or expanding the pilot program.

(E) Such other matters as the Secretary considers appropriate.

(l)TERMINATION.—-The pilot program required under subsection (b) shall terminate on December 27, 2026.

§ 10808. CyberSentry program

(a) Definition of Industrial Control System.—In this section, the term ''industrial control system'' means an information system used to monitor and control industrial processes such as manufacturing, product handling, production, and distribution, including supervisory control and data acquisition (SCADA) systems used to monitor and control geographically dispersed assets, distributed control systems (DCSs), Human-Machine Interfaces (HMIs), and programmable logic controllers that control localized processes.

(b) ESTABLISHMENT.—There is in the Agency a program, to be known as ''CyberSentry'', to provide continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions, on request and subject to the consent of the owner or operator.

(c) ACTIVITIES.—The Director, through CyberSentry, shall—

(1) enter into strategic partnerships with critical infrastructure owners and operators that, in the determination of the Director and subject to the availability of resources, own or operate regionally or nationally significant industrial control systems that support national critical functions, in order to provide technical assistance in the form of continuous monitoring of industrial control systems and the information systems that support the systems and detection of cybersecurity risks to the industrial control systems and other cybersecurity services, as appropriate, based on and subject to the agreement and consent of the owner or operator;

(2) leverage sensitive or classified intelligence about cybersecurity risks regarding particular sectors, particular adversaries, and trends in tactics, techniques, and procedures to advise critical infrastructure owners and operators regarding mitigation measures and share information as appropriate;

(3) identify cybersecurity risks in the information technology and information systems that support industrial control systems that could be exploited by adversaries attempting to gain access to the industrial control systems, and work with owners and operators to remediate the vulnerabilities;

(4) produce aggregated, anonymized analytic products, based on threat hunting and continuous monitoring and detection activities and partnerships, with findings and recommendations that can be disseminated to critical infrastructure owners and operators; and

(5) support activities authorized in accordance with section 1501 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81, 135 Stat. 2020).

(d) PRIVACY REVIEW.—Not later than 180 days after December 27, 2021, the Privacy Officer of the Agency undersection 10304(d) of this titleshall review the policies, guidelines, and activities of CyberSentry for compliance with all applicable privacy laws, including the laws governing the acquisition, interception, retention, use, and disclosure of communities.

(e) REPORTS TO CONGRESS.—

(1) COMPLIANCE WITH PRIVACY LAWS.—Not later than 180 days after December 27, 2021, the Privacy Officer of the Agency undersection 10304(d) of this titleshall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report certifying compliance with all applicable privacy laws as referred to in paragraph (1) or identifying any instances of noncompliance with those privacy laws.

(2) IMPLEMENTATION.—Not later than December 27, 2022, the Director shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing and written report on implementation of this section.

(f) RULE OF CONSTRUCTION.—Nothing in this section may be construed to permit the Federal Government to gain access to information of a remote computing service provider to the public or an electronic service provider to the public, the disclosure of which is not permitted undersection 2702 of title 18.

(g) TERMINATION.—The authority to carry out a program under this section shall terminate on December 27, 2028.

§ 10809. Inventory of cryptographic systems; migration to post-quantum cryptography

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency''—

(A) means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

(B) does not include—

(i) the Government Accountability Office; or

(ii) the governments of the District of Columbia and of the territories (including possessions) of the United States, and their various subdivisions.

(2)CLASSICAL COMPUTER.—The term ''classical computer'' means a device that accepts digital data and manipulates the information based on a program or sequence of instructions for how data is to be processed and encodes information in binary bits that can either be 0s or 1s.

(3)DIRECTOR OF CISA.—The term ''Director of CISA''means the Director of the Cybersecurity and Infrastructure Security Agency.

(4)DIRECTOR OF NIST.—The term ''Director of NIST'' means the Director of the National Institute of Standards and Technology.

(5)DIRECTOR OF OMB.—The term ''Director of OMB'' means the Director of the Office of Management and Budget.

(6)INFORMATION TECHNOLOGY.—.-The term ''information technology'' has the meaning given the term insection 3502 of title 44.

(7)NATIONAL SECURITY SYSTEM.—The term ''national security system'' has the meaning given the term insection 3552 of title 44.

(8)POST-QUANTUM CRYPTOGRAPHY.—The term ''post-quantum cryptography'' means those cryptographic algorithms or methods that are assessed not to be specifically vulnerable to attack by either a quantum computer or classical computer.

(9)QUANTUM COMPUTER.—The term ''quantum computer'' means a computer that uses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations.

(b) INVENTORY.—

(1) ESTABLISHMENT.—Not later than 180 days after December 21, 2022, the Director of OMB, in coordination with the National Cyber Director and in consultation with the Director of CISA, shall issue guidance on the migration of information technology to post-quantum cryptography, which shall include at a minimum—

(A) a requirement for each agency to establish and maintain a current inventory of information technology in use by the agency

that is vulnerable to decryption by quantum computers, prioritized using the criteria described in subparagraph (B);

(B) criteria to allow agencies to prioritize their inventory efforts; and

(C) a description of the information required to be reported pursuant to subsection (c).

(2) ADDITIONAL CONTENT IN GUIDANCE.—In the guidance established by paragraph (1), the Director of OMB shall include, in addition to the requirements described in that paragraph—

(A) a description of information technology to be prioritized for migration to post-quantum cryptography; and

(B) a process for evaluating progress on migrating information technology to post-quantum cryptography, which shall be automated to the greatest extent practicable.

(3) PERIODIC UPDATES.—The Director of OMB shall update the guidance required under paragraph (1) as the Director of OMB determines necessary, in coordination with the National Cyber Director and in consultation with the Director of CISA.

(c) AGENCY REPORTS.—Not later than December 21, 2023, and on an ongoing basis thereafter, the head of each agency shall provide to the Director of OMB, the Director of CISA, and the National Cyber Director—

(1) the inventory described in subsection (b)(1); and

(2) any other information required to be reported under subsection (b)(1)(C).

(d) MIGRATION AND ASSESSMENT.—Not later than 1 year after the date on which the Director of NIST has issued post-quantum cryptography standards, the Director of OMB shall issue guidance requiring each agency to—

(1) prioritize information technology described under subsection (b)(2)(A) for migration to post-quantum cryptography; and

(2) develop a plan to migrate information technology of the agency to post-quantum cryptography consistent with the prioritization under paragraph (1).

(e) INTEROPERABILITY.—The Director of OMB shall ensure that the prioritizations made under subsection (d)(1) are assessed and coordinated to ensure interoperability.

(f) OFFICE OF MANAGEMENT AND BUDGET REPORTS.—

(1) Report on post-quantum crytography.—Not later than 15 months after December 21, 2022, the Director of OMB, in coordination with the National Cyber Director and in consultation with the Director of CISA, shall submit to the Committee on Homeland Security

and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a report on the following:

(A) A strategy to address the risk posed by the vulnerabilities of information technology of agencies to weakened encryption due to the potential and possible capability of a quantum computer to breach that encryption.

(B) An estimate of the amount of funding needed by agencies to secure the information technology described in subsection (b)(1)(A) from the risk posed by an adversary of the United States using a quantum computer to breach the encryption of the information technology.

(C) A description of Federal civilian executive branch coordination efforts led by the National Institute of Standards and Technology, including timelines, to develop standards for post-quantum cryptography, including any Federal Information Processing Standards developed underchapter 35 of title 44, as well as standards developed through voluntary, consensus standards bodies such as the International Organization for Standardization.

(2) REPORT ON MIGRATION TO POST-QUANTUM CRYPTOGRAPHY IN INFORMATION TECHNOLOGY.—Not later than 1 year after the date on which the Director of OMB issues guidance under subsection (d)(2), and thereafter until the date that is 5 years after the date on which post-quantum cryptographic standards are issued, the Director of OMB, in coordination with the National Cyber Director and in consultation with the Director of CISA, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives, with the report submitted pursuant tosection 3553(c) of title 44, a report on the progress of agencies in adopting post-quantum cryptography standards.

§10810. Competition relating to cybersecurity vulnerabilities

The Under Secretary for Science and Technology of the Department, in consultation with the Director, may establish an incentive-based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities (as that term is defined in section 10706 of this title) to information systems (as that term is defined in section 10701 of this title) and industrial control systems, including supervisory control and data acquisition systems.

§ 10811. Ransomware threat mitigation activities

(a) DEFINITIONS.—In this section:

(1) SECTION 10701 DEFINITIONS.—The terms ''Director'', ''information system'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 10701 of this title.

(2) SECTION 10761 DEFINITIONS—The terms ''covered cyber incident'', ''covered entity'', ''cyber incident'', and ''ransom payment'' have the meanings given those terms in section 10761 of this title.

(b) JOINT RANSOMWARE TASK FORCE.—

(1) ESTABLISHMENT.—The Director, in consultation with the National Cyber Director, the Attorney General, and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) COMPOSITION.—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary.

(3) RESPONSIBILITIES.— The Joint Ransomware Task Force, utilizing only existing authorities of each participating Federal agency, shall coordinate across the Federal Government the following activities:

(A) Prioritizing intelligence-driven operations to disrupt specific ransomware actors.

(B) Consulting with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Joint Ransomware Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, to facilitate—-j

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identification ofmetrics for success of the actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collecting, sharing, and analyzing ransomware trends to inform Federal actions.

(G) Creating after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the Joint Ransomware Task Force to mitigate the threat of ransomware attacks.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to provide any additional authority to any Federal agency.

(c) RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM

(1)ESTABLISHMENT.—Not later than March 15, 2023, the Director shall establish a ransomware vulnerability warning pilot program to leverage existing authorities and technology to specifically develop processes and procedures for, and to dedicate resources to, identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

(2)IDENTIFICATION OF VULNERABLE SYSTEMS.—The pilot program established under paragraph (1) shall—

(A) identify the most common security vulnerabilities utilized in ransomware attacks and mitigation techniques; and

(B) utilize existing authorities to identify information systems that contain the security vulnerabilities identified in subparagraph (A).

(3)ENTITY NOTIFICATION.—

(A)IDENTIFICATION.—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in paragraph (2), the Director may notify the owner of the information system.

(B)NO IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in paragraph (2), the Director may utilize the subpoena authority pursuant to section 10706 of this title to identify and notify the entity at risk pursuant to the procedures under that section.

(C)REQUIRED INFORMATION.—A notification made under subparagraph (A) shall include information on the identified security vulnerability and mitigation techniques.

(4)PRIORITIZATION OF NOTIFICATIONS.—To the extent practicable, the Director shall prioritize covered entities for identification and notification activities under the pilot program established under this subsection.

(5)LIMITATION ON PROCEDURES.—No procedure, notification, or other authorities utilized in the execution of the pilot program established under paragraph (1) shall require an owner or operator of a vulnerable information system to take any action as a result of a notice of a security vulnerability made pursuant to paragraph (3).

(6)Rule of construction.—Nothing in this subsection shall be construed to provide additional authorities to the Director to identify vulnerabilities or vulnerable systems.

(7)TERMINATION.—The pilot program established under paragraph (1) shall terminate on March 15, 2026.

§ 10812. National cybersecurity preparedness consortium

(a) DEFINITIONS.—In this section:

(1) COMMUNITY COLLEGE.—The term ''community college'' has the meaning given the term ''junior or community college'' in section 312 of the Higher Education Act of 1965 (20 U.S.C. 1058).

(2) CONSORTIUM.—The term ''consortium'' means a group primarily composed of nonprofit entities, including academic institutions, that develop, update, and deliver cybersecurity training and education in support of homeland security.

(3) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given the term in section 10701 of this title.

(4) HISPANIC-SERVING INSTITUTION.—The term ''Hispanic-serving institution'' has the meaning given the term in section 502 of the Higher Education Act of 1965 (20 U.S.C. 1101a).

(5) HISTORICALLY BLACK COLLEGE AND UNIVERSITY.—The term ''historically Black college and university'' has the meaning given the term ''part B institution'' in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

(6) INCIDENT.—The term ''incident'' has the meaning given the term in section 10701 of this title.

(7) MINORITY-SERVING INSTITUTION.—The term ''minority-serving institution'' means an institution of higher education described in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

(8) STATE.—The term ''State'' means a State, the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, the Northern Mariana Islands, and any possession of the United States.

(9) TRIBAL COLLEGES AND UNIVERSITIES.—The term ''Tribal Colleges and Universities'' has the meaning given the term in section 316 of the Higher Education Act of 1965 (20 U.S.C. 1059c).

(10) TRIBAL ORGANIZATION.—The term ''Tribal organization'' has the meaning given the term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304).

(b) IN GENERAL.—The Secretary may work with one or more consortia to support efforts to address cybersecurity risks and incidents.

(c) ASSISTANCE TO CARRY OUT SECRETARY'S RESPONSIBILITIES.—The Secretary may work with one or more consortia to carry out the Secretary's responsibility pursuant to section 10702(b)(1)(P) of this title to—-

(1) provide training and education to State, Tribal, and local first responders and officials specifically for preparing for and responding to cybersecurity risks and incidents, in accordance with applicable law;

(2) develop and update a curriculum utilizing existing training and educational programs and models, in accordance with section 10706 of this title for State, Tribal, and local first responders and officials, related to cybersecurity risks and incidents;

(3) provide technical assistance services, training, and educational programs to build and sustain capabilities in support of preparedness for and response to cybersecurity risks and incidents, including threats of acts of terrorism, in accordance with section 10706 of this title;

(4) conduct cross-sector cybersecurity training, education, and simulation exercises for entities, including State and local governments and Tribal organizations, critical infrastructure owners and operators, and private industry, to encourage community-wide coordination in defending against and responding to cybersecurity risks and incidents, in accordance with section 10707(c) of this title;

(5) help States, Tribal organizations, and communities develop cybersecurity information sharing programs, in accordance with section 10706 of this title, for the dissemination of homeland security information related to cybersecurity risks and incidents;

(6) help incorporate cybersecurity risk and incident prevention and response into existing State, Tribal, and local emergency plans, including continuity of operations plans; and

(7) assist State governments and Tribal organizations in developing cybersecurity plans.

(d) CONSIDERATIONS REGARDING SELECTION OF A CONSORTIUM.—In selecting a consortium with which to work under this section, the Secretary shall take into consideration the following:

(1) Prior experience conducting cybersecurity training, education, and exercises for State and local entities.

(2) Geographic diversity of the members of the consortium so as to maximize coverage of the different regions of the United States.

(3) The participation in the consortium of one or more historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, other minority-serving institutions, and community colleges that participate in the National Centers of Excellence in Cybersecurity program, as carried out by the Department.

(e) METRICS.—If the Secretary works with a consortium under subsection (b), the Secretary shall measure the effectiveness of the activities undertaken by the consortium under this section.

(f) OUTREACH.—The Secretary shall conduct outreach to universities and colleges, including, in particular, outreach to historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, other minority-serving institutions, and community colleges, regarding opportunities to support efforts to address cybersecurity risks and incidents, by working with the Secretary under subsection (b).

(g) RULE OF CONSTRUCTION.—Nothing in this section may be construed to authorize a consortium to control or direct any law enforcement agency in the exercise of the duties of the law enforcement agency.

Part B—Other Areas

§ 10821. Enhancement of emergency services

(a) COLLECTION OF DATA.—The Secretary, acting through the National Cybersecurity and Communications Integration Center, in coordination with appropriate Federal entities and the Assistant Director for Emergency Communications, shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers in that State.

(b) ANALYSIS OF DATA.—Not later than December 18, 2016, the Secretary, acting through the Director of the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Assistant Director for Emergency Communications, and in consultation with the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology, shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations on security and resilience measures for any information system or network used by State emergency response providers.

(c) BEST PRACTICES.—

(1) IN GENERAL.—Using the results of the integration and analysis conducted under subsection (b), and any other relevant information, the Director of the National Institute of Standards and Technology shall, on an ongoing basis, facilitate and support the development of methods for reducing cybersecurity risks to emergency response pro-

viders using the process described in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)).

(2) REPORT.—The Director of the National Institute of Standards and Technology shall submit to Congress a report on the result of the activities of the Director under paragraph (1), including any methods developed by the Director under paragraph (1), and shall make the report publicly available on the website of the National Institute of Standards and Technology.

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to—

(1) require a State to report data under subsection (a); or

(2) require a non-Federal entity (as defined in section 10801 of this title) to—

(A) adopt a recommended measure developed under subsection (b); or

(B) follow the result of the activities carried out under subsection (c), including any methods developed under subsection (c).

§ 10822. Improving cybersecurity in the health care industry

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Health, Education, Labor, and Pensions, the Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Energy and Commerce, the Committee on Homeland Security, and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) BUSINESS ASSOCIATE.—The term ''business associate'' has the meaning given the term in section 160.103 of title 45, Code of Federal Regulations (as in effect on December 17, 2015).

(3) COVERED ENTITY.—The term ''covered entity'' has the meaning given the term in section 160.103 of title 45, Code of Federal Regulations (as in effect on December 17, 2015).

(4) CYBERSECURITY THREAT; CYBER THREAT INDICATOR; DEFENSIVE MEASURE; FEDERAL ENTITY.—The terms ''cybersecurity threat'', ''cyber threat indicator'', ''defensive measure'', and ''Federal entity'' have the meanings given the terms in section 10781 of this title.

(5) HEALTH CARE CLEARINGHOUSE; HEALTH CARE PROVIDER; HEALTH PLAN.—The terms ''health care clearinghouse'', ''health care provider'', and ''health plan'' have the meanings given the terms in sec-

tion 160.103 of title 45, Code of Federal Regulations (as in effect on December 17, 2015).

(6) HEALTH CARE INDUSTRY STAKEHOLDER.—The term ''health care industry stakeholder'' means any—

(A) health plan, health care clearinghouse, or health care provider;

(B) advocate for patients or consumers;

(C) pharmacist;

(D) developer or vendor of health information technology;

(E) laboratory;

(F) pharmaceutical or medical device manufacturer; or

(G) additional stakeholder the Secretary determines necessary for purposes of subsection (b)(1), (c)(1), (c)(3), or (d)(1).

(7) NON-FEDERAL ENTITY; PRIVATE ENTITY.—The terms ''non-Federal entity'' and ''private entity'' have the meanings given the terms in section 10781 of this title.

(b) REPORT.—

(1) IN GENERAL.—Not later than December 18, 2016, the Secretary of Health and Human Services shall submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives a report on the preparedness of the Department of Health and Human Services and health care industry stakeholders in responding to cybersecurity threats.

(2) CONTENTS OF REPORT.—With respect to the internal response of the Department of Health and Human Services to emerging cybersecurity threats, the report under paragraph (1) shall include—

(A) a clear statement of the official in the Department of Health and Human Services to be responsible for leading and coordinating efforts of the Department of Health and Human Services regarding cybersecurity threats in the health care industry; and

(B) a plan from each relevant operating division and subdivision of the Department of Health and Human Services on how the division or subdivision will address cybersecurity threats in the health care industry, including a clear delineation of how the division or subdivision will divide responsibility among the personnel of the division or subdivision and communicate with other divisions and subdivisions regarding efforts to address the threats.

(c) HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE.—

(1) IN GENERAL.—The Secretary of Health and Human Services, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary of Health and Human Services determines appropriate to establish a task force to—

(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats in their respective industries;

(B) analyze challenges and barriers private entities (excluding any State, tribal, or local government) in the health care industry face securing themselves against cyberattacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary of Health and Human Services with information to disseminate to health care industry stakeholders of all sizes for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for implementing Subchapter IV of this chapter, so that the Federal Government and health care industry stakeholders may in real time, share actionable cyber threat indicators and defensive measures; and

(F) report to the appropriate congressional committees on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

(2) TERMINATION.—The task force established under this subsection shall terminate 1 year after the date on which the task force is established.

(3) DISSEMINATION.—Not later than 60 days after the termination of the task force established under this subsection, the Secretary of Health and Human Services shall disseminate the information described in paragraph (1)(D) to health care industry stakeholders in accordance with paragraph (1)(D).

(d) ALIGNING HEALTH CARE INDUSTRY SECURITY APPROACHES.—

(1) IN GENERAL.—The Secretary of Health and Human Services shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary of Health and Human Services determines appropriate, a common set of voluntary, consensus-

based, and industry-led guidelines, best practices, methodologies, procedures, and processes that—

(A) serve as a resource for cost-effectively reducing cybersecurity risks for a range of health care organizations;

(B) support voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;

(C) are consistent with—

(i) the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)(15));

(ii) the security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note); and

(iii) the Health Information Technology for Economic and Clinical Health Act (Public Law 111–5, div. A, title XIII, div. B, title IV, 123 Stat. 226, 467), and the amendments made by the Act; and

(D) are updated on a regular basis and are applicable to a range of health care organizations.

(2) LIMITATION.—Nothing in this subsection shall be interpreted as granting the Secretary of Health and Human Services authority to—

(A) provide for audits to ensure that health care organizations are in compliance with this subsection; or

(B) mandate, direct, or condition the award of any Federal grant, contract, or purchase on compliance with this subsection.

(3) NO LIABILITY FOR NONPARTICIPATION.—Nothing in this section shall be construed to subject a health care industry stakeholder to liability for choosing not to engage in the voluntary activities authorized, or guidelines developed, under this subsection.

(e) INCORPORATING ONGOING ACTIVITIES.—In carrying out the activities under this section, the Secretary of Health and Human Services may incorporate activities that are ongoing as of December 17, 2015, and that are consistent with the objectives of this section.

(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit the antitrust exemption under section 10783(e) of this title or the protection from liability under section 10785 of this title.

§ 10823. K–12 education cybersecurity initiative

(a) DEFINITIONS.—In this section

(1) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given the term in section 10701 of this title.

(2)DIRECTOR.—The term ''Director'' means the Director of Cybersecurity and Infrastructure Security.

(3)INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term insection 3502 of title 44.

(4) K12EDUCATIONAL INSTITUTION.—The term ''K–12 educational institution'' means an elementary school or a secondary school, as those terms are defined in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(b) CYBERSECURITY RECOMMENDATIONS.—Not later than 60 days after the completion of the study required under section 3(b)(1) of the K–12 Cybersecurity Act of 2021 (Public Law 117–47, 135 Stat. 397), the Director, in accordance with subsection (f)(1), shall develop recommendations that include cybersecurity guidelines designed to assist K–12 educational institutions in facing the cybersecurity risks described in section 3(b)(1) of that Act, using the findings of the study.

(c) ONLINE TRAINING TOOLKIT.—Not later than 120 days after the completion of the development of the recommendations required under subsection (b), the Director shall develop an online training toolkit designed for officials at K–12 educational institutions to—

(1) educate the officials about the cybersecurity recommendations developed under subsection (b); and

(2) provide strategies for the officials to implement the recommendations developed under subsection (b).

(d) PUBLIC AVAILABILITY.—The Director shall make available on the website of the Department with other information relating to school safety the following:

(1) The findings of the study conducted under section 3(b)(1) of the K–12 Cybersecurity Act of 2021 (Public Law 117–47, 135 Stat. 397).

(2) The cybersecurity recommendations developed under subsection (b).

(3) The online training toolkit developed under subsection (c).

(e) VOLUNTARY USE.—The use of the cybersecurity recommendations developed under subsection (b) by K–12 educational institutions shall be voluntary.

(f)CONSULTATION.—

(1)IN GENERAL.—In the course of the development of the recommendations required under subsection (b), the Director shall consult with individuals and entities focused on cybersecurity and education, as appropriate, including—

(A) teachers;

(B) school administrators;

(C) Federal agencies;

(D) non-Federal cybersecurity entities with experience in education issues; and

(E) private sector organizations.

(2)INAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of title 5 shall not apply to any consultation under paragraph (1).

§ 10824. Federal Clearinghouse on School Safety Evidence-Based Practices

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Secretary, in coordination with the Secretary of Education, the Attorney General, and the Secretary of Health and Human Services, shall establish a Federal Clearinghouse on School Safety Evidence-Based Practices (in this section referred to as the ''Clearinghouse'') in the Department.

(2) PURPOSE.—The Clearinghouse shall serve as a Federal resource to identify and publish online through SchoolSafety.gov, or any successor website, evidence-based practices and recommendations to improve school safety for use by State and local educational agencies, institutions of higher education, State and local law enforcement agencies, health professionals, and the general public.

(3) PERSONNEL.—

(A) ASSIGNMENTS.—The Clearinghouse shall be assigned such personnel and resources as the Secretary considers appropriate to carry out this section.

(B) DETAILEES.— The Secretary of Education, the Attorney General, and the Secretary of Health and Human Services may detail personnel to the Clearinghouse.

(4) EXEMPTIONS.—

(A) CHAPTER 35 OF TITLE 44.— Chapter 35 of title 44 shall not apply to any rulemaking or information collection required under this section.

(B) CHAPTER 10 OF TITLE 5.—The Federal Advisory Committee Act (5 U.S.C. App.)Chapter 10 of title 5 shall not apply for the purposes of carrying out this section.

(b) CLEARINGHOUSE CONTENTS.—

(1) CONSULTATION.— In identifying the evidence-based practices and recommendations for the Clearinghouse, the Secretary shall—

(A) consult with appropriate Federal, State, local, Tribal, private sector, and nongovernmental organizations, including civil rights and disability rights organizations; and

(B) consult with the Secretary of Education to ensure that evidence-based practices published by the Clearinghouse are aligned with evidence-based practices to support a positive and safe learning environment for all students.

(2) CRITERIA FOR EVIDENCE-BASED PRACTICES AND RECOMMENDATIONS.— The evidence-based practices and recommendations of the Clearinghouse shall—

(A) include comprehensive evidence-based school safety measures;

(B) include the evidence or research rationale supporting the determination of the Clearinghouse that the evidence-based practice or recommendation under subparagraph (A) has been shown to have a significant effect on improving the health, safety, and welfare of persons in school settings, including—

(i) relevant research that is evidence-based, as defined insection 9101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801), supporting the evidence-based practice or recommendation;

(ii) findings and data from previous Federal or State commissions recommending improvements to the safety posture of a school; or

(iii) other supportive evidence or findings relied on by the Clearinghouse in determining evidence-based practices and recommendations, as determined in consultation with the officers described in subsection (a)(3)(B);

(C) include information on Federal programs for which implementation of each evidence-based practice or recommendation is an eligible use for the program;

(D) be consistent with Federal civil rights laws, including title II of the Americans with Disabilities Act of 1990 (42 U.S.C. 12131 et seq.), the Rehabilitation Act of 1973 (29 U.S.C. 701 et seq.), and title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.); and

(E) include options for developmentally appropriate recommendations for use in educational settings with respect to children's ages and physical, social, sensory, and emotionally developmental statuses.

(3) PAST RECOMMENDATIONS.—The Clearinghouse shall present, as determined in consultation with the officers described in subsection (a)(3)(B), Federal, State, local, Tribal, private sector, and nongovernmental organization issued best practices and recommendations and

identify any best practice or recommendation of the Clearinghouse that was previously issued by any organization or commission.

(c) ASSISTANCE AND TRAINING.—The Secretary may produce and publish materials on the Clearinghouse to assist and train educational agencies and law enforcement agencies on the implementation of the evidence-based practices and recommendations.

(d) CONTINUOUS IMPROVEMENT.— The Secretary shall—-

(1) collect for the purpose of continuous improvement of the Clearinghouse—-

(A) Clearinghouse data analytics;

(B) user feedback on the implementation of resources, evidence-based practices, and recommendations identified by the Clearinghouse; and

(C) any evaluations conducted on implementation of the evidence-based practices and recommendations of the Clearinghouse; and

(2) in coordination with the Secretary of Education, the Secretary of Health and Human Services, and the Attorney General—-

(A) regularly assess and identify Clearinghouse evidence-based practices and recommendations for which there are no resources available through Federal Government programs for implementation; and

(B) establish an external advisory board, which shall be comprised of appropriate State, local, Tribal, private sector, and non-governmental organizations, including organizations representing parents of elementary and secondary school students, representativesfrom civil rights organizations, representatives of disability rights organizations, representatives of educators, representatives of law enforcement, and nonprofit school safety and security organizations, to—-

(i) provide feedback on the implementation of evidence-based practices and recommendations of the Clearinghouse; and

(ii) propose additional recommendations for evidence-based practices for inclusion in the Clearinghouse that meet the requirements described in subsection (b)(2)(B).

(e) PARENTAL ASSISTANCE.—The Clearinghouse shall produce materials in accessible formats to assist parents and legal guardians of students in identifying relevant Clearinghouse resources related to supporting the implementation of Clearinghouse evidence-based practices and recommendations.

(f) NOTIFICATION.—

(1) BY SECRETARY OF EDUCATION.— The Secretary of Education shall provide written notification of the publication of the Clearinghouse to—

(A) every State and local educational agency; and

(B) other Department of Education partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Secretary of Education.

(2)By Secretary.—The Secretary shall provide written notification of the publication of the Clearinghouse to—

(A) every State homeland security advisor;

(B) every State department of homeland security; and

(C) other Department partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Secretary.

(3)By secretary of health and human services.—The Secretary of Health and Human Services shall provide written notification of the publication of the Clearinghouse to—-

(A) every State department of public health; and

(B) other Department of Health and Human Services partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Secretary of Health and Human Services.

(4)By Attorney General.—The Attorney General shall provide written notification of the publication of the Clearinghouse to—

(A) every State department of justice; and

(B) other Department of Justice partners in the implementation of the evidence-based practices and recommendations of the Clearinghouse, as determined appropriate by the Attorney General.

(g) GRANT PROGRAM REVIEW.—

(1) FEDERAL GRANTS AND RESOURCES.— Not later June 25, 2023, the Clearinghouse or the external advisory board shall—

(A) review grant programs and identify any grant program that may be used to implement evidence-based practices and recommendations of the Clearinghouse;

(B) identify any evidence-based practices and recommendations of the Clearinghouse for which there is not a Federal grant program that may be used for the purposes of implementing the evidence-based practice or recommendation as applicable to the agency; and

(C) periodically report any findings under subparagraph (B) to the appropriate committees of Congress.

(2) STATE GRANTS AND RESOURCES.—The Clearinghouse shall, to the extent practicable, identify, for each State—

(A) each agency responsible for school safety in the State, or any State that does not have an agency designated;

(B) any grant program that may be used for the purposes of implementing evidence-based practices and recommendations of the Clearinghouse; and

(C) any resources other than grant programs that may be used to assist in implementation of evidence-based practices and recommendations of the Clearinghouse.

(h) RULES OF CONSTRUCTION.—

(1) WAIVER OF REQUIREMENTS.—Nothing in this section shall be construed to create, satisfy, or waive any requirement under—

(A) title II of the Americans with Disabilities Act of 1990 (42 U.S.C. 12131 et seq.);

(B) the Rehabilitation Act of 1973 (29 U.S.C. 701 et seq.);

(C) title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.);

(D) title IX of the Education Amendments of 1972 (20 U.S.C. 1681 et seq.); or

(E) the Age Discrimination Act of 1975 (42 U.S.C. 6101 et seq.).

(2) PROHIBITION OF FEDERALLY DEVELOPED, MANDATED, OR ENDORSED CURRICULUM.—Nothing in this section shall be construed to authorize any officer or employee of the Federal Government to engage in an activity otherwise prohibited under section 103(b) of the Department of Education Organization Act (20 U.S.C. 3403(b)).

§ 10825. Report and briefing on school and daycare protection

(a) DEFINITIONS.—In this section, the terms ''early childhood education program'', ''elementary school'', and ''secondary school'' have the meanings given those terms in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(b) REPORTS TO CONGRESS.—Not later than 180 days after December 23, 2022, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report regarding the following:

(1) The Department's activities, policies, and plans to enhance the security of early childhood education programs, elementary schools, and secondary schools during the preceding year that includes information on the Department's activities through the Federal School Safety Clearinghouse.

(2) Information on all structures or efforts in the Department intended to bolster coordination among departmental components and offices involved in carrying out paragraph (1) and with respect to each structure or effort specificity on which components or offices are involved and which component or office leads the structure or effort.

(3) A detailed description of the measures used to ensure privacy rights, civil rights, and civil liberties protections in carrying out these activities.

(c) BRIEFINGS.—Not later than 30 days after the submission of each report required under subsection (b), the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing regarding the report and the status of efforts to carry out plans included in the report for the preceding year.

Subchapter VII—Secure Handling of Ammonium Nitrate

§ 10841. Definitions

In this subchapter:

(1) AMMONIUM NITRATE.—The term ''ammonium nitrate'' means—

(A) solid ammonium nitrate that is chiefly the ammonium salt of nitric acid and contains not less than 33 percent nitrogen by weight; and

(B) a mixture containing a percentage of ammonium nitrate that is equal to or greater than the percentage determined by the Secretary under section 10842(b) of this title.

(2) AMMONIUM NITRATE FACILITY.—The term ''ammonium nitrate facility'' means an entity that produces, sells or otherwise transfers ownership of, or provides application services for, ammonium nitrate.

(3) AMMONIUM NITRATE PURCHASER.—The term ''ammonium nitrate purchaser'' means a person who purchases ammonium nitrate from an ammonium nitrate facility.

§ 10842. Regulation of the sale and transfer of ammonium nitrate

(a) IN GENERAL.—The Secretary shall regulate the sale and transfer of ammonium nitrate by an ammonium nitrate facility in accordance with this subchapter to prevent the misappropriation or use of ammonium nitrate in

an act of terrorism. The regulations shall be carried out by the Cybersecurity and Infrastructure Security Agency.

(b) AMMONIUM NITRATE MIXTURES.—The Secretary, in consultation with the heads of appropriate Federal departments and agencies (including the Secretary of Agriculture), shall, after notice and an opportunity for comment, establish a threshold percentage for ammonium nitrate in a substance.

(c) REGISTRATION OF OWNERS OF AMMONIUM NITRATE FACILITIES.—

(1) PROCESS.—The Secretary shall establish a process by which a person that—

(A) owns an ammonium nitrate facility is required to register with the Department; and

(B) registers under subparagraph (A) is issued a registration number for purposes of this subchapter.

(2) INFORMATION.—A person applying to register under paragraph (1) shall submit to the Secretary—

(A) the name, address, and telephone number of each ammonium nitrate facility owned by that person;

(B) the name of the person designated by that person as the point of contact for each facility, for purposes of this subchapter; and

(C) other information the Secretary determines is appropriate.

(d) REGISTRATION OF AMMONIUM NITRATE PURCHASERS.—

(1) PROCESS.—The Secretary shall establish a process by which a person that—

(A) intends to be an ammonium nitrate purchaser is required to register with the Department; and

(B) registers under subparagraph (A) is issued a registration number for purposes of this subchapter.

(2) INFORMATION.—A person applying to register under paragraph (1) as an ammonium nitrate purchaser shall submit to the Secretary—

(A) the name, address, and telephone number of the applicant; and

(B) the intended use of ammonium nitrate to be purchased by the applicant.

(e) RECORDS.—

(1) MAINTENANCE OF RECORDS.—The owner of an ammonium nitrate facility shall—

(A) maintain a record of each sale or transfer of ammonium nitrate during the 2-year period beginning on the date of that sale or transfer; and

(B) include in the record the information described in paragraph (2).

(2) SPECIFIC INFORMATION REQUIRED.—For each sale or transfer of ammonium nitrate, the owner of an ammonium nitrate facility shall—

(A) record the name, address, telephone number, and registration number issued under subsection (c) or (d) of each person that purchases ammonium nitrate, in a manner prescribed by the Secretary;

(B) if applicable, record the name, address, and telephone number of an agent acting on behalf of the person described in subparagraph (A), at the point of sale;

(C) record the date and quantity of ammonium nitrate sold or transferred; and

(D) verify the identity of the persons described in subparagraphs (A) and (B), as applicable, in accordance with a procedure established by the Secretary.

(3) PROTECTION OF INFORMATION.—In maintaining records under paragraph (1), the owner of an ammonium nitrate facility shall take reasonable actions to ensure the protection of the information included in the records.

(f) EXEMPTION FOR EXPLOSIVE PURPOSES.—The Secretary may exempt from this subchapter a person producing, selling, or purchasing ammonium nitrate exclusively for use in the production of an explosive under a license or permit issued under chapter 40 of title 18.

(g) CONSULTATION.—In carrying out this section, the Secretary shall consult with the Secretary of Agriculture, States, and appropriate private-sector entities, to ensure that the access of agricultural producers to ammonium nitrate is not unduly burdened.

(h) DATA CONFIDENTIALITY.—

(1) IN GENERAL.—Notwithstanding section 552 of title 5 or the USA PATRIOT Act (Public Law 107–56, 115 Stat. 272), and except as provided in paragraph (2), the Secretary may not disclose to any person any information obtained under this subchapter.

(2) EXCEPTION.—The Secretary may disclose information obtained by the Secretary under this subchapter to—

(A) an officer or employee of the United States, or a person that has entered into a contract with the United States, that has a need to know the information to perform the duties of the officer, employee, or person; or

(B) a State agency under section 10844 of this title, under appropriate arrangements to ensure the protection of the information.

(i) REGISTRATION PROCEDURES AND CHECK OF TERRORIST SCREENING DATABASE.—

(1) REGISTRATION PROCEDURES.—

(A) IN GENERAL.—The Secretary shall establish procedures to efficiently receive applications for registration numbers under this subchapter, conduct the checks required under paragraph (2), and promptly issue or deny a registration number.

(B) INITIAL 6-MONTH REGISTRATION PERIOD.—The Secretary shall take steps to maximize the number of registration applications that are submitted and processed during the 6-month period described in section 10846(e) of this title.

(2) CHECK OF TERRORIST SCREENING DATABASE.—

(A) CHECK REQUIRED.—The Secretary shall conduct a check of appropriate identifying information of a person seeking to register with the Department under subsection (c) or (d) against identifying information that appears in the terrorist screening database of the Department.

(B) AUTHORITY TO DENY REGISTRATION NUMBER.—If the identifying information of a person seeking to register with the Department under subsection (c) or (d) appears in the terrorist screening database of the Department, the Secretary may deny issuance of a registration number under this subchapter.

(3) EXPEDITED REVIEW OF APPLICATIONS.—

(A) IN GENERAL.—Following the 6-month period described in section 10846(e) of this title, the Secretary shall, to the extent practicable, issue or deny registration numbers under this subchapter not later than 72 hours after the time the Secretary receives a complete registration application, unless the Secretary determines, in the interest of national security, that additional time is necessary to review an application.

(B) NOTICE OF APPLICATION STATUS.—In all cases, the Secretary shall notify a person seeking to register with the Department under subsection (c) or (d) of the status of the application of that person not later than 72 hours after the time the Secretary receives a complete registration application.

(4) EXPEDITED APPEALS PROCESS.—

(A) REQUIREMENT.—

(i) ESTABLISHMENT.—The Secretary shall establish an expedited appeals process for persons denied a registration number under this subchapter.

(ii) TIME FOR RESOLVING APPEALS.—The Secretary shall, to the extent practicable, resolve appeals not later than 72 hours after receiving a complete request for appeal unless the Secretary determines, in the interest of national security, that additional time is necessary to resolve an appeal.

(B) CONSULTATION.—The Secretary, in developing the appeals process under subparagraph (A), shall consult with appropriate stakeholders.

(C) GUIDANCE.—The Secretary shall provide guidance regarding the procedures and information required for an appeal under subparagraph (A) to any person denied a registration number under this subchapter.

(5) RESTRICTIONS ON USE AND MAINTENANCE OF INFORMATION.—

(A) IN GENERAL.—Information constituting grounds for denial of a registration number under this section shall be maintained confidentially by the Secretary and may be used only for making determinations under this section.

(B) SHARING OF INFORMATION.—Notwithstanding this subchapter, the Secretary may share information with Federal, State, local, and tribal law enforcement agencies, as appropriate.

(6) REGISTRATION INFORMATION.—

(A) AUTHORITY TO REQUIRE INFORMATION.—The Secretary may require a person applying for a registration number under this subchapter to submit information necessary to carry out the requirements of this section.

(B) REQUIREMENT TO UPDATE INFORMATION.—The Secretary may require persons issued a registration under this subchapter to update registration information submitted to the Secretary under this subchapter, as appropriate.

(7) RECHECKS AGAINST TERRORIST SCREENING DATABASE.—

(A) IN GENERAL.—The Secretary shall, as appropriate, recheck persons provided a registration number pursuant to this subchapter against the terrorist screening database of the Department, and may revoke the registration number if the Secretary determines the person may pose a threat to national security.

(B) NOTICE OF REVOCATION.—The Secretary shall, as appropriate, provide prior notice to a person whose registration number

is revoked under this section, and the person shall have an opportunity to appeal, as provided in paragraph (4).

§ 10843. Inspection and auditing of records

The Secretary shall establish a process for the periodic inspection and auditing of the records maintained by owners of ammonium nitrate facilities for the purpose of monitoring compliance with this subchapter or for the purpose of deterring or preventing the misappropriation or use of ammonium nitrate in an act of terrorism.

§ 10844. Administrative provisions

(a) COOPERATIVE AGREEMENTS.—The Secretary—

(1) may enter into a cooperative agreement with the Secretary of Agriculture, or the head of any State department of agriculture or its designee involved in agricultural regulation, in consultation with the State agency responsible for homeland security, to carry out this subchapter; and

(2) wherever possible, shall seek to cooperate with State agencies or their designees that oversee ammonium nitrate facility operations when seeking cooperative agreements to implement the registration and enforcement provisions of this subchapter.

(b) DELEGATION.—

(1) AUTHORITY.—The Secretary may delegate to a State the authority to assist the Secretary in the administration and enforcement of this subchapter.

(2) DELEGATION REQUIRED.—At the request of a Governor of a State, the Secretary shall delegate to that State the authority to carry out functions under sections 10842 and 10843 of this title, if the Secretary determines that the State is capable of satisfactorily carrying out the functions.

(3) FUNDING.—Subject to the availability of appropriations, if the Secretary delegates functions to a State under this subsection, the Secretary shall provide to that State sufficient funds to carry out the delegated functions.

(c) PROVISION OF GUIDANCE AND NOTIFICATION MATERIALS TO AMMONIUM NITRATE FACILITIES.—

(1) GUIDANCE.—The Secretary shall make available to each owner of an ammonium nitrate facility registered under section 10842(c) of this title guidance on—

(A) the identification of suspicious ammonium nitrate purchases or transfers or attempted purchases or transfers;

(B) the appropriate course of action to be taken by the ammonium nitrate facility owner with respect to such a purchase or transfer or attempted purchase or transfer, including—

(i) exercising the right of the owner of the ammonium nitrate facility to decline sale of ammonium nitrate; and

(ii) notifying appropriate law enforcement entities; and

(C) additional subjects determined appropriate to prevent the misappropriation or use of ammonium nitrate in an act of terrorism.

(2) USE OF MATERIALS AND PROGRAMS.—In providing guidance under this subsection, the Secretary shall, to the extent practicable, leverage relevant materials and programs.

(3) NOTIFICATION MATERIALS.—

(A) IN GENERAL.—The Secretary shall make available materials suitable for posting at locations where ammonium nitrate is sold.

(B) DESIGN.—Materials made available under subparagraph (A) shall be designed to notify prospective ammonium nitrate purchasers of—

(i) the record-keeping requirements under section 10842 of this title; and

(ii) the penalties for violating the requirements.

§ 10845. Theft reporting requirement

A person who is required to comply with section 10842(e) of this title who has knowledge of the theft or unexplained loss of ammonium nitrate shall report the theft or loss to the appropriate Federal law enforcement authorities not later than 1 calendar day after the date on which the person becomes aware of the theft or loss. On receipt of the report, the relevant Federal authorities shall inform State, local, and tribal law enforcement entities, as appropriate.

§ 10846. Prohibitions and penalty

(a) PROHIBITIONS.—

(1) TAKING POSSESSION.—A person may not purchase ammonium nitrate from an ammonium nitrate facility unless the person is registered under subsection (c) or (d) of section 10842 of this title or is an agent of a person registered under subsection (c) or (d) of section 10842.

(2) TRANSFERRING POSSESSION.—An owner of an ammonium nitrate facility shall not transfer possession of ammonium nitrate from the ammonium nitrate facility to an ammonium nitrate purchaser who is not registered under subsection (c) or (d) of section 10842 of this title, or to an agent acting on behalf of an ammonium nitrate pur-

chaser when the purchaser is not registered under subsection (c) or (d) of section 10842.

(3) OTHER PROHIBITIONS.—A person may not—

(A) purchase ammonium nitrate without a registration number required under subsection (c) or (d) of section 10842 of this title;

(B) own or operate an ammonium nitrate facility without a registration number required under section 10842(c) of this title; or

(C) fail to comply with a requirement or violate another prohibition under this subchapter.

(b) CIVIL PENALTY.—A person that violates this subchapter may be assessed a civil penalty by the Secretary of not more than $50,000 per violation.

(c) PENALTY CONSIDERATIONS.—In determining the amount of a civil penalty under this section, the Secretary shall consider—

(1) the nature and circumstances of the violation;

(2) with respect to the person who commits the violation, any history of prior violations, the ability to pay the penalty, and any effect the penalty is likely to have on the ability of the person to do business; and

(3) any other matter that the Secretary determines that justice requires.

(d) NOTICE AND OPPORTUNITY FOR A HEARING.—A civil penalty may not be assessed under this subchapter unless the person liable for the penalty has been given notice and an opportunity for a hearing on the violation for which the penalty is to be assessed in the county, parish, or incorporated city of residence of that person.

(e) DELAY IN APPLICATION OF PROHIBITION.—Paragraphs (1) and (2) of subsection (a) shall apply on and after the date that is 6 months after the date that the Secretary issues a final rule implementing this subchapter.

§ 10847. Protection from civil liability

(a) IN GENERAL.—Notwithstanding another law, an owner of an ammonium nitrate facility that in good faith refuses to sell or transfer ammonium nitrate to a person, or that in good faith discloses to the Department or to appropriate law enforcement authorities an actual or attempted purchase or transfer of ammonium nitrate, based upon a reasonable belief that the person seeking purchase or transfer of ammonium nitrate may use the ammonium nitrate to create an explosive device to be employed in an act of terrorism (as defined in section 3077 of title 18), or to use ammonium nitrate for any other unlawful purpose, shall not be liable in any civil action relating to that refusal to sell ammonium nitrate or that disclosure.

(b) REASONABLE BELIEF.—A reasonable belief that an individual may use ammonium nitrate to create an explosive device to be employed in an act of terrorism under subsection (a) may not solely be based on the individual's race, sex, national origin, creed, religion, status as a veteran, or status as a member of the armed forces of the United States.

§ 10848. Preemption of other laws

(a) OTHER FEDERAL REGULATIONS.—Except as provided in section 10847 of this title, nothing in this subchapter affects a regulation issued by an agency other than an agency of the Department.

(b) STATE LAW.—Subject to section 10847 of this title, this subchapter preempts the laws of a State to the extent that the laws are inconsistent with this subchapter, except that this subchapter shall not preempt any State law that provides additional protection against the acquisition of ammonium nitrate by terrorists or the use of ammonium nitrate in explosives in acts of terrorism or for other illicit purposes, as determined by the Secretary.

Subchapter VIII—Chemical Facilities

§ 10861. Definitions

In this subchapter:

(1) CFATS REGULATION.—The term ''CFATS regulation'' means—

(A) an existing CFATS regulation; and

(B) any regulation or amendment to an existing CFATS regulation issued pursuant to the authority under section 10867 of this title.

(2) CHEMICAL FACILITY OF INTEREST.—The term ''chemical facility of interest'' means a facility that—

(A) holds, or that the Secretary has a reasonable basis to believe holds, a chemical of interest, as designated under Appendix A to part 27 of title 6, Code of Federal Regulations, or any successor to the Appendix, at a threshold quantity set pursuant to relevant risk-related security principles; and

(B) is not an excluded facility.

(3) COVERED CHEMICAL FACILITY.—The term ''covered chemical facility'' means a facility that—

(A) the Secretary—

(i) identifies as a chemical facility of interest; and

(ii) based on review of the facility's Top-Screen, determines meets the risk criteria developed under section 10862(e)(2)(B) of this title; and

(B) is not an excluded facility.

(4) EXCLUDED FACILITY.—The term ''excluded facility'' means—

(A) a facility regulated under the Maritime Transportation Security Act of 2002 (Public Law 107–295; 116 Stat. 2064);

(B) a public water system, as that term is defined in section 1401 of the Public Health Service Act (42 U.S.C. 300f);

(C) a treatment works, as that term is defined in section 212 of the Federal Water Pollution Control Act (33 U.S.C. 1292);

(D) a facility owned or operated by the Department of Defense or the Department of Energy; or

(E) a facility subject to regulation by the Nuclear Regulatory Commission, or by a State that has entered into an agreement with the Nuclear Regulatory Commission under section 274(b) of the Atomic Energy Act of 1954 (42 U.S.C. 2021(b)) to protect against unauthorized access of any material, activity, or structure licensed by the Nuclear Regulatory Commission.

(5) EXISTING CFATS REGULATION.—The term ''existing CFATS regulation'' means—

(A) a regulation promulgated under section 550 of the Department of Homeland Security Appropriations Act, 2007 (Public Law 109–295) that was in effect on December 17, 2014; and

(B) a Federal Register notice or other published guidance relating to section 550 of the Department of Homeland Security Appropriations Act, 2007 (Public Law 109–295) that was in effect on December 17, 2014.

(6) EXPEDITED APPROVAL FACILITY.—The term ''expedited approval facility'' means a covered chemical facility for which the owner or operator elects to submit a site security plan in accordance with section 10862(c)(4) of this title.

(7) FACIALLY DEFICIENT.—The term ''facially deficient'', relating to a site security plan, means a site security plan that does not support a certification that the security measures in the plan address the security vulnerability assessment and the risk-based performance standards for security for a facility, based on a review of—

(A) the facility's site security plan;

(B) the facility's Top-Screen;

(C) the facility's security vulnerability assessment; or

(D) any other information that—

(i) the facility submits to the Department; or

(ii) the Department obtains from a public source or other source.

(8) GUIDANCE FOR EXPEDITED APPROVAL FACILITIES.—The term ''guidance for expedited approval facilities'' means the guidance issued under section 10862(c)(4)(B)(i) of this title.

(9) RISK ASSESSMENT.—The term ''risk assessment'' means the Secretary's application of relevant risk criteria identified in section 10862(e)(2)(B) of this title.

(10) TERRORIST SCREENING DATABASE.—The term ''terrorist screening database'' means the terrorist screening database maintained by the Federal Government Terrorist Screening Center or its successor.

(11) TIER.—The term ''tier'' has the meaning given the term in section 27.105 of title 6, Code of Federal Regulations, or any successor to section 27.105.

(12) TIERING; TIERING METHODOLOGY.—The terms ''tiering'' and ''tiering methodology'' mean the procedure by which the Secretary assigns a tier to each covered chemical facility based on the risk assessment for that covered chemical facility.

(13) TOP-SCREEN.—The term ''Top-Screen'' has the meaning given the term in section 27.105 of title 6, Code of Federal Regulations, or any successor to section 27.105.

(14) VULNERABILITY ASSESSMENT.—The term ''vulnerability assessment'' means the identification of weaknesses in the security of a chemical facility of interest.

§ 10862. Chemical Facility Anti-Terrorism Standards Program

(a) DUTIES OF SECRETARY.—In carrying out the Chemical Facility Anti-Terrorism Standards Program, the Secretary shall—

(1) identify—

(A) chemical facilities of interest; and

(B) covered chemical facilities;

(2) require each chemical facility of interest to submit a Top-Screen and any other information the Secretary determines necessary to enable the Department to assess the security risks associated with the facility;

(3) establish risk-based performance standards designed to address high levels of security risk at covered chemical facilities; and

(4) require each covered chemical facility to—

(A) submit a security vulnerability assessment; and

(B) develop, submit, and implement a site security plan.

(b) SECURITY MEASURES.—

(1) IN GENERAL.—A facility, in developing a site security plan as required under subsection (a), shall include security measures that, in combination, appropriately address the security vulnerability assess-

ment and the risk-based performance standards for security for the facility.

(2) EMPLOYEE INPUT.—To the greatest extent practicable, a facility's security vulnerability assessment and site security plan shall include input from at least 1 facility employee and, where applicable, 1 employee representative from the bargaining agent at that facility, each of whom possesses, in the determination of the facility's security officer, relevant knowledge, experience, training, or education as pertains to matters of site security.

(c) APPROVAL OR DISAPPROVAL OF SITE SECURITY PLANS.—

(1) IN GENERAL.—

(A) REVIEW.—Except as provided in paragraph (4), the Secretary shall review and approve or disapprove each site security plan submitted pursuant to subsection (a).

(B) BASES FOR DISAPPROVAL.—The Secretary—

(i) may not disapprove a site security plan based on the presence or absence of a particular security measure; and

(ii) shall disapprove a site security plan if the plan fails to satisfy the risk-based performance standards established pursuant to subsection (a)(3).

(2) ALTERNATIVE SECURITY PROGRAMS.—

(A) AUTHORITY TO APPROVE.—

(i) IN GENERAL.—The Secretary may approve an alternative security program established by a private-sector entity or a Federal, State, or local authority or under other applicable laws if the Secretary determines that the requirements of the program meet the requirements under this section.

(ii) ADDITIONAL SECURITY MEASURES.—If the requirements of an alternative security program do not meet the requirements under this section, the Secretary may recommend additional security measures to the program that will enable the Secretary to approve the program.

(B) SATISFACTION OF SITE SECURITY PLAN REQUIREMENT.—A covered chemical facility may satisfy the site security plan requirement under subsection (a)(4) by adopting an alternative security program that the Secretary has—

(i) reviewed and approved under subparagraph (A); and

(ii) determined to be appropriate for the operations and security concerns of the covered chemical facility.

(3) SITE SECURITY PLAN ASSESSMENTS.—

(A) RISK ASSESSMENT POLICIES AND PROCEDURES.—In approving or disapproving a site security plan under this subsection, the Secretary shall employ the risk assessment policies and procedures developed under this subchapter.

(B) PREVIOUSLY APPROVED PLANS.—In the case of a covered chemical facility for which the Secretary approved a site security plan before December 18, 2014, the Secretary may not require the facility to resubmit the site security plan solely by reason of the enactment of this subchapter.

(4) EXPEDITED APPROVAL PROGRAM.—

(A) IN GENERAL.—A covered chemical facility assigned to tier 3 or 4 may meet the requirement to develop and submit a site security plan under subsection (a)(4) by developing and submitting to the Secretary—

(i) a site security plan and the certification described in subparagraph (C); or

(ii) a site security plan in conformance with a template authorized under subparagraph (H).

(B) GUIDANCE FOR EXPEDITED APPROVAL FACILITIES.—

(i) IN GENERAL.—The Secretary shall issue guidance for expedited approval facilities that identifies specific security measures that are sufficient to meet the risk-based performance standards.

(ii) MATERIAL DEVIATION FROM GUIDANCE.—If a security measure in the site security plan of an expedited approval facility materially deviates from a security measure in the guidance for expedited approval facilities, the site security plan shall include an explanation of how the security measure meets the risk-based performance standards.

(iii) APPLICABILITY OF OTHER LAWS TO DEVELOPMENT AND ISSUANCE OF INITIAL GUIDANCE.—In developing and issuing, or amending, the guidance for expedited approval facilities under this subparagraph and in collecting information from expedited approval facilities, the Secretary shall not be subject to—

(I) section 553 of title 5;

(II) subchapter I of chapter 35 of title 44; or

(III) section 10867(b) of this title.

(C) CERTIFICATION.—The owner or operator of an expedited approval facility shall submit to the Secretary a certification, signed under penalty of perjury, that—

(i) the owner or operator is familiar with the requirements of this subchapter and part 27 of title 6, Code of Federal Regulations, or any successor to this subchapter or part 27, and the site security plan being submitted;

(ii) the site security plan includes the security measures required by subsection (a);

(iii)(I) the security measures in the site security plan do not materially deviate from the guidance for expedited approval facilities except where indicated in the site security plan;

(II) any deviations from the guidance for expedited approval facilities in the site security plan meet the risk-based performance standards for the tier to which the facility is assigned; and

(III) the owner or operator has provided an explanation of how the site security plan meets the risk-based performance standards for any material deviation;

(iv) the owner or operator has visited, examined, documented, and verified that the expedited approval facility meets the criteria set forth in the site security plan;

(v) the expedited approval facility has implemented all the required performance measures outlined in the site security plan or set out planned measures that will be implemented within a reasonable time period stated in the site security plan;

(vi) each individual responsible for implementing the site security plan has been made aware of the requirements relevant to the individual's responsibility contained in the site security plan and has demonstrated competency to carry out those requirements;

(vii) the owner or operator has committed, or, in the case of planned measures, will commit, the necessary resources to fully implement the site security plan; and

(viii) the planned measures include an adequate procedure for addressing events beyond the control of the owner or operator in implementing any planned measures.

(D) DEADLINE.—

(i) DATE FOR SUBMISSION TO SECRETARY.—The owner or operator of an expedited approval facility shall submit to the Secretary the site security plan and the certification described in subparagraph (C) not later than 120 days after—

(I) for an expedited approval facility that was assigned to tier 3 or 4 under existing CFATS regulations before December 18, 2014, the date that is 210 days after December 18, 2014; and

(II) for any expedited approval facility not described in subclause (I), the later of—

(aa) the date on which the expedited approval facility is assigned to tier 3 or 4 under subsection (e)(2)(A); or

(bb) the date that is 210 days after December 18, 2014.

(ii) NOTICE.—An owner or operator of an expedited approval facility shall notify the Secretary of the intent of the owner or operator to certify the site security plan for the expedited approval facility not later than 30 days before the date on which the owner or operator submits the site security plan and certification described in subparagraph (C).

(E) COMPLIANCE.—

(i) IN GENERAL.—For an expedited approval facility submitting a site security plan and certification in accordance with subparagraphs (A), (B), (C), and (D)—

(I) the expedited approval facility shall comply with all of the requirements of its site security plan; and

(II) the Secretary—

(aa) except as provided in subparagraph (G), may not disapprove the site security plan; and

(bb) may audit and inspect the expedited approval facility under subsection (d) to verify compliance with its site security plan.

(ii) NONCOMPLIANCE.—If the Secretary determines an expedited approval facility is not in compliance with the requirements of the site security plan or is otherwise in violation of this subchapter, the Secretary may enforce compliance in accordance with section 10864 of this title.

(F) AMENDMENTS TO SITE SECURITY PLAN.—

(i) REQUIREMENT.—

(I) IN GENERAL.—If the owner or operator of an expedited approval facility amends a site security plan submitted under subparagraph (A), the owner or operator shall submit the amended site security plan and a certifi-

cation relating to the amended site security plan that contains the information described in subparagraph (C).

(II) TECHNICAL AMENDMENTS.—For purposes of this clause, an amendment to a site security plan includes any technical amendment to the site security plan.

(ii) WHEN AMENDMENT REQUIRED.—The owner or operator of an expedited approval facility shall amend the site security plan if—

(I) there is a change in the design, construction, operation, or maintenance of the expedited approval facility that affects the site security plan;

(II) the Secretary requires additional security measures or suspends a certification and recommends additional security measures under subparagraph (G); or

(III) the owner or operator receives notice from the Secretary of a change in tiering under subsection (e)(3).

(iii) DEADLINE.—An amended site security plan and certification shall be submitted under clause (i)—

(I) in the case of a change in design, construction, operation, or maintenance of the expedited approval facility that affects the security plan, not later than 120 days after the date on which the change in design, construction, operation, or maintenance occurred;

(II) in the case of the Secretary requiring additional security measures or suspending a certification and recommending additional security measures under subparagraph (G), not later than 120 days after the date on which the owner or operator receives notice of the requirement for additional security measures or suspension of the certification and recommendation of additional security measures; and

(III) in the case of a change in tiering under subsection (e)(3), not later than 120 days after the date on which the owner or operator receives notice.

(G) FACIALLY DEFICIENT SITE SECURITY PLANS.—

(i) PROHIBITION.—Notwithstanding subparagraph (A) or (E), the Secretary may suspend the authority of a covered chemical facility to certify a site security plan if the Secretary—

(I) determines the certified site security plan or an amended site security plan is facially deficient; and

(II) not later than 100 days after the date on which the Secretary receives the site security plan and certification, provides the covered chemical facility with written notification that the site security plan is facially deficient, including a clear explanation of each deficiency in the site security plan.

(ii) ADDITIONAL SECURITY MEASURES.—

(I) IN GENERAL.—If, during or after a compliance inspection of an expedited approval facility, the Secretary determines that planned or implemented security measures in the site security plan of the facility are insufficient to meet the risk-based performance standards based on misrepresentation, omission, or an inadequate description of the site, the Secretary may—

(aa) require additional security measures; or

(bb) suspend the certification of the facility.

(II) RECOMMENDATION OF ADDITIONAL SECURITY MEASURES.—If the Secretary suspends the certification of an expedited approval facility under subclause (I), the Secretary shall—

(aa) recommend specific additional security measures that, if made part of the site security plan by the facility, would enable the Secretary to approve the site security plan; and

(bb) provide the facility an opportunity to submit a new or modified site security plan and certification under subparagraph (A).

(III) SUBMISSION; REVIEW.—If an expedited approval facility determines to submit a new or modified site security plan and certification as authorized under subclause (II)(bb)—

(aa) not later than 90 days after the date on which the facility receives recommendations under subclause (II)(aa), the facility shall submit the new or modified plan and certification; and

(bb) not later than 45 days after the date on which the Secretary receives the new or modified plan under item (aa), the Secretary shall review the plan and determine whether the plan is facially deficient.

(IV) DETERMINATION NOT TO INCLUDE ADDITIONAL SECURITY MEASURES.—

(aa) REVOCATION OF CERTIFICATION.—If an expedited approval facility does not agree to include in its site security plan specific additional security measures recommended by the Secretary under subclause (II)(aa), or does not submit a new or modified site security plan in accordance with subclause (III), the Secretary may revoke the certification of the facility by issuing an order under section 10864(a)(1)(B) of this title.

(bb) EFFECT OF REVOCATION.—If the Secretary revokes the certification of an expedited approval facility under item (aa) by issuing an order under section 10864(a)(1)(B) of this title—

(AA) the order shall require the owner or operator of the facility to submit a site security plan or alternative security program for review by the Secretary under paragraph (1) or (2); and

(BB) the facility shall no longer be eligible to certify a site security plan under this paragraph.

(V) FACIAL DEFICIENCY.—If the Secretary determines that a new or modified site security plan submitted by an expedited approval facility under subclause (III) is facially deficient—

(aa) not later than 120 days after the date of the determination, the owner or operator of the facility shall submit a site security plan or alternative security program for review by the Secretary under paragraph (1) or (2); and

(bb) the facility shall no longer be eligible to certify a site security plan under this paragraph.

(H) TEMPLATES.—

(i) IN GENERAL.—The Secretary may develop prescriptive site security plan templates with specific security measures to meet the risk-based performance standards under subsection (a)(3) for adoption and certification by a covered chemical facility assigned to tier 3 or 4 in lieu of developing and certifying its own plan.

(ii) APPLICABILITY OF OTHER LAWS TO DEVELOPING AND ISSUING INITIAL SITE SECURITY PLAN TEMPLATES AND RELATED GUIDANCE AND TO COLLECTING INFORMATION.—During the period before the Secretary has met the deadline under subparagraph (D)(i), in developing and issuing, or amending, the site security plan templates under this subparagraph, in issuing guidance for implementation of the templates, and in collecting information from expedited approval facilities, the Secretary shall not be subject to—

(I) section 553 of title 5;

(II) subchapter I of chapter 35 of title 44; or

(III) section 10867(b) of this title.

(iii) RULE OF CONSTRUCTION.—Nothing in this subparagraph shall be construed to prevent a covered chemical facility from developing and certifying its own security plan in accordance with subparagraph (A).

(I) EVALUATION.—

(i) IN GENERAL.—The Secretary shall take any appropriate action necessary for a full evaluation of the expedited approval program authorized under this paragraph, including conducting an appropriate number of inspections, as authorized under subsection (d), of expedited approval facilities.

(ii) REPORT.—The Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives a report that contains—

(I)(aa) the number of eligible facilities using the expedited approval program authorized under this paragraph; and

(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 (a)(4);

(II) any costs and efficiencies associated with the expedited approval program;

(III) the impact of the expedited approval program on the backlog for site security plan approval and authorization inspections;

(IV) an assessment of the ability of expedited approval facilities to submit facially sufficient site security plans;

(V) an assessment of any impact of the expedited approval program on the security of chemical facilities; and

(VI) a recommendation by the Secretary on the frequency of compliance inspections that may be required for expedited approval facilities.

(d) COMPLIANCE.—

(1) AUDITS AND INSPECTIONS.—

(A) DEFINITIONS.—In this paragraph:

(i) NONDEPARTMENTAL.—The term ''nondepartmental''—

(I) with respect to personnel, means personnel who are not employed by the Department; and

(II) with respect to an entity, means an entity that is not a component or other authority of the Department.

(ii) NONGOVERNMENTAL.—The term ''nongovernmental''—

(I) with respect to personnel, means personnel who are not employed by the Federal Government; and

(II) with respect to an entity, means an entity that is not an agency, department, or other authority of the Federal Government.

(B) AUTHORITY TO CONDUCT AUDITS AND INSPECTIONS.—The Secretary shall conduct audits or inspections under this subchapter using—

(i) employees of the Department;

(ii) nondepartmental or nongovernmental personnel approved by the Secretary; or

(iii) a combination of individuals described in clauses (i) and (ii).

(C) SUPPORT PERSONNEL.—The Secretary may use nongovernmental personnel to provide administrative and logistical services in support of audits and inspections under this subchapter.

(D) REPORTING STRUCTURE.—

(i) NONDEPARTMENTAL AND NONGOVERNMENTAL AUDITS AND INSPECTIONS.—Any audit or inspection conducted by an individual employed by a nondepartmental or nongovernmental entity shall be assigned in coordination with a regional supervisor with responsibility for supervising inspectors in the Infrastructure Security Compliance Division of the Department for the region in which the audit or inspection is to be conducted.

(ii) REQUIREMENT TO REPORT.—While an individual employed by a nondepartmental or nongovernmental entity is in

the field conducting an audit or inspection under this subsection, the individual shall report to the regional supervisor with responsibility for supervising inspectors in the Infrastructure Security Compliance Division of the Department for the region in which the individual is operating.

(iii) APPROVAL.—The authority to approve a site security plan under subsection (c) or determine if a covered chemical facility is in compliance with an approved site security plan shall be exercised solely by the Secretary or a designee of the Secretary in the Department.

(E) STANDARDS FOR AUDITORS AND INSPECTORS.—The Secretary shall prescribe standards for the training and retraining of each individual used by the Department as an auditor or inspector, including each individual employed by the Department and all nondepartmental or nongovernmental personnel, including—

(i) minimum training requirements for new auditors and inspectors;

(ii) retraining requirements;

(iii) minimum education and experience levels;

(iv) the submission of information as required by the Secretary to enable determination of whether the auditor or inspector has a conflict of interest;

(v) the proper certification necessary to handle chemical-terrorism vulnerability information (as defined in section 27.105 of title 6, Code of Federal Regulations, or any successor to section 27.105);

(vi) the reporting of any issue of non-compliance with this section to the Secretary within 24 hours; and

(vii) any additional qualifications for fitness of duty as the Secretary may require.

(F) CONDITIONS FOR NONGOVERNMENTAL AUDITORS AND INSPECTORS.—If the Secretary arranges for an audit or inspection under subparagraph (B) to be carried out by a nongovernmental entity, the Secretary shall—

(i) prescribe standards for the qualification of the individuals who carry out the audits and inspections that are commensurate with the standards for similar Government auditors or inspectors; and

(ii) ensure that any duties carried out by a nongovernmental entity are not inherently governmental functions.

(2) PERSONNEL SURETY PROGRAM.—

(A) ESTABLISHMENT.—For purposes of this subchapter, the Secretary shall establish and carry out a Personnel Surety Program that—

(i) does not require an owner or operator of a covered chemical facility that voluntarily participates in the program to submit information about an individual more than 1 time;

(ii) provides a participating owner or operator of a covered chemical facility with relevant information about an individual based on vetting the individual against the terrorist screening database, to the extent that the feedback is necessary for the facility to be in compliance with regulations promulgated under this subchapter; and

(iii) provides redress to an individual—

(I) whose information was vetted against the terrorist screening database under the program; and

(II) who believes that the personally identifiable information submitted to the Department for vetting by a covered chemical facility, or its designated representative, was inaccurate.

(B) IMPLEMENTATION.—To the extent that a risk-based performance standard established under subsection (b) requires identifying individuals with ties to terrorism—

(i) a covered chemical facility—

(I) may satisfy its obligation under the standard by using any Federal screening program that periodically vets individuals against the terrorist screening database, or any successor program, including the Personnel Surety Program established under subparagraph (A); and

(II) shall—

(aa) accept a credential from a Federal screening program described in subclause (I) if an individual who is required to be screened presents the credential; and

(bb) address in its site security plan or alternative security program the measures it will take to verify that a credential or documentation from a Federal screening program described in subclause (I) is current;

(ii) visual inspection shall be sufficient to meet the requirement under clause (i)(II)(bb), but the facility should consider other means of verification, consistent with the facility's as-

sessment of the threat posed by acceptance of the credentials; and

(iii) the Secretary may not require a covered chemical facility to submit any information about an individual unless the individual—

(I) is to be vetted under the Personnel Surety Program; or

(II) has been identified as presenting a terrorism security risk.

(C) RIGHTS UNAFFECTED.—Nothing in this section shall supersede the ability—

(i) of a facility to maintain its own policies regarding the access of individuals to restricted areas or critical assets; or

(ii) of an employing facility and a bargaining agent, where applicable, to negotiate as to how the results of a background check may be used by the facility with respect to employment status.

(3) AVAILABILITY OF INFORMATION.—The Secretary shall share with the owner or operator of a covered chemical facility any information that the owner or operator needs to comply with this section.

(e) RESPONSIBILITIES OF THE SECRETARY.—

(1) IDENTIFICATION OF CHEMICAL FACILITIES OF INTEREST.—In carrying out this subchapter, the Secretary shall consult with the heads of other Federal agencies, States and political subdivisions thereof, relevant business associations, and public and private labor organizations to identify all chemical facilities of interest.

(2) RISK ASSESSMENT.—

(A) IN GENERAL.—For purposes of this subchapter, the Secretary shall develop a security risk assessment approach and corresponding tiering methodology for covered chemical facilities that incorporates the relevant elements of risk, including threat, vulnerability, and consequence.

(B) CRITERIA FOR DETERMINING SECURITY RISK.—The criteria for determining the security risk of terrorism associated with a covered chemical facility shall take into account—

(i) relevant threat information;

(ii) potential severe economic consequences and the potential loss of human life in the event of the facility's being subject to attack, compromise, infiltration, or exploitation by terrorists; and

(iii) vulnerability of the facility to attack, compromise, infiltration, or exploitation by terrorists.

(3) CHANGES IN TIERING.—

(A) MAINTENANCE OF RECORDS.—The Secretary shall document the basis for each instance in which—

(i) tiering for a covered chemical facility is changed; or

(ii) a covered chemical facility is determined to no longer be subject to the requirements under this subchapter.

(B) REQUIRED INFORMATION.—The records maintained under subparagraph (A) shall include information on whether and how the Secretary confirmed the information that was the basis for the change or determination described in subparagraph (A).

(4) SEMIANNUAL PERFORMANCE REPORTING.—Not later than 6 months after December 18, 2014, and not less frequently than once every 6 months after that date, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives a report that includes, for the period covered by the report—

(A) the number of covered chemical facilities in the United States;

(B) information—

(i) describing—

(I) the number of instances in which the Secretary—

(aa) placed a covered chemical facility in a lower risk tier; or

(bb) determined that a facility that had previously met the criteria for a covered chemical facility under section 10861(3) of this title no longer met the criteria; and

(II) the basis, in summary form, for each action or determination under subclause (I); and

(ii) that is provided in a sufficiently anonymized form to ensure that the information does not identify any specific facility or company as the source of the information when viewed alone or in combination with other public information;

(C) the average number of days spent reviewing site security or an alternative security program for a covered chemical facility prior to approval;

(D) the number of covered chemical facilities inspected;

(E) the average number of covered chemical facilities inspected per inspector; and

(F) any other information that the Secretary determines will be helpful to Congress in evaluating the performance of the Chemical Facility Anti-Terrorism Standards Program.

§ 10863. Protection and sharing of information

(a) IN GENERAL.—Notwithstanding another law, information developed under this subchapter, including vulnerability assessments, site security plans, and other security related information, records, and documents shall be given protections from public disclosure consistent with the protection of similar information under section 70103(d) of title 46.

(b) SHARING OF INFORMATION WITH STATES AND LOCAL GOVERNMENTS.—Nothing in this section shall be construed to prohibit the sharing of information developed under this subchapter, as the Secretary determines appropriate, with State and local government officials possessing a need to know and the necessary security clearances, including law enforcement officials and first responders, for the purpose of carrying out this subchapter, provided that the information may not be disclosed pursuant to any State or local law.

(c) SHARING OF INFORMATION WITH FIRST RESPONDERS.—

(1) REQUIREMENT.—The Secretary shall provide to State, local, and regional fusion centers (as that term is defined in section 10512(a)(1) of this title) and State and local government officials, as the Secretary determines appropriate, such information as is necessary to help ensure that first responders are properly prepared and provided with the situational awareness needed to respond to security incidents at covered chemical facilities.

(2) DISSEMINATION.—The Secretary shall disseminate information under paragraph (1) through a medium or system determined by the Secretary to be appropriate to ensure the secure and expeditious dissemination of the information to necessary selected individuals.

(d) ENFORCEMENT PROCEEDINGS.—In any proceeding to enforce this section, vulnerability assessments, site security plans, and other information submitted to or obtained by the Secretary under this subchapter, and related vulnerability or security information, shall be treated as if the information were classified information.

(e) AVAILABILITY OF INFORMATION.—Notwithstanding another law (including section 552(b)(3) of title 5), section 552 of title 5 shall not apply to information protected from public disclosure pursuant to subsection (a).

(f) SHARING OF INFORMATION WITH MEMBERS OF CONGRESS.—Nothing in this section shall prohibit the Secretary from disclosing information devel-

oped under this subchapter to a Member of Congress in response to a request by a Member of Congress.

§ 10864. Civil enforcement

(a) NOTICE OF NONCOMPLIANCE.—

(1) IN GENERAL.—If the Secretary determines that a covered chemical facility is not in compliance with this subchapter, the Secretary shall—

(A) provide the owner or operator of the facility—

(i) not later than 14 days after the date on which the Secretary makes the determination, a written notification of noncompliance that includes a clear explanation of any deficiency in the security vulnerability assessment or site security plan; and

(ii) an opportunity for consultation with the Secretary or the Secretary's designee; and

(B) issue to the owner or operator of the facility an order to comply with this subchapter by a date specified by the Secretary in the order, which date shall be not later than 180 days after the date on which the Secretary issues the order.

(2) CONTINUED NONCOMPLIANCE.—If an owner or operator remains noncompliant after the procedures outlined in paragraph (1) have been executed, or demonstrates repeated violations of this subchapter, the Secretary may enter an order in accordance with this section assessing a civil penalty, an order to cease operations, or both.

(b) CIVIL PENALTIES.—

(1) VIOLATIONS OF ORDERS.—Any person who violates an order issued under this subchapter shall be liable for a civil penalty under section 70119(a) of title 46.

(2) NON-REPORTING CHEMICAL FACILITIES OF INTEREST.—Any owner of a chemical facility of interest who fails to comply with, or knowingly submits false information under, this subchapter or the CFATS regulations shall be liable for a civil penalty under section 70119(a) of title 46.

(c) EMERGENCY ORDERS.—

(1) IN GENERAL.—Notwithstanding subsection (a) or any site security plan or alternative security program approved under this subchapter, if the Secretary determines that there is an imminent threat of death, serious illness, or severe personal injury, due to a violation of this subchapter or the risk of a terrorist incident that may affect a chemical facility of interest, the Secretary—

(A) shall consult with the facility, if practicable, on steps to mitigate the risk; and

(B) may order the facility, without notice or opportunity for a hearing, effective immediately or as soon as practicable, to—

(i) implement appropriate emergency security measures; or

(ii) cease or reduce some or all operations, in accordance with safe shutdown procedures, if the Secretary determines that such a cessation or reduction of operations is the most appropriate means to address the risk.

(2) LIMITATION ON DELEGATION.—The Secretary may not delegate the authority under paragraph (1) to any official other than the Director of the Cybersecurity and Infrastructure Security Agency.

(3) LIMITATION ON AUTHORITY.—The Secretary may exercise the authority under this subsection only to the extent necessary to abate the imminent threat determination under paragraph (1).

(4) DUE PROCESS FOR FACILITY OWNER OR OPERATOR.—

(A) WRITTEN ORDERS.—An order issued by the Secretary under paragraph (1) shall be in the form of a written emergency order that—

(i) describes the violation or risk that creates the imminent threat;

(ii) states the security measures or order issued or imposed; and

(iii) describes the standards and procedures for obtaining relief from the order.

(B) OPPORTUNITY FOR REVIEW.—After issuing an order under paragraph (1) with respect to a chemical facility of interest, the Secretary shall provide for review of the order under section 554 of title 5 if a petition for review is filed not later than 20 days after the date on which the Secretary issues the order.

(C) EXPIRATION OF EFFECTIVENESS OF ORDER.—If a petition for review of an order is filed under subparagraph (B) and the review under subparagraph (B) is not completed by the last day of the 30-day period beginning on the date on which the petition is filed, the order shall vacate automatically at the end of that period unless the Secretary determines, in writing, that the imminent threat providing a basis for the order continues to exist.

(d) RIGHT OF ACTION.—Nothing in this subchapter confers upon any individual except the Secretary or his or her designee a right of action against an owner or operator of a covered chemical facility to enforce any provision of this subchapter.

§ 10865. Whistleblower protections

(a) PROCEDURE FOR REPORTING PROBLEMS.—

(1) ESTABLISHMENT.—The Secretary shall establish, and provide information to the public regarding, a procedure under which any employee or contractor of a chemical facility of interest may submit a report to the Secretary regarding a violation of a requirement under this subchapter.

(2) CONFIDENTIALITY.—The Secretary shall keep confidential the identity of an individual who submits a report under paragraph (1), and the report shall be treated as a record containing protected information to the extent that the report does not consist of publicly available information.

(3) ACKNOWLEDGMENT OF RECEIPT.—If a report submitted under paragraph (1) identifies the individual making the report, the Secretary shall promptly respond to the individual directly and shall promptly acknowledge receipt of the report.

(4) STEPS TO ADDRESS PROBLEMS.—The Secretary—

(A) shall review and consider the information provided in any report submitted under paragraph (1); and

(B) may take action under section 10864 of this title if necessary to address any substantiated violation of a requirement under this subchapter identified in the report.

(5) DUE PROCESS FOR FACILITY OWNER OR OPERATOR.—

(A) IN GENERAL.—If, on the review described in paragraph (4), the Secretary determines that a violation of a provision of this subchapter, or a regulation prescribed under this subchapter, has occurred, the Secretary may—

(i) institute a civil enforcement under section 10864(a) of this title; or

(ii) if the Secretary makes the determination under section 10864(c) of this title, issue an emergency order.

(B) WRITTEN ORDERS.—The action of the Secretary under paragraph (4) shall be in a written form that—

(i) describes the violation;

(ii) states the authority under which the Secretary is proceeding; and

(iii) describes the standards and procedures for obtaining relief from the order.

(C) OPPORTUNITY FOR REVIEW.—After taking action under paragraph (4), the Secretary shall provide for review of the action

if a petition for review is filed within 20 calendar days of the date of issuance of the order for the action.

(D) EXPIRATION OF EFFECTIVENESS OF ORDER.—If a petition for review of an action is filed under subparagraph (C) and the review under that subparagraph is not completed by the end of the 30-day period beginning on the date the petition is filed, the action shall cease to be effective at the end of that period unless the Secretary determines, in writing, that the violation providing a basis for the action continues to exist.

(6) RETALIATION PROHIBITED.—

(A) IN GENERAL.—An owner or operator of a chemical facility of interest or agent thereof may not discharge an employee or otherwise discriminate against an employee with respect to the compensation provided to, or terms, conditions, or privileges of the employment of, the employee because the employee (or an individual acting pursuant to a request of the employee) submitted a report under paragraph (1).

(B) EXCEPTION.—An employee shall not be entitled to the protections under this section if the employee—

(i) knowingly and willfully makes any false, fictitious, or fraudulent statement or representation; or

(ii) uses any false writing or document knowing the writing or document contains any false, fictitious, or fraudulent statement or entry.

(b) PROTECTED DISCLOSURES.—Nothing in this subchapter shall be construed to limit the right of an individual to make any disclosure—

(1) protected or authorized under section 2302(b)(8) or 7211 of title 5;

(2) protected under any other Federal or State law that shields the disclosing individual against retaliation or discrimination for having made the disclosure in the public interest; or

(3) to the Special Counsel of an agency, the inspector general of an agency, or any other employee designated by the head of an agency to receive disclosures similar to the disclosures described in paragraphs (1) and (2).

(c) PUBLICATION OF RIGHTS.—The Secretary, in partnership with industry associations and labor organizations, shall make publicly available both physically and online the rights that an individual who discloses information, including security-sensitive information, regarding problems, deficiencies, or vulnerabilities at a covered chemical facility would have under Federal whistleblower protection laws or this subchapter.

(d) PROTECTED INFORMATION.—All information contained in a report made under subsection (a) shall be protected in accordance with section 10863 of this title.

§ 10866. Relationship to other laws

(a) OTHER FEDERAL LAWS.—Nothing in this subchapter shall be construed to supersede, amend, alter, or affect any Federal law that—

(1) regulates (including by requiring information to be submitted or made available) the manufacture, distribution in commerce, use, handling, sale, other treatment, or disposal of chemical substances or mixtures; or

(2) authorizes or requires the disclosure of any record or information obtained from a chemical facility under any law other than this subchapter.

(b) STATES AND POLITICAL SUBDIVISIONS.—This subchapter shall not preclude or deny any right of any State or political subdivision of a State to adopt or enforce any regulation, requirement, or standard of performance with respect to chemical facility security that is more stringent than a regulation, requirement, or standard of performance issued under this subchapter, or otherwise impair any right or jurisdiction of any State with respect to chemical facilities within that State, unless there is an actual conflict between this section and the law of that State.

§ 10867. CFATS regulations

(a) GENERAL AUTHORITY.—The Secretary may, in accordance with chapter 5 of title 5, promulgate regulations or amend CFATS regulations that existed 30 days after December 18, 2014, to implement the provisions under this subchapter.

(b) EXISTING CFATS REGULATIONS.—

(1) IN GENERAL.—Notwithstanding section 4(b) of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (Public Law 113–254, 128 Stat. 2919), each CFATS regulation that existed on December 18, 2014, remains in effect unless the Secretary amends, consolidates, or repeals the regulation.

(2) REPEAL.—Not later than 30 days after December 18, 2014, the Secretary shall repeal any CFATS regulation that existed on that date that the Secretary determines is duplicative of, or conflicts with, this subchapter.

(c) AUTHORITY.—The Secretary shall exclusively rely upon authority provided under this subchapter in—

(1) determining compliance with this subchapter;

(2) identifying chemicals of interest; and

(3) determining security risk associated with a chemical facility.

§ 10868. Small covered chemical facilities

(a) DEFINITION OF SMALL COVERED CHEMICAL FACILITY.—In this section, the term ''small covered chemical facility'' means a covered chemical facility that—

(1) has fewer than 100 employees employed at the covered chemical facility; and

(2) is owned and operated by a small business concern (as defined in section 3 of the Small Business Act (15 U.S.C. 632).

(b) ASSISTANCE TO FACILITIES.—The Secretary may provide guidance and, as appropriate, tools, methodologies, or computer software, to assist small covered chemical facilities in developing the physical security, cybersecurity, recordkeeping, and reporting procedures required under this subchapter.

(c) REPORT.—The Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives a report on best practices that may assist small covered chemical facilities in the development of physical security best practices.

§ 10869. Outreach to chemical facilities of interest

The Secretary shall establish an outreach implementation plan, in coordination with the heads of other appropriate Federal and State agencies, relevant business associations, and public and private labor organizations, to—

(1) identify chemical facilities of interest; and

(2) make available compliance assistance materials and information on education and training.

§ 10870. Termination

The authority provided under this subchapter terminates on July 27, 2023.

Subchapter IX—Miscellaneous

§ 10881. Duties and authorities relating to .gov internet domain

(a) PURPOSE.—The purpose of the .gov internet domain program is to—

(1) legitimize and enhance public trust in government entities and their online services;

(2) facilitate trusted electronic communication and connections to and from government entities;

(3) provide simple and secure registration of .gov internet domains;

(4) improve the security of the services hosted within these .gov internet domains, and of the .gov namespace in general; and

(5) enable the discoverability of government services to the public and to domain registrants.

(b) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44.

(2) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(3) ONLINE SERVICE.—The term ''online service'' means an internet-facing service, including a website, email, a virtual private network, or a custom application.

(4) STATE.—The term ''State'' means a State, the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, Northern Mariana Islands, and a possession of the United States.

(c) TRANSITION.—The Director shall operationally administer the .gov internet domain program formerly operated by the General Services Administration under title 41, Code of Federal Regulations, and shall publish on a publicly available website the requirements for domain registrants as described in subsection (d). The requirements in part 102–173 of title 41, Code of Federal Regulations, are rescinded.

(d) AVAILABILITY OF .GOV INTERNET DOMAIN.—The Director shall make .gov internet domain name registration services, as well as any supporting services described in subsection (g), generally available—

(1) to any Federal, State, local, or territorial government entity, or other publicly controlled entity, including any Tribal government recognized by the Federal Government or a State government, that complies with the requirements for registration developed by the Director as described in subsection (e);

(2) without conditioning registration on the sharing of any information with the Director or any other Federal entity, other than the information required to meet the requirements described in subsection (e); and

(3) without conditioning registration on participation in any separate service offered by the Director or any other Federal entity.

(e) REQUIREMENTS.—The Director, with the approval of the Director of the Office of Management and Budget for agency .gov internet domain requirements and in consultation with the Director of the Office of Management and Budget for .gov internet domain requirements for entities that are not agencies, shall establish and publish on a publicly available website requirements for the registration and operation of .gov internet domains sufficient to—

(1) minimize the risk of .gov internet domains whose names could mislead or confuse users;

(2) establish that .gov internet domains may not be used for commercial or political campaign purposes;

(3) ensure that domains are registered and maintained only by authorized individuals; and

(4) limit the sharing or use of any information obtained through the administration of the .gov internet domain with any other Department component or any other agency for a purpose other than the administration of the .gov internet domain, the services described in subsection (g), and the requirements for establishing a .gov inventory described in subsection (k).

(f) EXECUTIVE BRANCH.—

(1) IN GENERAL.—The Director of the Office of Management and Budget shall establish applicable processes and guidelines for the registration and acceptable use of .gov internet domains by agencies.

(2) APPROVAL REQUIRED.—The Director shall obtain the approval of the Director of the Office of Management and Budget before registering a .gov internet domain name for an agency.

(3) COMPLIANCE.—Each agency shall ensure that any website or digital service of the agency that uses a .gov internet domain is in compliance with the 21st Century Integrated Digital Experience Act (44 U.S.C. 3501 note) and implementation guidance issued pursuant to that Act.

(g) SUPPORTING SERVICES.—

(1) IN GENERAL.—The Director may provide services to the entities described in subsection (d)(1) specifically intended to support the security, privacy, reliability, accessibility, and speed of registered .gov internet domains.

(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to—-

(A) limit other authorities of the Director to provide services or technical assistance to an entity described in subsection (d)(1); or

(B) establish new authority for services other than those the purpose of which expressly supports the operation of .gov internet domains and the needs of .gov internet domain registrants.

(h) FEES.—

(1) IN GENERAL.—The Director may provide a service relating to the availability of the .gov internet domain program, including .gov internet domain name registration services described in subsection (d) and supporting services described in subsection (g), to entities de-

scribed in subsection (d)(1) with or without reimbursement, including variable pricing.

(2) PRICING.—The total fees collected for new .gov internet domain registrants or annual renewals of .gov internet domains shall not exceed the direct operational expenses of improving, maintaining, and operating the .gov internet domain, .gov internet domain services, and .gov internet domain supporting services.

(3) ENTITIES NOT AGENCIES.—During the 5-year period beginning on December 27, 2020, a fee charged to entities that are not agencies for new .gov internet domain registrants or annual renewals of .gov internet domains shall be not more than the amount of the fee charged for the registration or renewal as of October 1, 2019.

(i) CONSULTATION.—The Director shall consult with the Director of the Office of Management and Budget, the Administrator of General Services, other civilian Federal agencies as appropriate, and entities representing State, local, Tribal, or territorial governments in developing the strategic direction of the .gov internet domain and in establishing requirements under subsection (e), in particular on matters of privacy, accessibility, transparency, and technology modernization.

(j) REFERENCE GUIDE.—Not later than 1 year after December 27, 2020, the Director, in consultation with the Administrator of General Services and entities representing State, local, Tribal, or territorial governments, shall develop and publish on a publicly available website a reference guide for migrating online services to the .gov internet domain, which shall include

(1) process and technical information on how to carry out a migration of common categories of online services, such as web and email services;

(2) best practices for cybersecurity pertaining to registration and operation of a .gov internet domain; and

(3) references to contract vehicles and other private-sector resources vetted by the Director that may assist in performing the migration.

(k) .GOV INVENTORY.—

(1) IN GENERAL.—The Director shall, on a continuous basis—

(A) inventory all hostnames and services in active use within the .gov internet domain; and

(B) provide the data described in subparagraph (A) to domain registrants at no cost.

(2) REQUIREMENTS.—In carrying out paragraph (1)—

(A) the Director may collect the data through analysis of public and non-public sources, including commercial data sets;

(B) the Director shall share with Federal and non-Federal domain registrants all unique hostnames and services discovered within the zone of their registered domain;

(C) the Director shall share any data or information collected or used in the management of the .gov internet domain name registration services relating to Federal executive branch registrants with the Director of the Office of Management and Budget for the purpose of fulfilling the duties of the Director of the Office of Management and Budget under section 3553 of title 44;

(D) the Director shall publish on a publicly available website discovered hostnames that describe publicly accessible agency websites, to the extent consistent with the security of Federal information systems but with the presumption of disclosure;

(E) the Director may publish on a publicly available website any analysis conducted and data collected relating to compliance with Federal mandates and industry best practices, to the extent consistent with the security of Federal information systems but with the presumption of disclosure; and

(F) the Director shall—

(i) collect information on the use of non-.gov internet domain suffixes by agencies for their official online services;

(ii) collect information on the use of non-.gov internet domain suffixes by State, local, Tribal, and territorial governments; and

(iii) publish the information collected under clause (i) on a publicly available website to the extent consistent with the security of the Federal information systems, but with the presumption of disclosure.

(3) NATIONAL SECURITY COORDINATION.—

(A) IN GENERAL.—In carrying out this subsection, the Director shall inventory, collect, and publish hostnames and services in a manner consistent with the protection of national security information.

(B) LIMITATION.—The Director may not inventory, collect, or publish hostnames or services under this subsection if the Director, in coordination with other heads of agencies, as appropriate, determines that the collection or publication would—

(i) disrupt a law enforcement investigation;

(ii) endanger national security or intelligence activities;

(iii) impede national defense activities or military operations; or

(iv) hamper security remediation actions.

(4) STRATEGY.—Not later than 180 days after December 27, 2020, the Director shall develop and submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Rules and Administration of the Senate and the Committee on Homeland Security, the Committee on Oversight and Reform, and the Committee on House Administration of the House of Representatives a strategy to utilize the information collected under this subsection for countering malicious cyber activity.

§ 10882. Intelligence and cybersecurity diversity fellowship program

(a) DEFINITIONS.–In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) EXCEPTED SERVICE.—The term ''excepted service'' has the meaning given that term in section 2103 of title 5.

(3) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term ''historically Black college or university'' has the meaning given the term ''part B institution'' in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

(4) INSTITUTION OF HIGHER LEARNING.—The term ''institution of higher learning'' has the meaning given that term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

(5) MINORITY-SERVING INSTITUTION.—The term ''minority-serving institution'' means an institution of higher education described in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

(b) PROGRAM.—The Secretary shall carry out an intelligence and cybersecurity diversity fellowship program (in this section referred to as the ''Program'') under which an eligible individual may—

(1) participate in a paid internship at the Department that relates to intelligence, cybersecurity, or some combination of intelligence and cybersecurity;

(2) receive tuition assistance from the Secretary; and

(3) on graduation from an institution of higher education and successful completion of the Program (as defined by the Secretary), re-

ceive an offer of employment to work in an intelligence or cybersecurity position of the Department that is in the excepted service.

(c) ELIGIBILITY.—To be eligible to participate in the Program, an individual shall—

(1) be a citizen of the United States; and

(2) as of the date of submitting the application to participate in the Program—

(A) have a cumulative grade point average of at least 3.2 on a 4.0 scale;

(B) be a socially disadvantaged individual (as that term is defined in section 124.103 of title 13, Code of Federal Regulations, or a successor regulation); and

(C) be a sophomore, junior, or senior at an institution of higher education.

(d) DIRECT HIRE AUTHORITY.—If an individual who receives an offer of employment under subsection (b)(3) accepts the offer, the Secretary shall appoint, without regard to provisions of subchapter I of chapter 33 of title 5 (except for section 3328 of title 5) the individual to the position specified in the offer.

(e) REPORTS.—Not later than 1 year after December 27, 2020, and on an annual basis thereafter, the Secretary shall submit to the appropriate committees of Congress a report on the Program. Each report shall include, with respect to the most recent year, the following:

(1) A description of outreach efforts by the Secretary to raise awareness of the Program among institutions of higher education in which eligible individuals are enrolled.

(2) Information on specific recruiting efforts conducted by the Secretary to increase participation in the Program.

(3) The number of individuals participating in the Program, listed by the institution of higher education in which the individual is enrolled at the time of participation, and information on the nature of the participation, including on whether the duties of the individual under the Program relate primarily to intelligence or to cybersecurity.

(4) The number of individuals who accepted an offer of employment under the Program and an identification of the element in the Department to which each individual was appointed.

§ 10883. Cybersecurity State Coordinator

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''Agency'' means the Cybersecurity and Infrastructure Security Agency

(2) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(b) APPOINTMENT.—The Director shall appoint an employee of the Agency in each State, with the appropriate cybersecurity qualifications and expertise, who shall serve as the Cybersecurity State Coordinator.

(c) DUTIES.—The duties of a Cybersecurity State Coordinator appointed under subsection (b) shall include—

(1) building strategic public- and, on a voluntary basis, private-sector relationships, including by advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure;

(2) serving as the Federal cybersecurity risk advisor and supporting preparation, response, and remediation efforts relating to cybersecurity risks and incidents;

(3) facilitating the sharing of cyber threat information to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;

(4) raising awareness of the financial, technical, and operational resources available from the Federal Government to non-Federal entities to increase resilience against cyber threats;

(5) supporting training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents, including ransomware;

(6) serving as a principal point of contact for non-Federal entities to engage, on a voluntary basis, with the Federal Government on preparing for, managing, and responding to cybersecurity incidents;

(7) assisting non-Federal entities in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards;

(8) assisting State, local, Tribal, and territorial governments, on a voluntary basis, in the development of State cybersecurity plans;

(9) coordinating with appropriate officials in the Agency; and

(10) performing such other duties as determined necessary by the Director to achieve the goal of managing cybersecurity risks in the United States and reducing the impact of cyber threats to non-Federal entities.

(d) REPORTING STRUCTURE AND COORDINATION PROCESSES AND PROCEDURES.—The Director shall establish and submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a plan de-

scribing the reporting structure and coordination processes and procedures of Cybersecurity State Coordinators in the Agency.

(e) FEEDBACK.—The Director shall consult with relevant State, local, Tribal, and territorial officials regarding the appointment, and State, local, Tribal, and territorial officials and other non-Federal entities regarding the performance, of the Cybersecurity State Coordinator of a State.

(f) OVERSIGHT.—The Director shall establish and submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a briefing on the placement and efficacy of the Cybersecurity State Coordinators appointed under subsection (b) and the coordination plan required under subsection (d)—

(1) not later than 1 year after January 1, 2021; and

(2) not later than 2 years after providing the 1st briefing under this subsection.

(g) RULE OF CONSTRUCTION.—Nothing in this section may be construed to affect or otherwise modify the authority of Federal law enforcement agencies with respect to investigations relating to cybersecurity incidents.

§ 10884. Sector Risk Management Agencies

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and the Committee on Armed Services of the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services of the Senate.

(2) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given that term in section 1016 of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c).

(3) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(4) SECTOR RISK MANAGEMENT AGENCY.—The term ''sector risk management agency'' has the meaning given that term in section 10701 of this title.

(b) CRITICAL INFRASTRUCTURE SECTOR DESIGNATION.—

(1) INITIAL REVIEW.—Not later than 180 days after January 1, 2021, the Secretary, in consultation with the heads of Sector Risk Management Agencies, shall—

(A) review the current framework for securing critical infrastructure, as described in section 10702(a)(1)(D) of this title and Presidential Policy Directive 21; and

(B) submit to the President and appropriate congressional committees a report that includes—

(i) information relating to—

(I) the analysis framework or methodology used to—

(aa) evaluate the current framework for securing critical infrastructure referred to in subparagraph (A); and

(bb) develop recommendations to—

(AA) revise the current list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, a successor or related document, or a policy; or

(BB) identify and designate any subsectors of those sectors; and

(II) the data, metrics, and other information used to develop the recommendations required under clause (ii); and

(ii) recommendations relating to—

(I) revising—

(aa) the current framework for securing critical infrastructure referred to in subparagraph (A);

(bb) the current list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, a successor or related document, or a policy; or

(cc) the identification and designation of any subsectors of those sectors; and

(II) any revisions to the list of designated Federal departments or agencies that serve as the Sector Risk Management Agency for a sector or subsector of that sector, necessary to comply with paragraph (3)(B).

(2) PERIODIC EVALUATION BY SECRETARY.—At least once every 5 years, the Secretary, in consultation with the Director and the heads of Sector Risk Management Agencies, shall—

(A) evaluate the current list of designated critical infrastructure sectors and subsectors of those sectors and the appropriateness of Sector Risk Management Agency designations, as set forth in Presidential Policy Directive 21, a successor or related document, or a policy; and

(B) recommend, as appropriate, to the President—

(i) revisions to the current list of designated critical infrastructure sectors or subsectors of those sectors; and

(ii) revisions to the designation of a Federal department or agency designated as the Sector Risk Management Agency for a sector or subsector of that sector.

(3) REVIEW AND REVISION BY THE PRESIDENT.—Not later than 180 days after the Secretary submits a recommendation pursuant to paragraph (1) or (2), the President shall—

(A) review the recommendation and revise, as appropriate, the designation of a critical infrastructure sector or subsector or the designation of a Sector Risk Management Agency; and

(B) submit to the appropriate congressional committees, the Majority and Minority Leaders of the Senate, and the Speaker and Minority Leader of the House of Representatives, a report that includes—

(i) an explanation with respect to the basis for accepting or rejecting the recommendations of the Secretary; and

(ii) information relating to the analysis framework, methodology, metrics, and data used to—

(I) evaluate the current framework for securing critical infrastructure referred to in paragraph (1)(A); and

(II) develop—

(aa) recommendations to revise—

(AA) the list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, a successor or related document, or a policy; or

(BB) the designation of any subsectors of those sectors; and

(bb) the recommendations of the Secretary.

(4) PUBLICATION.—Any designation of critical infrastructure sectors shall be published in the Federal Register.

(c) DUTIES.—

(1) IN GENERAL.—Consistent with applicable law, Presidential directives, Federal regulations, and strategic guidance from the Secretary, each Sector Risk Management Agency, in coordination with the Director, shall—

(A) provide specialized sector-specific expertise to critical infrastructure owners and operators in its designated critical infrastructure sector or subsector of that sector; and

(B) support programs and associated activities of that sector or subsector of that sector.

(2) IMPLEMENTATION.—In carrying out this subsection, Sector Risk Management Agencies shall—

(A) coordinate with the Department and, as appropriate, other relevant Federal departments and agencies;

(B) collaborate with critical infrastructure owners and operators in the designated critical infrastructure sector or subsector of that sector; and

(C) coordinate with independent regulatory agencies, and State, local, Tribal, and territorial entities, as appropriate.

(3) RESPONSIBILITIES.—Consistent with applicable law, Presidential directives, Federal regulations, and strategic guidance from the Secretary, each Sector Risk Management Agency shall utilize its specialized expertise regarding its designated critical infrastructure sector or subsector of that sector and authorities under applicable law—

(A) to support sector risk management, in coordination with the Director, including—

(i) establishing and carrying out programs to assist critical infrastructure owners and operators in the designated sector or subsector of that sector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets, or in a region, sector, or subsector of that sector; and

(ii) recommending security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets;

(B) to assess sector risk, in coordination with the Director, including—

(i) identifying, assessing, and prioritizing risks in the designated sector or subsector of that sector, considering physical security and cybersecurity threats, vulnerabilities, and consequences; and

(ii) supporting national risk assessment efforts led by the Department;

(C) to oversee sector coordination, including—

(i) serving as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities and responsibilities under this title;

(ii) serving as the Federal Government coordinating council chair for the designated sector or subsector of that sector; and

(iii) participating in cross-sector coordinating councils, as appropriate;

(D) to facilitate, in coordination with the Director, the sharing with the Department and other appropriate Federal departments of information regarding physical security and cybersecurity threats in the designated sector or subsector of that sector, including—

(i) facilitating, in coordination with the Director, access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure, including through Information Sharing and Analysis Organizations and the National Cybersecurity and Communications Integration Center established pursuant to section 10706 of this title;

(ii) facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators in the designated sector or subsector of that sector, in coordination with the Director of National Intelligence and the heads of other Federal departments and agencies, as appropriate;

(iii) providing the Director, and facilitating awareness in the designated sector or subsector of that sector, of ongoing, and where possible, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of the sector or subsector of that sector; and

(iv) supporting the reporting requirements of the Department under applicable law by providing, on an annual basis, sector-specific critical infrastructure information;

(E) to support incident management, including—

(i) supporting, in coordination with the Director, incident management and restoration efforts during or following a security incident; and

(ii) supporting the Director, on request, in national cybersecurity asset response activities for critical infrastructure; and

(F) to contribute to emergency preparedness efforts, including—

(i) coordinating with critical infrastructure owners and operators in the designated sector or subsector of that sector and the Director in the development of planning documents

for coordinated action in the event of a natural disaster, act of terrorism, or other man-made disaster or emergency;

(ii) participating in and, in coordination with the Director, conducting or facilitating, exercises and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies in the designated sector or subsector of that sector; and

(iii) supporting the Department and other Federal departments or agencies in developing planning documents or conducting exercises or simulations when relevant to the designated sector or subsector of that sector.

(d) REPORT AND AUDITING.—Not later than 2 years after January 1, 2021 and every 4 years thereafter for 12 years, the Comptroller General shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the effectiveness of Sector Risk Management Agencies in carrying out their responsibilities under subsection (c)(3).

(e) REFERENCES.—Any reference to a Sector Specific Agency (including any permutation or conjugation of Sector Specific Agency) in a law, regulation, map, document, record, or other paper of the United States shall be deemed—

(1) to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector; and

(2) to have the meaning given the term ''sector risk management agency'' in section 10701 of this title.

§ 10885. National Cyber Director

(a) DEFINITIONS.—In this section:

(1) CYBER ATTACK OR CYBER CAMPAIGN OF SIGNIFICANT CONSEQUENCE.—The term ''cyber attack or cyber campaign of significant consequence'' means an incident or series of incidents that has the purpose or effect of—

(A) causing a significant disruption to the confidentiality, integrity, or availability of a Federal information system;

(B) harming, or otherwise significantly compromising the provision of service by, a computer or network of computers that support 1 or more entities in a critical infrastructure sector;

(C) significantly compromising the provision of services by 1 or more entities in a critical infrastructure sector;

(D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial informa-

tion for commercial or competitive advantage or private financial gain; or

(E) otherwise constituting a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

(2) CYBERSECURITY POSTURE.—The term ''cybersecurity posture'' means the ability to identify, to protect against, to detect, to respond to, and to recover from an intrusion in an information system the compromise of which could constitute a cyber attack or cyber campaign of significant consequence.

(3) INCIDENT.—The term ''incident'' has the meaning given the term in section 3552 of title 44.

(4) INCIDENT RESPONSE.—The term ''incident response'' means a government or private-sector activity that detects, mitigates, or recovers from a cyber attack or cyber campaign of significant consequence.

(5) INFORMATION SECURITY.—The term ''information security'' has the meaning given the term in section 3552 of title 44.

(6) INTELLIGENCE.—The term ''intelligence'' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(b) IN GENERAL.—There is, in the Executive Office of the President, the Office of the National Cyber Director (in this section referred to as the ''Office'').

(c) NATIONAL CYBER DIRECTOR.—

(1) IN GENERAL.—The National Cyber Director (in this section referred to as the ''Director'') is the head of the Office.

(2) APPOINTMENT AND PERIOD OF SERVICE.—The Director shall be appointed by the President, by and with the advice and consent of the Senate, and shall hold office at the pleasure of the President.

(3) PAY AND ALLOWANCES.—The Director shall be entitled to receive the same pay and allowances as are provided for level II of the Executive Schedule under section 5313 of title 5.

(d) DUTIES.—

(1) IN GENERAL.—Subject to the authority, direction, and control of the President, the Director shall—

(A) serve as the principal advisor to the President on cybersecurity policy and strategy relating to the coordination of—

(i) information security and data protection;

(ii) programs and policies intended to improve the cybersecurity posture of the United States;

(iii) efforts to understand and deter malicious cyber activity;

(iv) efforts to increase the security of information and communications technology and services and to promote national supply chain risk management and vendor security;

(v) diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace;

(vi) awareness and adoption of emerging technology that may enhance, augment, or degrade the cybersecurity posture of the United States; and

(vii) engaging in such other cybersecurity matters as the President considers appropriate;

(B) offer advice and consultation to the National Security Council and its staff, the Homeland Security Council and its staff, and relevant Federal departments and agencies, for their consideration, relating to the development and coordination of national cyber policy and strategy, including the National Cyber Strategy;

(C) lead the coordination of implementation of national cyber policy and strategy, including the National Cyber Strategy, by—

(i) in coordination with the heads of relevant Federal departments or agencies, monitoring and assessing the effectiveness, including cost-effectiveness, of the implementation of the national cyber policy and strategy by Federal departments and agencies;

(ii) making recommendations, relevant to changes in the organization, personnel, and resource allocation and to policies of Federal departments and agencies, to the heads of relevant Federal departments and agencies to implement the national cyber policy and strategy;

(iii) reviewing the annual budget proposals for relevant Federal departments and agencies and advising the heads of those departments and agencies whether the proposals are consistent with the national cyber policy and strategy;

(iv) continuously assessing and making relevant recommendations to the President on the appropriate level of integration and interoperability across the Federal cyber centers;

(v) coordinating with the Attorney General, the Federal Chief Information Officer, the Director of the Office of Management and Budget, the Director of National Intelligence,

and the Director of the Cybersecurity and Infrastructure Security Agency, on the streamlining of Federal policies and guidelines, including with respect to implementation of subchapter II of chapter 35 of title 44, and, as appropriate or applicable, regulations relating to cybersecurity;

(vi) reporting annually to the President, the Assistant to the President for National Security Affairs, and Congress on the state of the cybersecurity posture of the United States, the effectiveness of the national cyber policy and strategy, and the status of the implementation of the national cyber policy and strategy by Federal departments and agencies; and

(vii) engaging in such other activity as the President considers appropriate to further the national cyber policy and strategy;

(D) lead the coordination of the development, and ensure implementation by the Federal Government, of integrated incident response to a cyber attack or cyber campaign of significant consequence, including—

(i) ensuring and facilitating coordination among relevant Federal departments and agencies in the development of integrated operational plans, processes, and playbooks, including for incident response, that feature—

(I) clear lines of authority and lines of effort across the Federal Government;

(II) authorities that have been delegated to an appropriate level to facilitate effective operational responses across the Federal Government; and

(III) support for the integration of defensive cyber plans and capabilities with offensive cyber plans and capabilities in a manner consistent with improving the cybersecurity posture of the United States;

(ii) ensuring the exercising of defensive operational plans, processes, and playbooks for incident response;

(iii) ensuring the updating of defensive operational plans, processes, and playbooks for incident response as needed to keep them updated; and

(iv) reviewing and ensuring that defensive operational plans, processes, and playbooks improve coordination with relevant private-sector entities, as appropriate;

(E) prepare the response by the Federal Government to a cyber attack or cyber campaign of significant consequence across Fed-

eral departments and agencies with responsibilities pertaining to cybersecurity and with the relevant private-sector entities, including—

(i) developing for the approval of the President, in coordination with the Assistant to the President for National Security Affairs and the heads of relevant Federal departments and agencies, operational priorities, requirements, and plans;

(ii) ensuring incident response is executed consistent with the plans described in clause (i); and

(iii) ensuring relevant Federal department and agency consultation with relevant private-sector entities in incident response;

(F) coordinate and consult with private-sector leaders on cybersecurity and emerging technology issues in support of, and in coordination with, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the heads of other Federal departments and agencies, as appropriate;

(G) annually report to Congress on cybersecurity threats and issues facing the United States, including any new or emerging technologies that may affect national security, economic prosperity, or enforcing the rule of law; and

(H) be responsible for such other functions as the President may direct.

(2) ADDITIONAL DUTIES.—

(A) IN GENERAL.—The Director may—

(i) serve as the senior representative to any organization that the President may establish for the purpose of providing the President advice on cybersecurity; and

(ii) subject to subparagraph (B), be included as a participant in preparations for and, when appropriate, the execution of domestic and international summits and other international meetings at which cybersecurity is a major topic.

(B) COORDINATION WITH SECRETARY OF STATE.—In acting under subparagraph (A)(ii) in the case of a summit or a meeting with an international partner, the Director shall act in coordination with the Secretary of State.

(3) DELEGATION OF AUTHORITY.—The Director may—

(A) delegate any of the Director's functions, powers, and duties to such officers and employees of the Office as the Director considers appropriate; and

(B) authorize such successive redelegations of the functions, powers, and duties to such officers and employees of the Office as the Director considers appropriate.

(e) POWERS.—

(1) IN GENERAL.—The Director may, for the purposes of carrying out the functions of the Director under this section—

(A) subject to the civil service and classification laws, select, appoint, employ, and fix the compensation of such officers and employees as are necessary and prescribe their duties, except that not more than 75 individuals may be employed without regard to any provision of law regulating the employment or compensation at rates not to exceed the basic rate of basic pay payable for level IV of the Executive Schedule under section 5315 of title 5;

(B) employ experts and consultants in accordance with section 3109 of title 5, and compensate individuals so employed for each day (including travel time) at rates not in excess of the maximum rate of basic pay for grade GS–15 as provided in section 5332 of title 5, and while those experts and consultants are so serving away from their homes or regular place of business, pay those employees travel expenses and per diem in lieu of subsistence at rates authorized by section 5703 of title 5 for individuals in Federal Government service employed intermittently;

(C) accept officers or employees of the United States or members of the Armed Forces on a detail from an element of the intelligence community (as that term is defined insection 3 of the National Security Act of 1947 (50 U.S.C. 3003) or from another element of the Federal Government on a nonreimbursable basis, as jointly agreed to by the heads of the receiving and detailing elements, for a period not to exceed 3 years;

(D) promulgate such rules and regulations as may be necessary to carry out the functions, powers, and duties vested in the Director;

(E) utilize, with their consent, the services, personnel, and facilities of other Federal agencies;

(F) enter into and perform such contracts, leases, cooperative agreements, or other transactions as may be necessary in the conduct of the work of the Office and on such terms as the Director may determine appropriate, with a Federal agency, or with a public or private person or entity;

(G) accept voluntary and uncompensated services, notwithstanding the provisions of section 1342 of title 31;

(H) adopt an official seal, which shall be judicially noticed; and

(I) provide, where authorized by law, copies of documents to persons at cost, except that any funds so received shall be credited to, and be available for use from, the account from which expenditures relating to copying documents were made.

(2) RULES OF CONSTRUCTION REGARDING DETAILS.— Nothing in paragraph (1)(C) may be construed as imposing any limitation on any other authority for reimbursable or nonreimbursable details. A nonreimbursable detail made pursuant to paragraph (1)(C) shall not be considered an augmentation of the appropriations of the receiving element of the Office of the National Cyber Director.

(f) RULES OF CONSTRUCTION.—Nothing in this section may be construed as—

(1) modifying any authority or responsibility, including any operational authority or responsibility of any head of a Federal department or agency;

(2) authorizing the Director or an individual acting under the authority of the Director to interfere with or to direct a criminal or national security investigation, arrest, search, seizure, or disruption operation;

(3) amending a legal restriction that was in effect on December 31, 2020, that requires a law enforcement agency to keep confidential information learned in the course of a criminal or national security investigation;

(4) authorizing the Director or an individual acting under the authority of the Director to interfere with or to direct a military operation;

(5) authorizing the Director or an individual acting under the authority of the Director to interfere with or to direct a diplomatic or consular activity;

(6) authorizing the Director or an individual acting under the authority of the Director to interfere with or to direct an intelligence activity, resource, or operation; or

(7) authorizing the Director or an individual acting under the authority of the Director to modify the classification of intelligence information.

§ 10886. Apprehension and prosecution of international cyber criminals

(a) DEFINITION OF INTERNATIONAL CYBER CRIMINAL.—In this section, the term ''international cyber criminal'' means an individual—

(1) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or the citizens of the United States; and

(2) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a ''Red Notice'') has been circulated by Interpol.

(b) CONSULTATIONS FOR NONCOOPERATION.—The Secretary of State shall consult with the appropriate government official of each country from which extradition is not likely due to the lack of an extradition treaty with the United States or other reasons, in which 1 or more international cyber criminals are physically present, to determine what actions the government of the country has taken—

(1) to apprehend and prosecute the criminals; and

(2) to prevent the criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

(c) ANNUAL REPORT.—

(1) DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEES.—For purposes of this subsection, the term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations, the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Financial Services, the Permanent Select Committee on Intelligence, and the Committee on the Judiciary of the House of Representatives.

(2) CONTENTS.—The Secretary of State shall submit to the appropriate congressional committees an annual report that includes—

(A) the number of international cyber criminals located in other countries, disaggregated by country, and indicating from which countries extradition is not likely due to the lack of an extradition treaty with the United States or other reasons;

(B) the nature and number of significant discussions by an official of the Department of State on ways to thwart or prosecute

international cyber criminals with an official of another country, including the name of each country; and

(C) for each international cyber criminal who was extradited to the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited to the United States.

(3) FORM.—The report shall be in unclassified form to the maximum extent possible, but may include a classified annex.

§ 10887. President's Cup Cybersecurity Competition

(a) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency (in this section referred to as the ''Director'') may hold an annual cybersecurity competition to be known as the ''Department of Homeland Security Cybersecurity and Infrastructure Security Agency's President's Cup Cybersecurity Competition'' (in this section referred to as the ''competition'') for the purpose of identifying challenging and comparatively awarding prizes, including cash prizes, to the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines.

(b) ELIGIBILITY.—To be eligible to participate in the competition, an individual shall be a Federal Civilian employee or member of the uniformed services (as the term is defined in section 2101 of title 5) and shall comply with any rules promulgated by the Director regarding the competition.

(c) ADMINISTRATION.—The Director may enter into a grant, contract, cooperative agreement, or other agreement with a private sector for-profit or nonprofit entity or State or local government agency to administer the competition.

(d) PARAMETERS.—Each competition shall incorporate the following elements:

(1) Cybersecurity skills outlined in the National Institute for Cybersecurity Education Framework or any successor framework.

(2) Individual and team events.

(3) Categories demonstrating offensive and defensive cyber operations, such as software reverse engineering and software exploitation, network operations, forensics, big data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, obfuscated coding, or cyber-physical systems.

(4) Any other elements related to paragraph (1), (2), or (3) as determined necessary by the Director.

(e) USE OF FUNDS.—To further the goals and objectives of the competition, the Director may use amounts made available to the Director for the competition for reasonable expenses for the following:

(1) Advertising, marketing, and promoting the competition.

(2) Meals for participants and organizers of the competition if attendance the meal during the competition is necessary to maintain the integrity of the competition.

(3) Promotional items, including merchandise and apparel.

(4) Consistent with section 4503 of title 5, necessary expenses for the honorary recognition of competition participants, including members of the uniformed services.

(5) Monetary and nonmonetary awards for competition participants, including members of the uniformed services, subject to subsection (f).

(f) PRIZE LIMITATION.—

(1) AWARDS BY THE DIRECTOR.—The Director may make 1 or more awards per competition, except that the amount or value of each shall not exceed $10,000.

(2) AWARDS BY THE SECRETARY.—The Secretary may make 1 or more awards per competition, except that the amount or value of each shall not exceed $25,000.

(3) ADDITION TO REGULAR PAY.—A monetary award under this section shall be in addition to the regular pay of the recipient.

(4) OVERALL YEARLY AWARD LIMIT.—The total amount or value of awards made under this section during a fiscal year may not exceed $100,000.

(g) REPORTING REQUIREMENTS.—The Director shall annually provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes the following with respect to each competition conducted in the preceding year:

(1) A description of available amounts.

(2) A description of authorized expenditures.

(3) Information relating to participation.

(4) Information relating to lessons learned and how those lessons may be applied to improve cybersecurity operations and recruitment of the Cybersecurity and Infrastructure Security Agency.

§ 10888. Incentive pay for positions requiring significant cyber skills

Subject to the availability of appropriations, and in accordance with the comparable level of the General Schedule, the Attorney General and the Secretary shall provide incentive pay, in an amount that is not more than 25 percent of the basic pay of the individual, to an individual appointed to a position in the Department of Justice (including the Federal Bureau of Investigation) or the Department (including positions in Homeland Security Investigations), respectively, requiring significant cyber skills, including to aid in—-

(1) the protection of trafficking victims;

(2) the prevention of trafficking in individuals; or

(3) the prosecution of technology-facilitated crimes against children by buyers or traffickers in individuals.

Chapter 109—Science and Technology in Support of Homeland Security

Subchapter I—General

Subchapter II—Supporting Anti-Terrorism by Protecting Effective Technologies

Subchapter III—Biodefense

Subchapter I—General

§ 10901. Responsibilities and authorities of Under Secretary for Science and Technology

The Secretary, acting through the Under Secretary for Science and Technology, is responsible for—

(1) advising the Secretary regarding research and development efforts and priorities in support of the Department's missions;

(2) developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for identifying priorities, goals, objectives, and policies for, and coordinating the Federal Government's civilian efforts to identify and develop, countermeasures to chemical, biological, and other emerging terrorist threats, including the development of—

(A) comprehensive, research-based definable goals for the efforts; and

(B) annual measurable objectives and specific targets to accomplish and evaluate the goals for the efforts;

(3) supporting the Under Secretary for Intelligence and Analysis and the Director of the Cybersecurity and Infrastructure Security Agency, by assessing and testing homeland security vulnerabilities and possible threats;

(4) conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, except that the responsibility does not extend to human health-related research and development activities;

(5) establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of, technology and systems for—

(A) preventing the importation of chemical, biological, and related weapons and material; and

(B) detecting, preventing, protecting against, and responding to terrorist attacks;

(6) establishing a system for transferring homeland security developments or technologies to Federal, State, local government, and private-sector entities;

(7) entering into work agreements, joint sponsorships, contracts, or other agreements with the Department of Energy regarding the use of the national laboratories or sites, and the support of the science and technology base at those facilities;

(8) collaborating with the Secretary of Agriculture and the Attorney General as provided in section 212 of the Agricultural Bioterrorism Protection Act of 2002 (7 U.S.C. 8401);

(9) collaborating with the Secretary of Health and Human Services and the Attorney General in determining any new biological agents and toxins that shall be listed as ''select agents'' in Appendix A of part 72 of title 42, Code of Federal Regulations, pursuant to section 351A of the Public Health Service Act (42 U.S.C. 262a);

(10) supporting United States leadership in science and technology;

(11) establishing and administering the primary research and development activities of the Department, including the long-term research and development needs and capabilities for all elements of the Department;

(12) coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department;

(13) coordinating with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs; and

(14) developing and overseeing the administration of guidelines for merit review of research and development projects throughout the Department, and for the dissemination of research conducted or sponsored by the Department.

§ 10902. Functions transferred

The Secretary succeeds to the functions, personnel, assets, and liabilities of the following entities:

(1) The following programs and activities of the Department of Energy, including the functions of the Secretary of Energy relating thereto (but not including programs and activities relating to the strategic nuclear defense posture of the United States):

(A) The chemical and biological national security and supporting programs and activities of the nonproliferation and verification research and development program.

(B) The nuclear smuggling programs and activities within the proliferation detection program of the nonproliferation and verification research and development program. The programs and activities described in this subparagraph may be designated by the President either for transfer to the Department or for joint operation by the Secretary and the Secretary of Energy.

(C) The nuclear assessment program and activities of the assessment, detection, and cooperation program of the international materials protection and cooperation program.

(D) Life sciences activities of the biological and environmental research program related to microbial pathogens designated by the President for transfer to the Department.

(E) The Environmental Measurements Laboratory.

(F) The advanced scientific computing research program and activities at Lawrence Livermore National Laboratory.

(2) The National Bio-Weapons Defense Analysis Center of the Department of Defense, including the functions of the Secretary of Defense related thereto.

§ 10903. Conduct of certain public health-related activities

(a) IN GENERAL.—With respect to civilian human health-related research and development activities relating to countermeasures for chemical, biological, radiological, and nuclear and other emerging terrorist threats carried out by the Department of Health and Human Services (including the Public Health Service), the Secretary of Health and Human Services shall set priorities, goals, objectives, and policies and develop a coordinated strategy for the activities in collaboration with the Secretary of Homeland Security to ensure consistency with the national policy and strategic plan developed under section 10901 of this title.

(b) EVALUATION OF PROGRESS.—In carrying out subsection (a), the Secretary of Health and Human Services shall collaborate with the Secretary in developing specific benchmarks and outcome measurements for evaluating progress toward achieving the priorities and goals described in that subsection.

§ 10904. Federally funded research and development centers

The Secretary, acting through the Under Secretary for Science and Technology, shall have the authority to establish or contract with one or more federally funded research and development centers to provide independent analysis of homeland security issues, or to carry out other responsibilities under this subtitle, including coordinating and integrating both the extramural and intramural programs described in section 10907 of this title.

§ 10905. Miscellaneous provisions

(a) CLASSIFICATION.—To the greatest extent practicable, research conducted or supported by the Department shall be unclassified.

(b) CONSTRUCTION.—Nothing in this chapter shall be construed to preclude any Under Secretary of the Department from carrying out research, development, demonstration, or deployment activities, as long as the activities are coordinated through the Under Secretary for Science and Technology.

(c) REGULATIONS.—The Secretary, acting through the Under Secretary for Science and Technology, may issue necessary regulations with respect

to research, development, demonstration, testing, and evaluation activities of the Department, including the conducting, funding, and reviewing of the activities.

§ 10906. Homeland Security Advanced Research Projects Agency

(a) DEFINITIONS.—In this section:

(1) FUND.—The term ''Fund'' means the Acceleration Fund for Research and Development of Homeland Security Technologies established in subsection (c).

(2) HOMELAND SECURITY RESEARCH.—The term ''homeland security research'' means research relevant to the detection of, prevention of, protection against, response to, attribution of, and recovery from homeland security threats, particularly acts of terrorism.

(3) HSARPA.—The term ''HSARPA'' means the Homeland Security Advanced Research Projects Agency established in subsection (b).

(4) UNDER SECRETARY.—The term ''Under Secretary'' means the Under Secretary for Science and Technology.

(b) HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY.—

(1) ESTABLISHMENT.—There is in the Department the Homeland Security Advanced Research Projects Agency (HSARPA).

(2) DIRECTOR.—The Director is the head of HSARPA. The Director is appointed by the Secretary. The Director reports to the Under Secretary.

(3) RESPONSIBILITIES.—The Director shall administer the Fund to award competitive, merit-reviewed grants, cooperative agreements, or contracts to public or private entities, including businesses, federally funded research and development centers, and universities. The Director shall administer the Fund to—

(A) support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security;

(B) advance the development, testing and evaluation, and deployment of critical homeland security technologies;

(C) accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities; and

(D) conduct research and development for the purpose of advancing technology for the investigation of child exploitation crimes, including child victim identification, trafficking in individuals, and child pornography, and for advanced forensics.

(4) TARGETED COMPETITIONS.—The Director may solicit proposals to address specific vulnerabilities identified by the Director.

(5) COORDINATION.—The Director shall ensure that the activities of HSARPA are coordinated with those of other relevant research agencies, and may run projects jointly with other agencies.

(6) PERSONNEL.—In hiring personnel for HSARPA, the Secretary has the hiring and management authorities described in section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (Public Law 105–261, 5 U.S.C. 3104 note). The term of appointments for employees under subsection (c)(1) of that section may not exceed 5 years before the granting of an extension under subsection (c)(2) of that section.

(7) DEMONSTRATIONS.—The Director shall periodically hold homeland security technology demonstrations to improve contact among technology developers, vendors and acquisition personnel.

(c) ACCELERATION FUND.—There is in the Department the Acceleration Fund for Research and Development of Homeland Security Technologies (in this subsection referred to as the ''Acceleration Fund''). The Director administers the Acceleration Fund.

§ 10907. Conduct of research, development, demonstration, testing, and evaluation

(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall carry out the responsibilities under section 10901(4) of this title through both extramural and intramural programs.

(b) EXTRAMURAL PROGRAMS.—

(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall operate extramural research, development, demonstration, testing, and evaluation programs so as to—

(A) ensure that colleges, universities, private research institutes, and companies (and consortia thereof) from as many areas of the United States as practicable participate;

(B) ensure that the research funded is of high quality, as determined through merit review processes developed under section 10901(14) of this title; and

(C) distribute funds through grants, cooperative agreements, and contracts.

(2) UNIVERSITY-BASED CENTERS FOR HOMELAND SECURITY.—

(A) DESIGNATION.—The Secretary, acting through the Under Secretary for Science and Technology, shall designate a university-based center or several university-based centers for homeland security. The purpose of the center or these centers shall be to estab-

lish a coordinated, university-based system to enhance the Nation's homeland security.

(B) CRITERIA FOR DESIGNATION.—Criteria for the designation of colleges or universities as a center or as centers for homeland security shall include demonstrated expertise in—

(i) the training of first responders;

(ii) the response to incidents involving weapons of mass destruction and biological warfare;

(iii) emergency and diagnostic medical services;

(iv) chemical, biological, radiological, and nuclear countermeasures or detection;

(v) animal and plant health and diagnostics;

(vi) food safety;

(vii) water and wastewater operations;

(viii) port and waterway security;

(ix) multi-modal transportation;

(x) information security and information engineering;

(xi) engineering;

(xii) educational outreach and technical assistance;

(xiii) border transportation and security; and

(xiv) the public policy implications and public dissemination of homeland security related research and development;

(C) DISCRETION OF SECRETARY.—To the extent that exercising discretion is in the interest of homeland security, and with respect to the designation of any given university-based center for homeland security, the Secretary may except certain criteria as specified in subparagraph (B) and consider additional criteria beyond those specified in subparagraph (B). On designation of a university-based center for homeland security, the Secretary shall that day publish in the Federal Register the criteria that were excepted or added in the selection process and the justification for the set of criteria that were used for that designation.

(D) REPORT TO CONGRESS.—The Secretary shall report annually to Congress concerning the implementation of this section. The report shall indicate which center or centers have been designated and how the designation or designations enhance homeland security, as well as list any decisions to revoke or modify the designations.

(c) INTRAMURAL PROGRAMS.—

(1) CONSULTATION.—In carrying out the duties under section 10901 of this title, the Secretary, acting through the Under Secretary for

Science and Technology, may draw upon the expertise of any laboratory of the Federal Government, whether operated by a contractor or the Government.

(2) LABORATORIES.—The Secretary, acting through the Under Secretary for Science and Technology, may establish a headquarters laboratory for the Department at any laboratory or site and may establish additional laboratory units at other laboratories or sites.

(3) CRITERIA FOR HEADQUARTERS LABORATORY.—If the Secretary chooses to establish a headquarters laboratory under paragraph (2), the Secretary shall do the following:

(A) Establish criteria for the selection of the headquarters laboratory in consultation with the National Academy of Sciences, appropriate Federal agencies, and other experts.

(B) Publish the criteria in the Federal Register.

(C) Evaluate all appropriate laboratories or sites against the criteria.

(D) Select a laboratory or site on the basis of the criteria.

(E) Report to the appropriate congressional committees on which laboratory was selected, how the selected laboratory meets the published criteria, and what duties the headquarters laboratory shall perform.

(4) LIMITATION ON OPERATION OF LABORATORIES.—A laboratory may not begin operating as the headquarters laboratory of the Department until at least 30 days after the transmittal of the report required by paragraph (3)(E).

(d) PREFERENCE FOR UNITED STATES INDUSTRY.—

(1) DEFINITIONS.—In this subsection

(A) COUNTRY OF CONCERN.—The term ''country of concern'' means a country that—

(i) is a covered nation, as the term is defined in section 4872(d) of title 10; or

(ii) the Secretary determines is engaged in conduct that is detrimental to the national security of the United States.

(B) DOMESTIC END PRODUCT.—The term ''domestic end product'' has the meaning given the term in section 25.003 of title 48, Code of Federal Regulations, or any successor regulation.

(C) MANUFACTURED SUBSTANTIALLY IN THE UNITED STATES.—The term 'manufactured substantially in the United States'' means an item is a domestic end product.

(D) NONPROFIT ORGANIZATION; SMALL BUSINESS FIRM; SUBJECT INVENTION.—The terms ''nonprofit organization'', ''small

business firm, and ''subject invention'' have the meanings given those terms in section 201 of title 35.

(2) WAIVERS.—

(A) IN GENERAL.—Subject to subparagraph (B), in individual cases, the Secretary may waive the requirements of section 204 of title 35 on a showing by the small business firm, nonprofit organization, or assignee that reasonable but unsuccessful efforts have been made to grant licenses on similar terms to potential licensees that would be likely to manufacture substantially in the United States or that under the circumstances domestic manufacture is not commercially feasible.

(B) CONDITIONS.—

(i) BEFORE GRANT OF WAIVER.—Before granting a waiver under subparagraph (A), the Secretary shall comply with the procedures developed and implemented by the Department pursuant to section 70923(b)(2) of the Build America, Buy America Act (Public Law 117–58, div. G, title IX, subtitle A, 135 Stat. 1306).

(ii) PROHIBITION ON GRANTING CERTAIN WAIVERS.—The Secretary may not grant a waiver under subparagraph (A) if, as a result of the waiver, products embodying the applicable subject invention, or produced through the use of the applicable subject invention, would be manufactured substantially in a country of concern.

§ 10908. Utilization of Department of Energy national laboratories and sites in support of homeland security activities

(a) AUTHORITY TO UTILIZE NATIONAL LABORATORIES AND SITES.—

(1) IN GENERAL.—In carrying out the missions of the Department, the Secretary may utilize the Department of Energy national laboratories and sites through one or more of the following methods, as the Secretary considers appropriate:

(A) A joint sponsorship arrangement referred to in subsection (b).

(B) A direct contract between the Department and the applicable Department of Energy laboratory or site, subject to subsection (c).

(C) A ''work for others'' basis made available by that laboratory or site.

(D) Any other method provided by law.

(2) ACCEPTANCE AND PERFORMANCE BY LABS AND SITES.—Notwithstanding another law governing the administration, mission, use, or operations of Department of Energy national laboratories and sites, the laboratories and sites may accept and perform work for the Secretary, consistent with resources provided, and perform work on an equal basis to other missions at the laboratory and not on a noninterference basis with other missions of the laboratory or site.

(b) JOINT SPONSORSHIP ARRANGEMENTS.—

(1) LABORATORIES.—The Department may be a joint sponsor, under a multiple agency sponsorship arrangement with the Department of Energy, of one or more Department of Energy national laboratories in the performance of work.

(2) SITES.—The Department may be a joint sponsor of a Department of Energy site in the performance of work as if the site were a federally funded research and development center and the work were performed under a multiple agency sponsorship arrangement with the Department.

(3) PRIMARY SPONSOR.—The Department of Energy shall be the primary sponsor under a multiple agency sponsorship arrangement referred to in paragraph (1) or (2).

(4) LEAD AGENT.—The Secretary of Energy shall act as the lead agent in coordinating the formation and performance of a joint sponsorship arrangement under this subsection between the Department and a Department of Energy national laboratory or site.

(5) COMPLIANCE WITH FEDERAL ACQUISITION REGULATION.—Work performed by a Department of Energy national laboratory or site under a joint sponsorship arrangement under this subsection shall comply with the policy on the use of federally funded research and development centers under the Federal Acquisition Regulation.

(6) FUNDING.—The Department shall provide funds for work at the Department of Energy national laboratories or sites, as the case may be, under a joint sponsorship arrangement under this subsection under the same terms and conditions as apply to the primary sponsor of a national laboratory under section 3303(a)(1)(C) of title 41 or of a site to the extent that section applies to the site as a federally funded research and development center by reason of this subsection.

(c) SEPARATE CONTRACTING.—To the extent that programs or activities transferred by the Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2135) from the Department of Energy to the Department are being carried out through direct contracts with the operator of a national laboratory or site of the Department of Energy, the Secretary and the Sec-

retary of Energy shall ensure that direct contracts for the programs and activities between the Department and the operator are separate from the direct contracts of the Department of Energy with the operator.

(d) AUTHORITY WITH RESPECT TO COOPERATIVE RESEARCH AND DEVELOPMENT AGREEMENTS AND LICENSING AGREEMENTS.—In connection with utilization of Department of Energy national laboratories and sites under this section, the Secretary may permit the director of a national laboratory or site to enter into cooperative research and development agreements or to negotiate licensing agreements with any person, any agency or instrumentality of the United States, any unit of State or local government, and any other entity under the authority granted by section 12 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3710a). Technology may be transferred to a non-Federal party to an agreement consistent with sections 11 and 12 of that Act (15 U.S.C. 3710, 3710a).

(e) REIMBURSEMENT OF COSTS.—In the case of an activity carried out by the operator of a Department of Energy national laboratory or site in connection with the utilization of the laboratory or site under this section, the Department shall reimburse the Department of Energy for costs of the activity through a method under which the Secretary of Energy waives any requirement for the Department to pay administrative charges or personnel costs of the Department of Energy or its contractors in excess of the amount that the Secretary of Energy pays for an activity carried out by the contractor and paid for by the Department of Energy.

(f) LABORATORY-DIRECTED RESEARCH AND DEVELOPMENT BY THE DEPARTMENT OF ENERGY.—No funds authorized to be appropriated or otherwise made available to the Department in a fiscal year may be obligated or expended for laboratory directed research and development activities carried out by the Department of Energy unless the activities support the missions of the Department.

(g) OFFICE FOR NATIONAL LABORATORIES.—There is in the Directorate of Science and Technology the Office for National Laboratories. The Office is responsible for the coordination and utilization of the Department of Energy national laboratories and sites under this section in a manner to create a networked laboratory system for the purpose of supporting the missions of the Department.

(h) DEPARTMENT OF ENERGY COORDINATION ON HOMELAND SECURITY-RELATED RESEARCH.—The Secretary of Energy shall ensure that research, development, test, and evaluation activities conducted in the Department of Energy that are directly or indirectly related to homeland security are fully coordinated with the Secretary to minimize duplication of effort and maximize the effective application of Federal budget resources.

§ 10909. Transfers from and to the Department of Agriculture

(a) PLUM ISLAND ANIMAL DISEASE CENTER.—

(1) IN GENERAL.—The Secretary succeeds the Secretary of Agriculture as head of the Plum Island Animal Disease Center of the Department of Agriculture (in this section referred to as the ''Center''), including the assets and liabilities of the Center.

(2) CONTINUED DEPARTMENT OF AGRICULTURE ACCESS.—The Secretary and the Secretary of Agriculture shall enter into an agreement to ensure that the Department of Agriculture is able to carry out research, diagnostic, and other activities of the Department of Agriculture at the Center.

(3) DIRECTION OF ACTIVITIES.—The Secretary of Agriculture shall continue to direct the research, diagnostic, and other activities of the Department of Agriculture at the Center.

(4) NOTIFICATION.—At least 180 days before a change in the biosafety level at the Center, the President shall notify Congress of the change and describe the reasons for the change.

(5) DISPOSITION OF PLUM ISLAND PROPERTY AND TRANSPORTATION ASSETS.—The Administrator of General Services shall ensure that—

(A) Federal property known as Plum Island, New York, including the Orient Point facility, all real and personal property, and transportation assets that support Plum Island operations and access to Plum Island, be disposed of as a single consolidated asset; and

(B) the disposal is subject to conditions as may be necessary to protect Government interests and meet program requirements.

(b) NATIONAL BIO AND AGRO-DEFENSE FACILITY.—The Secretary shall transfer to the Secretary of Agriculture the operation of and all property required to operate the National Bio- and Agro-Defense Facility in Manhattan, Kansas.The transfer of function shall include the transfer of up to 40 full time equivalent positions, to be completed within 120 days of the effective date of the transfer of function, as jointly determined by the Secretaries.

§ 10910. Homeland Security Science and Technology Advisory Committee

(a) ESTABLISHMENT.—There is in the Department a Homeland Security Science and Technology Advisory Committee (in this section referred to as the ''Advisory Committee''). The Advisory Committee shall make recommendations with respect to the activities of the Under Secretary for

Science and Technology, including identifying research areas of potential importance to the security of the Nation.

(b) MEMBERSHIP.—

(1) APPOINTMENT.—The Advisory Committee consists of 20 members appointed by the Under Secretary for Science and Technology, including emergency first-responders or representatives of organizations or associations of emergency first-responders. The Advisory Committee also shall include representatives of citizen groups, including economically disadvantaged communities. The individuals appointed as members of the Advisory Committee—

(A) shall be eminent in fields such as emergency response, research, engineering, new product development, business, and management consulting;

(B) shall be selected solely on the basis of established records of distinguished service;

(C) shall not be employees of the Federal Government; and

(D) shall be selected to provide representation of a cross-section of the research, development, demonstration, and deployment activities supported by the Under Secretary for Science and Technology.

(2) NATIONAL RESEARCH COUNCIL.—The Under Secretary for Science and Technology may enter into an arrangement for the National Research Council to select members of the Advisory Committee, but only if the panel used by the National Research Council reflects the representation described in paragraph (1).

(c) TERMS OF OFFICE.—

(1) IN GENERAL.—Except as otherwise provided in this subsection, the term of office of each member of the Advisory Committee shall be 3 years.

(2) VACANCIES.—A member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed for the remainder of the term.

(d) ELIGIBILITY.—A person who has completed 2 consecutive full terms of service on the Advisory Committee is ineligible for appointment during the 1-year period following the expiration of the 2d term.

(e) MEETINGS.—The Advisory Committee shall meet at least quarterly at the call of the Chair or whenever one-third of the members request a meeting in writing. Each member shall be given appropriate notice of the call of each meeting, whenever possible not less than 15 days before the meeting.

(f) QUORUM.—A majority of the members of the Advisory Committee not having a conflict of interest in the matter being considered by the Advisory Committee constitutes a quorum.

(g) CONFLICT OF INTEREST RULES.—The Advisory Committee shall establish rules for determining when 1 of its members has a conflict of interest in a matter being considered by the Advisory Committee.

(h) REPORTS.—

(1) ANNUAL REPORT.—The Advisory Committee shall submit an annual report to the Under Secretary for Science and Technology for transmittal to Congress on or before January 31 each year. The report shall describe the activities and recommendations of the Advisory Committee during the previous year.

(2) ADDITIONAL REPORTS.—The Advisory Committee may submit to the Under Secretary for transmittal to Congress additional reports on specific policy matters it considers appropriate.

(i) EXEMPTION FROM SECTION 1013 OF TITLE 5.—Section 1013 of title 5 shall not apply to the Advisory Committee.

§ 10911. Technology clearinghouse to encourage and support innovative solutions to enhance homeland security

(a) ESTABLISHMENT OF PROGRAM.—The Secretary, acting through the Under Secretary for Science and Technology, shall establish and promote a program to encourage technological innovation in facilitating the mission of the Department (as described in section 10301 of this title).

(b) ELEMENTS OF PROGRAM.—The program described in subsection (a) shall include the following components:

(1) The establishment of a centralized Federal clearinghouse for information relating to technologies that would further the mission of the Department for dissemination, as appropriate, to Federal, State, and local government and private-sector entities for additional review, purchase, or use.

(2) The issuance of announcements seeking unique and innovative technologies to advance the mission of the Department.

(3) The establishment of a technical assistance team to assist in screening, as appropriate, proposals submitted to the Secretary (except as provided in subsection (c)(2)) to assess the feasibility, scientific and technical merits, and estimated cost of the proposals, as appropriate.

(4) The provision of guidance, recommendations, and technical assistance, as appropriate, to assist Federal, State, and local government and private-sector efforts to evaluate and implement the use of technologies described in paragraphs (1) and (2).

(5) The provision of information for persons seeking guidance on how to pursue proposals to develop or deploy technologies that would enhance homeland security, including information relating to Federal funding, regulation, or acquisition.

(c) MISCELLANEOUS PROVISIONS.—

(1) IN GENERAL.—Nothing in this section shall be construed as authorizing the Secretary or the technical assistance team established under subsection (b)(3) to set standards for technology to be used by the Department, another executive agency, a State or local government entity, or a private-sector entity.

(2) CERTAIN PROPOSALS.—The technical assistance team established under subsection (b)(3) shall not consider or evaluate proposals submitted in response to a solicitation for offers for a pending procurement or for a specific agency requirement.

(3) COORDINATION.—In carrying out this section, the Secretary shall coordinate with the Technical Support Working Group (organized under the April 1982 National Security Decision Directive Numbered 30).

§ 10912. Enhancement of public safety communications interoperability

(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) COORDINATION OF PUBLIC SAFETY INTEROPERABLE COMMUNICATIONS PROGRAMS.—

(1) PROGRAM.—The Secretary, in consultation with the Secretary of Commerce and the Chairman of the Federal Communications Commission, shall establish a program to enhance public safety interoperable communications at all levels of government. The program shall—

(A) establish a comprehensive national approach to achieving public safety interoperable communications;

(B) coordinate with other Federal agencies in carrying out subparagraph (A);

(C) develop, in consultation with other appropriate Federal agencies and State and local authorities, appropriate minimum capabilities for communications interoperability for Federal, State, and local public safety agencies;

(D) accelerate, in consultation with other Federal agencies, including the National Institute of Standards and Technology, the private sector, and nationally recognized standards organizations as appropriate, the development of national voluntary consensus standards for public safety interoperable communications, recognizing—

(i) the value, life cycle, and technical capabilities of existing communications infrastructure;

(ii) the need for cross-border interoperability between States and nations;

(iii) the unique needs of small, rural communities; and

(iv) the interoperability needs for daily operations and catastrophic events;

(E) encourage the development and implementation of flexible and open architectures incorporating, where possible, technologies that currently are commercially available, with appropriate levels of security, for short-term and long-term solutions to public safety communications interoperability;

(F) assist other Federal agencies in identifying priorities for research, development, testing, and evaluation with regard to public safety interoperable communications;

(G) identify priorities in the Department for research, development, and testing and evaluation with regard to public safety interoperable communications;

(H) establish coordinated guidance for Federal grant programs for public safety interoperable communications;

(I) provide technical assistance to State and local public safety agencies regarding planning, acquisition strategies, interoperability architectures, training, and other functions necessary to achieve public safety communications interoperability;

(J) develop and disseminate best practices to improve public safety communications interoperability; and

(K) develop appropriate performance measures and milestones to systematically measure the Nation's progress toward achieving public safety communications interoperability, including the development of national voluntary consensus standards.

(2) OFFICE FOR INTEROPERABILITY AND COMPATIBILITY.—

(A) ESTABLISHMENT.—The Secretary may establish an Office for Interoperability and Compatibility in the Directorate of Science and Technology to carry out this subsection.

(B) FUNCTIONS.—If the Secretary establishes an office, the Secretary shall, through the office, carry out Department responsibilities and authorities relating to the SAFECOM Program.

(c) INTERNATIONAL INTEROPERABILITY.—The President shall establish a mechanism for coordinating cross-border interoperability issues between—

(1) the United States and Canada; and

(2) the United States and Mexico.

(d) MULTIYEAR INTEROPERABILITY GRANTS.—

(1) MULTIYEAR COMMITMENTS.—In awarding grants to a State, region, local government, or Indian tribe for the purposes of enhancing interoperable communications capabilities for emergency response providers, the Secretary may commit to obligate Federal assistance beyond the current fiscal year, subject to the limitations and restrictions in this subsection.

(2) RESTRICTIONS.—

(A) TIME LIMIT.—No multiyear interoperability commitment may exceed 3 years in duration.

(B) AMOUNT OF COMMITTED FUNDS.—The total amount of assistance the Secretary has committed to obligate for a future fiscal year under paragraph (1) may not exceed $150,000,000.

(3) LETTERS OF INTENT.—

(A) ISSUANCE.—Under paragraph (1), the Secretary may issue a letter of intent to an applicant committing to obligate from future budget authority an amount, not more than the Federal Government's share of the project's cost, for an interoperability communications project (including interest costs and costs of formulating the project).

(B) SCHEDULE.—A letter of intent under this paragraph shall establish a schedule under which the Secretary will reimburse the applicant for the Federal Government's share of the project's costs, as amounts become available, if the applicant, after the Secretary issues the letter, carries out the project before receiving amounts under a grant issued by the Secretary.

(C) NOTICE TO SECRETARY.—An applicant that is issued a letter of intent under this subsection shall notify the Secretary of the applicant's intent to carry out a project pursuant to the letter before the project begins.

(D) NOTICE TO CONGRESS.—The Secretary shall transmit a written notification to Congress no later than 3 days before the issuance of a letter of intent under this section.

(E) LIMITATIONS.—A letter of intent issued under this section is not an obligation of the Government under section 1501 of title 31, and is not deemed to be an administrative commitment for financing. An obligation or administrative commitment may be made only as amounts are provided in authorization and appropriations laws.

(F) STATUTORY CONSTRUCTION.—Nothing in this subsection shall be construed—

(i) to prohibit the obligation of amounts pursuant to a letter of intent under this subsection in the same fiscal year as the letter of intent is issued; or

(ii) to apply to, or replace, Federal assistance intended for interoperable communications that is not provided pursuant to a commitment under this subsection.

(e) INTEROPERABLE COMMUNICATIONS PLANS.—An applicant requesting funding assistance from the Secretary for interoperable communications for emergency response providers shall submit an Interoperable Communications Plan to the Secretary for approval. A plan shall—

(1) describe the current state of communications interoperability in the applicable jurisdictions among Federal, State, and local emergency response providers and other relevant private resources;

(2) describe the available and planned use of the public safety frequency spectrum and of resources for interoperable communications within the jurisdictions;

(3) describe how the planned use of the spectrum and the resources for interoperable communications is compatible with surrounding capabilities and interoperable communications plans of Federal, State, and local governmental entities, military installations, foreign governments, critical infrastructure, and other relevant entities;

(4) include a 5-year plan for the dedication of Federal, State, and local government and private resources to achieve a consistent, secure, and effective interoperable communications system, including planning, system design and engineering, testing and technology development, procurement and installation, training, and operations and maintenance;

(5) describe how the 5-year plan meets or exceeds applicable standards and grant requirements established by the Secretary;

(6) include information on the governance structure used to develop the plan, including this information about all agencies and organizations that participated in developing the plan and the scope and time frame of the plan; and

(7) describe the method by which multijurisdictional, multidisciplinary input is provided from all regions of the jurisdiction, including high-threat urban areas located in the jurisdiction, and the process for continuing to incorporate input.

(f) EXPANDED REPORTING REQUIREMENT.—In addition to the committees specifically enumerated to receive reports under title XII of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 381), any report transmitted under title XII shall be transmitted to the appropriate congressional committees.

§ 10913. Office for Interoperability and Compatibility

(a) CLARIFICATION OF RESPONSIBILITIES.—The Director of the Office for Interoperability and Compatibility shall—

(1) assist the Secretary in developing and implementing the science and technology aspects of the program described in subparagraphs (D), (E), (F), and (G) of section 10912(b)(1) of this title;

(2) in coordination with the Federal Communications Commission, the National Institute of Standards and Technology, and other Federal departments and agencies with responsibility for standards, support the creation of national voluntary consensus standards for interoperable emergency communications;

(3) establish a comprehensive research, development, testing, and evaluation program for improving interoperable emergency communications;

(4) establish, in coordination with the Director for Emergency Communications, requirements for interoperable emergency communications capabilities, which shall be nonproprietary where standards for the capabilities exist, for all public safety radio and data communications systems and equipment purchased using homeland security assistance administered by the Department, excluding an alert and warning device, technology, or system;

(5) carry out the Department's responsibilities and authorities relating to research, development, testing, evaluation, or standards-related elements of the SAFECOM Program;

(6) evaluate and assess new technology in real-world environments to achieve interoperable emergency communications capabilities;

(7) encourage more efficient use of existing resources, including equipment, to achieve interoperable emergency communications capabilities;

(8) test public safety communications systems that are less prone to failure, support new nonvoice services, use the spectrum more efficiently, and cost less than existing systems;

(9) coordinate with the private sector to develop solutions to improve emergency communications capabilities and achieve interoperable emergency communications capabilities; and

(10) conduct pilot projects, in coordination with the Director for Emergency Communications, to test and demonstrate technologies, including data and video, that enhance—

(A) the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(B) interoperable emergency communications capabilities.

(b) COORDINATION.—The Director of the Office for Interoperability and Compatibility shall coordinate with the Director for Emergency Communications with respect to the SAFECOM program.

(c) SUFFICIENCY OF RESOURCES.—The Secretary shall provide the Office for Interoperability and Compatibility the resources and staff necessary to carry out the responsibilities under this section.

§ 10914. Emergency communications interoperability research and development

(a) DEFINITION OF INTEROPERABLE EMERGENCY COMMUNICATIONS.—In this section, the term ''interoperable emergency communications'' has the meaning given the term ''interoperable communications'' under section 10912(a) of this title.

(b) IN GENERAL.—The Secretary, acting though the Under Secretary for Science and Technology and the Director of the Office for Interoperability and Compatibility, shall establish a comprehensive research and development program to support and promote—

(1) the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(2) interoperable emergency communications capabilities among emergency response providers and relevant government officials, including by—

(A) supporting research on a competitive basis, including through the Directorate of Science and Technology Homeland Security Advanced Research Projects Agency; and

(B) considering the establishment of a Center of Excellence under the Department of Homeland Security Centers of Excellence Program focused on improving emergency response providers' communication capabilities.

(c) PURPOSES.—The purposes of the program established under subsection (b) include—

(1) supporting research, development, testing, and evaluation on emergency communication capabilities;

(2) understanding the strengths and weaknesses of the public safety communications systems in use;

(3) examining how current and emerging technology can make emergency response providers more effective, and how Federal, State, local, and tribal government agencies can use this technology in a coherent and cost-effective manner;

(4) investigating technologies that could lead to long-term advancements in emergency communications capabilities and supporting research on advanced technologies and potential systemic changes to dramatically improve emergency communications; and

(5) evaluating and validating advanced technology concepts, and facilitating the development and deployment of interoperable emergency communication capabilities.

§ 10915. National Biosurveillance Integration Center

(a) DEFINITIONS.—In this section:

(1) BIOLOGICAL AGENT.—The term ''biological agent'' has the meaning given the term in section 178 of title 18.

(2) BIOLOGICAL EVENT OF NATIONAL CONCERN.—The term ''biological event of national concern'' means—

(A) an act of terrorism involving a biological agent or toxin; or

(B) a naturally occurring outbreak of an infectious disease that may result in a national epidemic.

(3) HOMELAND SECURITY INFORMATION.—The term ''homeland security information'' has the meaning given the term in section 11907 of this title.

(4) MEMBER AGENCY.—The term ''Member Agency'' means any Federal department or agency that, at the discretion of the head of that department or agency, has entered into a memorandum of understanding regarding participation in the National Biosurveillance Integration Center.

(5) PRIVACY OFFICER.—The term ''Privacy Officer'' means the Privacy Officer appointed under section 10520 of this title.

(6) TOXIN.—The term ''toxin'' has the meaning given the term in section 178 of title 18.

(b) ESTABLISHMENT.—The Secretary, acting through the Assistant Secretary for the Countering Weapons of Mass Destruction Office, shall establish, operate, and maintain a National Biosurveillance Integration Center

(in this section referred to as the ''NBIC'') under an office or directorate of the Department that was in existence as of August 3, 2007. The Directing Officer is the head of the NBIC.

(c) PRIMARY MISSION.—The primary mission of the NBIC is to—

(1) enhance the capability of the Federal Government to—

(A) rapidly identify, characterize, localize, and track a biological event of national concern by integrating and analyzing data relating to human health, animal, plant, food, and environmental monitoring systems (both national and international); and

(B) disseminate alerts and other information to Member Agencies and, in coordination with (and where possible through) Member Agencies, to agencies of State, local, and tribal governments, as appropriate, to enhance the ability of the agencies to respond to a biological event of national concern; and

(2) oversee development and operation of the National Biosurveillance Integration System.

(d) REQUIREMENTS.—The NBIC shall detect, as early as possible, a biological event of national concern that presents a risk to the United States or the infrastructure or key assets of the United States, including by—

(1) consolidating data from all relevant surveillance systems maintained by Member Agencies to detect biological events of national concern across human, animal, and plant species;

(2) seeking private sources of surveillance, both foreign and domestic, when the sources would enhance coverage of critical surveillance gaps;

(3) using an information technology system that uses the best available statistical and other analytical tools to identify and characterize biological events of national concern in as close to real time as is practicable;

(4) providing the infrastructure for integration, including information technology systems and space, and support for personnel from Member Agencies with sufficient expertise to enable analysis and interpretation of data;

(5) working with Member Agencies to create information technology systems that use the minimum amount of patient data necessary and consider patient confidentiality and privacy issues at all stages of development and apprise the Privacy Officer of these efforts; and

(6) alerting Member Agencies and, in coordination with (and where possible through) Member Agencies, public health agencies of State, local, and tribal governments regarding an incident that could develop into a biological event of national concern.

(e) RESPONSIBILITIES OF DIRECTING OFFICER.—

(1) IN GENERAL.—The Directing Officer of the NBIC shall—

(A) on an ongoing basis, monitor the availability and appropriateness of surveillance systems used by the NBIC and those systems that could enhance biological situational awareness or the overall performance of the NBIC;

(B) on an ongoing basis, review and seek to improve the statistical and other analytical methods used by the NBIC;

(C) receive and consider other relevant homeland security information, as appropriate; and

(D) provide technical assistance, as appropriate, to all Federal, regional, State, local, and tribal government entities and private-sector entities that contribute data relevant to the operation of the NBIC.

(2) ASSESSMENTS.—The Directing Officer of the NBIC shall—

(A) on an ongoing basis, evaluate available data for evidence of a biological event of national concern; and

(B) integrate homeland security information with NBIC data to provide overall situational awareness and determine whether a biological event of national concern has occurred.

(3) INFORMATION SHARING.—

(A) IN GENERAL.—The Directing Officer of the NBIC shall—

(i) establish a method of real-time communication with the National Operations Center;

(ii) in the event that a biological event of national concern is detected, notify the Secretary and disseminate results of NBIC assessments relating to that biological event of national concern to appropriate Federal response entities and, in coordination with relevant Member Agencies, regional, State, local, and tribal governmental response entities in a timely manner;

(iii) provide any report on NBIC assessments to Member Agencies and, in coordination with relevant Member Agencies, an affected regional, State, local, or tribal government, and any private-sector entity considered appropriate that may enhance the mission of the Member Agencies, governments, or entities or the ability of the Nation to respond to biological events of national concern; and

(iv) share NBIC incident or situational awareness reports, and other relevant information, consistent with the information sharing environment established under section 11908 of

this title and policies, guidelines, procedures, instructions, or standards established under that section.

(B) CONSULTATION.—The Directing Officer of the NBIC shall implement the activities described in subparagraph (A) consistent with the policies, guidelines, procedures, instructions, or standards established under section 11908 of this title and in consultation with the Director of National Intelligence, the Under Secretary for Intelligence and Analysis, and other offices or agencies of the Federal Government, as appropriate.

(f) RESPONSIBILITIES OF MEMBER AGENCIES.—Each Member Agency shall—

(1) use its best efforts to integrate biosurveillance information into the NBIC, with the goal of promoting information sharing between Federal, State, local, and tribal governments to detect biological events of national concern;

(2) provide timely information to assist the NBIC in maintaining biological situational awareness for accurate detection and response purposes;

(3) enable the NBIC to receive and use biosurveillance information from Member Agencies to carry out its requirements under subsection (d);

(4) connect the biosurveillance data systems of that Member Agency to the NBIC data system under mutually agreed protocols that are consistent with subsection (d)(5);

(5) participate in the formation of strategy and policy for the operation of the NBIC and its information sharing;

(6) provide personnel to the NBIC under an interagency personnel agreement and consider the qualifications of the personnel necessary to provide human, animal, and environmental data analysis and interpretation support to the NBIC; and

(7) retain responsibility for the surveillance and intelligence systems of that department or agency, if applicable.

(g) ADMINISTRATIVE AUTHORITIES.—

(1) HIRING OF EXPERTS.—The Directing Officer of the NBIC shall hire individuals with the necessary expertise to develop and operate the NBIC.

(2) DETAIL OF PERSONNEL.—On request of the Directing Officer of the NBIC, the head of a Federal department or agency may detail, on a reimbursable basis, personnel of the department or agency to the Department to assist the NBIC in carrying out this section.

(h) NBIC INTERAGENCY WORKING GROUP.—The Directing Officer of the NBIC shall—

(1) establish an interagency working group to facilitate interagency cooperation and to advise the Directing Officer of the NBIC regarding recommendations to enhance the biosurveillance capabilities of the Department; and

(2) invite Member Agencies to serve on that working group.

(i) RELATIONSHIP TO OTHER DEPARTMENTS AND AGENCIES.—The authority of the Directing Officer of the NBIC under this section shall not affect the authority or responsibility of another department or agency of the Federal Government with respect to biosurveillance activities under a program administered by that department or agency.

§ 10916. Promoting anti-terrorism through international cooperation program

(a) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ''Director'' means the Director selected under subsection (b)(2).

(2) INTERNATIONAL COOPERATIVE ACTIVITY.—The term ''international cooperative activity'' includes—

(A) coordinated research projects, joint research projects, or joint ventures;

(B) joint studies or technical demonstrations;

(C) coordinated field exercises, scientific seminars, conferences, symposia, and workshops;

(D) training of scientists and engineers;

(E) visits and exchanges of scientists, engineers, or other appropriate personnel;

(F) exchanges or sharing of scientific and technological information; and

(G) joint use of laboratory facilities and equipment.

(b) SCIENCE AND TECHNOLOGY HOMELAND SECURITY INTERNATIONAL COOPERATIVE PROGRAMS OFFICE.—

(1) ESTABLISHMENT.—There is in the Department the Science and Technology Homeland Security International Cooperative Programs Office.

(2) DIRECTOR.—A Director is the head of the Office. The Director—

(A) shall be selected, in consultation with the Assistant Secretary for International Affairs, by and shall report to the Under Secretary for Science and Technology; and

(B) may be an officer of the Department serving in another position.

(3) RESPONSIBILITIES.—

(A) DEVELOPMENT OF MECHANISMS.—The Director is responsible for developing, in coordination with the Department of State and, as appropriate, the Department of Defense, the Department of Energy, and other Federal agencies, understandings and agreements to allow and to support international cooperative activity in support of homeland security.

(B) PRIORITIES.—The Director is responsible for developing, in coordination with the Office of International Affairs and other Federal agencies, strategic priorities for international cooperative activity for the Department in support of homeland security.

(C) ACTIVITIES.—The Director shall facilitate the planning, development, and implementation of international cooperative activity to address the strategic priorities developed under subparagraph (B) through mechanisms the Under Secretary for Science and Technology considers appropriate, including grants, cooperative agreements, or contracts to or with foreign public or private entities, governmental organizations, businesses (including small businesses and socially and economically disadvantaged small businesses (as the terms are defined in sections 3 and 8 of the Small Business Act (15 U.S.C. 632 and 637), respectively)), federally funded research and development centers, and universities.

(D) IDENTIFICATION OF PARTNERS.—The Director shall facilitate the matching of United States entities engaged in homeland security research with non-United States entities engaged in homeland security research so that they may partner in homeland security research activities.

(4) COORDINATION.—The Director shall ensure that the activities under this subsection are coordinated with the Office of International Affairs and the Department of State and, as appropriate, the Department of Defense, the Department of Energy, and other relevant Federal agencies or interagency bodies. The Director may enter into joint activities with other Federal agencies.

(c) MATCHING FUNDING.—

(1) IN GENERAL.—

(A) EQUITABILITY.—The Director shall ensure that funding and resources expended in international cooperative activity will be equitably matched by the foreign partner government or other en-

tity through direct funding, funding of complementary activities, or the provision of staff, facilities, material, or equipment.

(B) GRANT MATCHING AND REPAYMENT.—

(i) IN GENERAL.—The Secretary may require a recipient of a grant under this section—

(I) to make a matching contribution of not more than 50 percent of the total cost of the proposed project for which the grant is awarded; and

(II) to repay to the Secretary the amount of the grant (or a portion thereof), interest on the amount at an appropriate rate, and charges for administration of the grant the Secretary determines appropriate.

(ii) LIMIT ON REPAYMENT.—The Secretary may not require that repayment under clause (i)(II) be more than 150 percent of the amount of the grant, adjusted for inflation on the basis of the Consumer Price Index.

(2) FOREIGN PARTNERS.—Partners may include Israel, the United Kingdom, Canada, Australia, Singapore, and other allies in the global war on terrorism as determined to be appropriate by the Secretary and the Secretary of State.

(3) LOANS OF EQUIPMENT.—The Director may make or accept loans of equipment for research and development and comparative testing purposes.

(d) FOREIGN REIMBURSEMENTS.—If the Science and Technology Homeland Security International Cooperative Programs Office participates in an international cooperative activity with a foreign partner on a cost-sharing basis, reimbursements or contributions received from that foreign partner to meet its share of the project may be credited to appropriate current appropriations accounts of the Directorate of Science and Technology.

(e) REPORT TO CONGRESS ON INTERNATIONAL COOPERATIVE ACTIVITIES.—The Secretary, acting through the Under Secretary for Science and Technology and the Director, shall submit to Congress not later than 1 year after August 3, 2007, and every 5 years thereafter a report containing—

(1) a brief description of each grant, cooperative agreement, or contract made or entered into under subsection (b)(3)(C), including the participants, goals, and amount and sources of funding;

(2) a list of international cooperative activities underway, including the participants, goals, expected duration, and amount and sources of funding, including resources provided to support the activities in lieu of direct funding;

(3) for international cooperative activities identified in the previous reporting period, a status update on the progress of such activities, including whether goals were realized, explaining any lessons learned, and evaluating overall success; and

(4) a discussion of obstacles encountered in the course of forming, executing, or implementing agreements for international cooperative activities, including administrative, legal, or diplomatic challenges or resource constraints.

(f) ANIMAL AND ZOONOTIC DISEASES.—As part of the international cooperative activities authorized in this section, the Under Secretary for Science and Technology, in coordination with the Assistant Secretary for the Office, the Department of State, and appropriate officials of the Department of Agriculture, the Department of Defense, and the Department of Health and Human Services, may enter into cooperative activities with foreign countries, including African nations, to strengthen American preparedness against foreign animal and zoonotic diseases overseas that could harm the Nation's agricultural and public health sectors if they were to reach the United States.

(g) CYBERSECURITY.—As part of the international cooperative activities authorized in this section, the Under Secretary for Science and Technology, in coordination with the Department of State and appropriate Federal officials, may enter into cooperative research activities with Israel to strengthen preparedness against cyber threats and enhance capabilities in cybersecurity.

(h) CONSTRUCTION; AUTHORITIES OF THE SECRETARY OF STATE.—Nothing in this section shall be construed to alter or affect the following provisions of law:

(1) Section 112b(c) of title 1.

(2) Section 622(c) of the Foreign Assistance Act of 1961 (22 U.S.C. 2382(c)).

(3) Section 1(e)(2) of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a(e)(2)).

(4) Title V of the Foreign Relations Authorization Act, Fiscal Year 1979 (22 U.S.C. 2656a et seq.).

(5) Sections 2 and 27 of the Arms Export Control Act (22 U.S.C. 2752, 2767).

§ 10917. Transparency in research and development

(a) DEFINITIONS.—In this section:

(1) ALL APPROPRIATE DETAILS.—The term ''all appropriate details'' means, with respect to a research and development project—

(A) the name of the project, including classified and unclassified names if applicable;

(B) the name of the component of the Department carrying out the project;

(C) an abstract or summary of the project;

(D) funding levels for the project;

(E) project duration or timeline;

(F) the name of each contractor, grantee, or cooperative agreement partner involved in the project;

(G) expected objectives and milestones for the project; and

(H) to the maximum extent practicable, relevant literature and patents that are associated with the project.

(2) CLASSIFIED.—The term ''classified'' means anything containing—

(A) classified national security information as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 3161 note) or any successor order;

(B) Restricted Data or data that was formerly Restricted Data, as defined in section 11(y) of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y));

(C) material classified at the Sensitive Compartmented Information (SCI) level, as defined in section 309 of the Intelligence Authorization Act for Fiscal Year 2001 (50 U.S.C. 3345); or

(D) information relating to a special access program, as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 3161 note) or any successor order.

(3) CONTROLLED UNCLASSIFIED INFORMATION.—The term ''controlled unclassified information'' means information described as ''Controlled Unclassified Information'' under Executive Order 13556 (44 U.S.C. 3501 note) or any successor order.

(4) PROJECT.—The term ''project'' means a research or development project, program, or activity administered by the Department, whether ongoing, completed, or otherwise terminated.

(b) REQUIREMENT TO LIST RESEARCH AND DEVELOPMENT PROJECTS.—

(1) IN GENERAL.—The Secretary shall maintain a detailed list of the following:

(A) Each classified and unclassified research and development project, and all appropriate details for each project, including the component of the Department responsible for each project.

(B) Each task order for a federally funded research and development center not associated with a research and development project.

(C) Each task order for a university-based center of excellence not associated with a research and development project.

(D) The indicators developed and tracked by the Under Secretary for Science and Technology with respect to transitioned projects pursuant to subsection (d).

(2) EXCEPTION.—Paragraph (1) shall not apply to a project completed or otherwise terminated before December 23, 2016.

(3) UPDATES.—The list required under paragraph (1) shall be updated as frequently as possible, but not less frequently than once per quarter.

(4) PROVIDE DEFINITION OF RESEARCH AND DEVELOPMENT.—For purposes of the list required under paragraph (1), the Secretary shall provide a definition for the term ''research and development''.

(c) REPORT.—The Secretary each year shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a classified and unclassified report, as applicable, that lists each ongoing classified and unclassified project at the Department, including all appropriate details of each project.

(d) INDICATORS OF SUCCESS FOR TRANSITIONED PROJECTS.—

(1) IN GENERAL.—For each project that has been transitioned to practice from research and development, the Under Secretary for Science and Technology shall develop and track indicators to demonstrate the uptake of the technology or project among customers or end-users.

(2) PERIOD OF TRACKING.—To the fullest extent possible, the tracking of a project required under paragraph (1) shall continue for the 3-year period beginning on the date the project was transitioned to practice from research and development.

(e) LIMITATION.—Nothing in this section overrides or otherwise affects the requirements specified in section 10312 of this title.

§ 10918. EMP and GMD mitigation research and development and threat assessment, response, and recovery

(a) IN GENERAL.—In furtherance of domestic preparedness and response, the Secretary, acting through the Under Secretary for Science and Technology, and in consultation with other relevant executive agencies, relevant State, local, and tribal governments, and relevant owners and operators of

critical infrastructure, shall, to the extent practicable, conduct research and development to mitigate the consequences of threats of EMP and GMD.

(b) SCOPE.—The scope of the research and development under subsection (a) shall include the following:

(1) An objective scientific analysis evaluating the risks to critical infrastructure from a range of threats of EMP and GMD that shall—

(A) be conducted in conjunction with the Office of Intelligence and Analysis; and

(B) include a review and comparison of the range of threats and hazards facing critical infrastructure of the electrical grid.

(2) A determination of the critical utilities and national security assets and infrastructure that are at risk from EMP and GMD.

(3) An evaluation of emergency planning and response technologies that would address the findings and recommendations of experts, including those of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, which shall include a review of the feasibility of rapidly isolating 1 or more portions of the electrical grid from the main electrical grid.

(4) An analysis of technology options that are available to improve the resiliency of critical infrastructure to threats of EMP and GMD, including an analysis of neutral current blocking devices that may protect high-voltage transmission lines.

(5) The restoration and recovery capabilities of critical infrastructure under different levels of damage and disruption from various threats of EMP and GMD, as informed by the scientific analysis conducted under paragraph (1).

(6) An analysis of the feasibility of a real-time alert system to inform electoral grid operators and other stakeholders within milliseconds of a high-altitude nuclear explosion.

(c) EXEMPTION FROM DISCLOSURE.—

(1) INFORMATION SHARED WITH FEDERAL GOVERNMENT.—Section 10733 of this title, and any regulations issued pursuant to section 10733 of this title, apply to any information shared with the Federal Government under this section.

(2) INFORMATION SHARED BY FEDERAL GOVERNMENT.—Information shared by the Federal Government with a State, local, or tribal government under this section is exempt from disclosure under any provision of State, local, or tribal freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring the disclosure of information or records.

(d) THREAT ASSESSMENT, RESPONSE, AND RECOVERY.—

(1) DEFINITIONS.—In this subsection:

(A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(i) the Committee on Homeland Security and Governmental Affairs, the Committee on Armed Services, the Committee on Energy and Natural Resources, and the Committee on Commerce, Science, and Transportation of the Senate; and

(ii) the Committee on Transportation and Infrastructure, the Committee on Homeland Security, the Committee on Armed Services, the Committee on Energy and Commerce, and the Committee on Science, Space and Technology of the House of Representatives.

(B) PREPARE; PREPAREDNESS.—The terms ''prepare'' and ''preparedness'' mean the actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the homeland, including the prediction and notification of impending EMPs and GMDs.

(C) SECTOR RISK MANAGEMENT AGENCY.—The term ''Sector Risk Management Agency'' has the meaning given that term in section 10701 of this title.

(2) ROLES AND RESPONSIBILITIES.—

(A) DISTRIBUTION OF INFORMATION.—

(i) IN GENERAL.—The Secretary shall provide timely distribution of information on EMPs and GMDs to Federal, State, and local governments, owners and operators of critical infrastructure, and other persons determined appropriate by the Secretary.

(ii) BRIEFING.—The Secretary shall brief the appropriate congressional committees on the effectiveness of the distribution of information under clause (i).

(B) RESPONSE AND RECOVERY.—

(i) IN GENERAL.—The Administrator of the Federal Emergency Management Agency shall—

(I) coordinate the response to and recovery from the effects of EMPs and GMDs on critical infrastructure, in coordination with the heads of appropriate Sector Risk Management Agencies, and on matters related to the bulk power system, in consultation with the Secretary of

Energy and the Federal Energy Regulatory Commission; and

(II) to the extent practicable, incorporate events that include EMPs and extreme GMDs as a factor in preparedness scenarios and exercises.

(ii) IMPLEMENTATION.—The Administrator of the Federal Emergency Management Agency, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, and on matters related to the bulk power system, the Secretary of Energy and the Federal Energy Regulatory Commission, shall—

(I) develop plans and procedures to coordinate the response to and recovery from EMP and GMD events; and

(II) not later than December 21, 2020, conduct a national exercise to test the preparedness and response of the Nation to the effect of an EMP or extreme GMD event.

(C) RESEARCH AND DEVELOPMENT.—

(i) IN GENERAL.—The Secretary, in coordination with the heads of relevant Sector Risk Management Agencies, shall—

(I) without duplication of existing or ongoing efforts, conduct research and development to better understand and more effectively model the effects of EMPs and GMDs on critical infrastructure (which shall not include any system or infrastructure of the Department of Defense or any system or infrastructure of the Department of Energy associated with nuclear weapons activities); and

(II) develop technologies to enhance the resilience of and better protect critical infrastructure.

(ii) PLAN.—In coordination with the heads of relevant Sector Risk Management Agencies, the Secretary shall submit to the appropriate congressional committees a research and development action plan to rapidly address modeling shortfall and technology development.

(D) EMERGENCY INFORMATION SYSTEM.—

(i) IN GENERAL.—The Administrator of the Federal Emergency Management Agency, in coordination with relevant stakeholders, shall maintain a network of systems, such as the alerting capabilities of the integrated public alert and warning system authorized under section 11322 of this title,

that are capable of providing appropriate emergency information to the public before (if possible), during, and in the aftermath of an EMP or GMD.

(ii) BRIEFING.—Not later than December 21, 2020, the Administrator of the Federal Emergency Management Agency, shall brief the appropriate congressional committees regarding the maintenance of systems, including the alerting capabilities of the integrated public alert and warning system authorized under section 11322 of this title.

(E) QUADRENNIAL RISK ASSESSMENTS.—

(i) IN GENERAL.—The Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, and the Secretary of Commerce, and informed by intelligence-based threat assessments, shall conduct a quadrennial EMP and GMD risk assessment.

(ii) BRIEFINGS.—Not later than March 26, 2020, and every four years thereafter until 2032, the Secretary, the Secretary of Defense, the Secretary of Energy, and the Secretary of Commerce shall provide a briefing to the appropriate congressional committees regarding the quadrennial EMP and GMD risk assessment.

(iii) ENHANCING RESILIENCE.—The Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, the Secretary of Commerce, and the heads of other relevant Sector Risk Management Agencies, shall use the results of the quadrennial EMP and GMD risk assessments to better understand and to improve resilience to the effects of EMPs and GMDs across all critical infrastructure sectors, including coordinating the prioritization of critical infrastructure at greatest risk to the effects of EMPs and GMDs.

(3) COORDINATION.—

(A) REPORT ON TECHNOLOGICAL OPTIONS.—Not later than December 21, 2020, and every four years thereafter until 2032, the Secretary, in coordination with the Secretary of Defense, the Secretary of Energy, the heads of other appropriate agencies, and, as appropriate, private-sector partners, shall submit to the appropriate congressional committees, a report that—

(i) assesses the technological options available to improve the resilience of critical infrastructure to the effects of EMPs and GMDs; and

(ii) identifies gaps in available technologies and opportunities for technological developments to inform research and development activities.

(B) TEST DATA.—

(i) IN GENERAL.—Not later than December 20, 2020, the Secretary, in coordination with the heads of Sector Risk Management Agencies, the Secretary of Defense, and the Secretary of Energy, shall—

(I) review test data regarding the effects of EMPs and GMDs on critical infrastructure systems, networks, and assets representative of those throughout the Nation; and

(II) identify gaps in the test data.

(ii) PLAN.—Not later than 180 days after identifying gaps in test data under clause (i), the Secretary, in coordination with the heads of Sector Risk Management Agencies and in consultation with the Secretary of Defense and the Secretary of Energy, shall use the sector partnership structure identified in the National Infrastructure Protection Plan to develop an integrated cross-sector plan to address the identified gaps.

(iii) IMPLEMENTATION.—The heads of each agency identified in the plan developed under clause (ii) shall implement the plan in collaboration with the voluntary efforts of the private sector, as appropriate.

(e) CONSTRUCTION.—Nothing in this section may be construed—

(1) to affect in any manner the authority of the executive branch to implement Executive Order 13865 (March 26, 2019, 84 Fed. Reg. 12041) or any other authority existing on the day before December 20, 2019, of any other component of the Department or any other Federal department or agency, including the authority provided to the Sector Risk Management Agency specified in section 61003(c) of division F of the Fixing America's Surface Transportation Act (Public Law 114–94, 129 Stat. 1778), including the authority under section 215 of the Federal Power Act (16 U.S.C. 824o), and including the authority of independent agencies to be independent; or

(2) as diminishing or transferring any authorities vested in the Administrator of the Federal Emergency Management Agency or in the Agency prior to December 20, 2019.

§ 10919. National Urban Security Technology Laboratory

(a) DESIGNATION.—The Secretary, acting through the Under Secretary for Science and Technology, shall designate as an additional laboratory pur-

suant to the authority undersection 10907(c)(2) of this title the laboratory known, as of December 27, 2021, as the National Urban Security Technology Laboratory and transferred to the Department pursuant tosection 10902(1)(E) of this title.

(b) USES.— The National Urban Security Technology Laboratory shall be used to test and evaluate emerging technologies and conduct research and development to assist emergency response providers in preparing for, and protecting against, threats of terrorism.

(c) ACTIVITIES.—The National Urban Security Technology Laboratory shall—

(1) conduct tests, evaluations, and assessments of current and emerging technologies, including, as appropriate, the cybersecurity of technologies that can connect to the internet, for emergency response providers;

(2) act as a technical advisor to emergency response providers; and

(3) carry out other such activities as the Secretary determines appropriate.

(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed as affecting in any manner the authorities or responsibilities of the Countering Weapons of Mass Destruction Office of the Department.

§ 10920. Chemical Security Analysis Center

(a) DESIGNATION.—The Secretary, acting through the Under Secretary for Science and Technology, shall designate as an additional laboratory pursuant to the authority undersection 10907(c)(2) of this title the laboratory known, as of December 23, 2022, as the Chemical Security Analysis Center.

(b) USES.— The Chemical Security Analysis Center shall be used to conduct studies, analysis, and research to assess and address domestic chemical security events.

(c) ACTIVITIES.—Pursuant to the authority under section 10910(4) of this title, the Chemical Security Analysisi Center shall—

(1) identify and develop approaches and mitigation strategies to domestic chemical security threats, including the development of comprehensive, research-based definable goals relating to those approaches and mitigation strategies;

(2) provide an enduring science-based chemical threat and hazard analysis capability;

(3) provide expertise regarding risk and consequence modeling, chemical sensing and detection, analytical chemistry, acute chemical toxicology, synthetic chemistry and reaction characterization, and nontraditional chemical agents and emerging chemical threats;

(4) staff and operate a technical assistance program that provides operational support and subject matter expertise, design and execute laboratory and field tests, and provide a comprehensive knowledge repository of chemical threat information that is continuously updated with data from scientific intelligence, operational, and private sector sources;

(5) consult, as appropriate, with the Countering Weapons of Mass Destruction Office of the Department to mitigate, prepare for, and respond to, threats, hazards, and risks associated with domestic chemical security threats; and

(6) carry out such other activities authorized under this section as the Secretary considers appropriate.

(d) SPECIAL RULE.—Nothing in this section amends, alters, or affects—

(1) the responsibilities of the Countering Weapons of Mass Destruction Office of the Department; or

(2) the activities or requirements authorized to other entities in the Federal Government, including the activities and requirements of the Environmental Protection Agency under section 112(r) of the Clen Air Act (42 U.S.C. 7412(r)), the Toxic Substances Control Act (15 U.S.C. 2601 et seq.), and the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 (42 U.S.C. 9601 et seq.).

Subchapter II—Supporting Anti-Terrorism by Protecting Effective Technologies

§ 10931. Definitions

In this subchapter:

(1) ACT OF TERRORISM.—The term ''act of terrorism'' means an act that the Secretary determines meets all of the following requirements, as the requirements are further defined and specified by the Secretary:

(A) The act is unlawful.

(B) The act causes harm to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States.

(C) The act uses or attempts to use instrumentalities, weapons, or other methods designed or intended to cause mass destruction, injury, or other loss to citizens or institutions of the United States.

(2) INSURANCE CARRIER.—The term ''insurance carrier'' means a 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.

§ 10932. 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.

(3) Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of the anti-terrorism technology.

(4) Substantial likelihood that the anti-terrorism technology will not be deployed unless protections under the system of risk management provided under this subchapter are extended.

(5) Magnitude of risk exposure to the public if the anti-terrorism technology is not deployed.

(6) Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm.

(7) Anti-terrorism technology that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat, or respond to the acts.

(c) REGULATIONS.—The Secretary may issue regulations, after notice and comment under section 553 of title 5, necessary to carry out this subchapter.

§ 10933. Litigation management

(a) FEDERAL CAUSE OF ACTION.—

(1) IN GENERAL.—There shall exist a Federal cause of action for claims arising out of, relating to, or resulting from, an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against, in response to, or in recovery from the act, and the claims result, or may result, in loss to the Seller. The substantive law for decision in any action shall be derived from the law, including choice of law principles, of the State in which the act of terrorism occurred, unless the law is inconsistent with or preempted by Federal law. The Federal cause of action shall be brought only for claims for injuries that are proximately caused by Sellers that provide qualified anti-terrorism technology to Federal and non-Federal Government customers.

(2) JURISDICTION.—An appropriate district court of the United States shall have original and exclusive jurisdiction over all actions for any claim for loss of property, personal injury, or death arising out of, relating to, or resulting from, an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against, in response to, or in recovery from the act, and the claims result, or may result, in loss to the Seller.

(b) SPECIAL RULES.—In an action brought under this section for damages, the following provisions apply:

(1) PUNITIVE DAMAGES; INTEREST.—No punitive damages intended to punish or deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses may be awarded, nor shall any party be liable for interest prior to the judgment.

(2) NONECONOMIC DAMAGES.—

(A) DEFINITION OF NONECONOMIC DAMAGES.—In this paragraph, the term ''noneconomic damages'' means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.

(B) WHEN AWARDED.—Noneconomic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of the defendant for the harm to the plaintiff, and no plaintiff may recover noneconomic damages unless the plaintiff suffered physical harm.

(c) COLLATERAL SOURCES.—Any recovery by a plaintiff in an action under this section shall be reduced by the amount of collateral source compensation, if any, that the plaintiff has received or is entitled to receive as a result of the act of terrorism that results or may result in loss to the Seller.

(d) GOVERNMENT CONTRACTOR DEFENSE.—

(1) IN GENERAL.—Should a product liability or other lawsuit be filed for claims arising out of, relating to, or resulting from, an act of terrorism when qualified anti-terrorism technologies approved by the Secretary, as provided in paragraphs (2) and (3), have been deployed in defense against, in response to, or in recovery from the act, and the claims result, or may result, in loss to the Seller, there shall be a rebuttable presumption that the government contractor's defense applies in the lawsuit. This presumption shall only be overcome by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary's consideration of the technology under this subsection. This presumption of the government contractor's defense shall apply regardless of whether the claim against the Seller arises from a sale of the product to Federal Government or non-Federal Government customers.

(2) EXCLUSIVE RESPONSIBILITY.—The Secretary is exclusively responsible for the review and approval of anti-terrorism technology for purposes of establishing a government contractor's defense in any product liability lawsuit for claims arising out of, relating to, or resulting

from, an act of terrorism when qualified anti-terrorism technologies approved by the Secretary, as provided in this paragraph and paragraph (3), have been deployed in defense against, in response to, or in recovery from the act, and the claims result, or may result, in loss to the Seller. Upon the Seller's submission to the Secretary for approval of anti-terrorism technology, the Secretary shall conduct a comprehensive review of the design of the technology and determine whether it will perform as intended, conforms to the Seller's specifications, and is safe for use as intended. The Seller shall conduct safety and hazard analyses on the technology and shall supply the Secretary with all such information relating to the analyses.

(3) CERTIFICATE.—For anti-terrorism technology reviewed and approved by the Secretary, the Secretary shall issue a certificate of conformance to the Seller and place the anti-terrorism technology on an Approved Product List for Homeland Security.

(e) EXCLUSION.—Nothing in this section shall in any way limit the ability of any person to seek any form of recovery from any person, government, or other entity that—

(1) attempts to commit, knowingly participates in, aids and abets, or commits any act of terrorism, or any criminal act related to or resulting from the act of terrorism; or

(2) participates in a conspiracy to commit an act of terrorism or a criminal act.

§ 10934. Risk management

(a) IN GENERAL.—

(1) LIABILITY INSURANCE REQUIRED.—The Seller shall obtain liability insurance of the types and in the amounts as required under this section and certified by the Secretary to satisfy otherwise compensable third party claims arising out of, relating to, or resulting from, an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against, in response to, or in recovery from the act.

(2) MAXIMUM AMOUNT.—For the total claims related to 1 act of terrorism, the Seller is not required to obtain liability insurance of more than the maximum amount of liability insurance reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price of Seller's anti-terrorism technologies.

(3) SCOPE OF COVERAGE.—Liability insurance obtained under this subsection shall protect, in addition to the Seller, the following, to the extent of their potential liability for involvement in the manufacture, qualification, sale, use, or operation of qualified anti-terrorism tech-

nologies deployed in defense against, in response to, or in recovery from an act of terrorism:

(A) Contractors, subcontractors, suppliers, vendors and customers of the Seller.

(B) Contractors, subcontractors, suppliers, and vendors of the customer.

(4) THIRD PARTY CLAIMS.—The liability insurance under this section shall provide coverage against third party claims arising out of, relating to, or resulting from the sale or use of anti-terrorism technologies.

(b) RECIPROCAL WAIVER OF CLAIMS.—The Seller shall enter into a reciprocal waiver of claims with its contractors, subcontractors, suppliers, vendors and customers, and contractors and subcontractors of the customers, involved in the manufacture, sale, use, or operation of qualified anti-terrorism technologies, under which each party to the waiver agrees to be responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against, in response to, or in recovery from the act.

(c) EXTENT OF LIABILITY.—Notwithstanding another law, liability for all claims against a Seller arising out of, relating to, or resulting from, an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against, in response to, or in recovery from the act, and the claims result, or may result, in loss to the Seller, whether for compensatory or punitive damages or for contribution or indemnity, shall not be in an amount greater than the limits of liability insurance coverage required to be maintained by the Seller under this section.

Subchapter III—Biodefense

§ 10941. National biodefense strategy and implementation plan

(a) DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEE.—In this section, the term ''appropriate congressional committee'' means the following:

(1) The Committees on Armed Services and Appropriations of the House of Representatives and the Senate.

(2) The Committee on Energy and Commerce of the House of Representatives and the Committee on Health, Education, Labor, and Pensions of the Senate.

(3) The Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(4) The Committee on Agriculture of the House of Representatives and the Committee on Agriculture, Nutrition, and Forestry of the Senate.

(b) STRATEGY AND IMPLEMENTATION PLAN.—The Secretary and the Secretaries of Defense, Health and Human Services, and Agriculture jointly shall develop a national biodefense strategy and associated implementation plan, which shall include a review and assessment of biodefense policies, practices, programs, and initiatives. The Secretaries shall review and, as appropriate, revise the strategy biennially.

(c) ELEMENTS OF STRATEGY AND PLAN.—The strategy and associated implementation plan required under subsection (b) shall include each of the following:

(1) An inventory and assessment of all existing strategies, plans, policies, laws, and interagency agreements relating to biodefense, including prevention, deterrence, preparedness, detection, response, attribution, recovery, and mitigation.

(2) A description of the biological threats, including biological warfare, bioterrorism, naturally occurring infectious diseases, and accidental exposures.

(3) A description of the current program, efforts, or activities of the United States Government with respect to preventing the acquisition, proliferation, and use of a biological weapon, preventing an accidental or naturally occurring biological outbreak, and mitigating the effects of a biological epidemic.

(4) A description of the roles and responsibilities of the executive agencies, including internal and external coordination procedures, in identifying and sharing information relating to, warning of, and protecting against, acts of terrorism using biological agents and weapons and accidental or naturally occurring biological outbreaks.

(5) An articulation of related or required interagency capabilities and whole-of-Government activities required to support the national biodefense strategy.

(6) Recommendations for strengthening and improving the current biodefense capabilities, authorities, and command structure of the United States Government.

(7) Recommendations for improving and formalizing interagency coordination and support mechanisms with respect to providing a robust national biodefense.

(8) Any other matters the Secretary and the Secretaries of Defense, Health and Human Services, and Agriculture determine necessary.

(d) SUBMITTAL TO CONGRESS.—The Secretary and the Secretaries of Defense, Health and Human Services, and Agriculture shall submit to the appropriate congressional committees the strategy and associated implementation plan required by subsection (b). The strategy and implementation plan shall be submitted in unclassified form but may include a classified annex.

(e) BRIEFINGS.—Not later than March 1, 2021, and annually thereafter until March 1, 2025, the Secretary and the Secretaries of Defense, Health and Human Services, and Agriculture shall provide to the Committees on Armed Services, Energy and Commerce, Homeland Security, and Agriculture of the House of Representatives a joint briefing on the strategy developed under subsection (b) and the status of the implementation of the strategy.

(f) COMPTROLLER GENERAL REVIEW.—Not later than 180 days after the date of the submittal of the strategy and implementation plan under subsection (d), the Comptroller General shall conduct a review of the strategy and implementation plan to analyze gaps and resources mapped against the requirements of the national biodefense strategy and existing United States biodefense policy documents.

§ 10942. Update of national biodefense implementation plan

(a) DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, the term ''appropriate congressional committees'' means the following:

(1) The Committees on Armed Services of the House of Representatives and the Senate.

(2) The Committee on Energy and Commerce of the House of Representatives and the Committee on Health, Education, Labor, and Pensions of the Senate.

(3) The Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(4) The Committee on Agriculture of the House of Representatives and the Committee on Agriculture, Nutrition, and Forestry of the Senate.

(5) The Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

(6) The Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate.

(b) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to alter, limit, or duplicate the roles, responsibilities, authorities, or current activities, as established in statute or otherwise through existing practice or policy, of each Federal department or agency with responsibilities for biodefense or otherwise relevant to implementation of the national biodefense strategy.

(c) UPDATED BIODEFENSE THREAT ASSESSMENT.—

(1) IN GENERAL.—The Secretary and the Secretaries of Health and Human Services, Defense, and Agriculture shall jointly, and in consultation with the Director of National Intelligence, and other agency heads as appropriate—

(A) conduct an assessment of current and potential biological threats against the United States, both naturally occurring and man-made, either accidental or deliberate, including the potential for catastrophic biological threats, such as a pandemic;

(B) not later than 1 year after January 1, 2021, submit the findings of the assessment conducted under subparagraph (A) to the Federal officials described in subsection (d)(1) and the appropriate congressional committees;

(C) not later than 30 days after the date on which the assessment is submitted under subparagraph (B), conduct a briefing for the appropriate congressional committees on the findings of the assessment;

(D) update the assessment under subparagraph (A) biennially, as appropriate, and provide the findings of the updated assessments to the Federal officials described in this paragraph and the appropriate congressional committees; and

(E) conduct briefings for the appropriate congressional committees as needed any time an assessment under this paragraph is updated.

(2) CLASSIFICATION AND FORMAT.—Assessments under paragraph (1) shall be submitted in an unclassified format and include a classified annex, as appropriate.

(d) UPDATED NATIONAL BIODEFENSE IMPLEMENTATION PLAN.—The Secretary, the Secretaries of Health and Human Services, Defense, and Agriculture, and all other departments and agencies with responsibilities for biodefense, such as the Department of State, in consultation with the Assistant to the President for National Security Affairs and the Director of the Office of Management and Budget, as appropriate, shall jointly, after reviewing the biodefense threat assessment described in subsection (c) and any relevant input from external stakeholders, as appropriate, update the

national biodefense implementation plan developed under section 10941 of this title to clearly document established processes, roles, and responsibilities related to the national biodefense strategy.

(e) SPECIFIC UPDATES.—The updated national biodefense implementation plan shall—

(1) describe the roles and responsibilities of the Federal departments and agencies, including internal and external coordination procedures, in identifying and sharing information between and among Federal departments and agencies, as described in section 10941(c)(4) of this title and consistent with the statutory roles and authorities of those departments and agencies;

(2) describe roles, responsibilities, and processes for decision-making, including decisions regarding use of resources for effective risk management across the enterprise;

(3) describe resource plans for each department and agency with responsibility for biodefense to support implementation of the strategy within the jurisdiction of the department or agency, including for the biodefense coordination team, as appropriate;

(4) describe guidance and methods for analyzing the data collected from agencies to include non-Federal resources and capabilities to the extent practicable; and

(5) describe and update, as appropriate, short-, medium-, and long-term goals for executing the national biodefense strategy and metrics for meeting each objective of the strategy.

(f) SUBMITTAL TO CONGRESS.—The Secretary and the Secretary of Health and Human Services, the Secretary of Defense, and the Secretary of Agriculture shall, not later than 6 months after the date of the completion of the assessment in subsection (c)(1)(A), submit the updated national biodefense implementation plan to the appropriate congressional committees.

§ 10943. Biodefense analysis and budget submission

(a) ANNUAL ANALYSIS.—For each fiscal year, beginning in fiscal year 2023, the Director of the Office of Management and Budget, in consultation with the Secretary of Health and Human Services, shall—

(1) conduct a detailed and comprehensive analysis of Federal biodefense programs; and

(2) develop an integrated biodefense budget submission.

(b) DEVELOPMENT OF DEFINITION OF BIODEFENSE.—In accordance with the national biodefense strategy, the Director of the Office of Management and Budget shall develop and disseminate to all Federal departments and agencies a unified definition of the term ''biodefense'' to identify which

programs and activities are included in the annual budget submission required under subsection (a).

(c) REQUIREMENTS FOR ANALYSIS.—The analysis required under subsection (a) shall include—

(1) the display of all funds requested for biodefense activities, both mandatory and discretionary, by agency and categorized by biodefense enterprise element, such as threat awareness, prevention, deterrence, preparedness, surveillance and detection, response, attribution (including bioforensic capabilities), recovery, and mitigation; and

(2) detailed explanations of how each program and activity included aligns with biodefense goals and objectives as part of the national biodefense strategy required under section 10941 of this title.

(d) SUBMITTAL TO CONGRESS.—The Director of the Office of Management and Budget, in consultation with the Secretary of Health and Human Services, shall submit to Congress the analysis required under subsection (a) for a fiscal year concurrently with the President's annual budget request for that fiscal year.

Chapter 111—Border Security

Subchapter I—Border Security Responsibilities and Functions

§ 11101. Secretary

(a) IN GENERAL.—The Secretary is responsible for the following:

(1) Preventing the entry of terrorists and the instruments of terrorism into the United States.

(2) Securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States, including managing and coordinating those functions transferred to the Department at ports of entry.

(3) Carrying out the immigration enforcement functions vested by statute in, or performed by, the Commissioner of Immigration and Naturalization (or an officer, employee, or component of the Immigration and Naturalization Service) immediately before the date on which the transfer of functions specified under section 11151 of this title takes effect.

(4) Establishing and administering rules, under section 11212 of this title, governing the granting of visas or other forms of permission, including parole, to enter the United States to individuals who are not citizens or aliens lawfully admitted for permanent residence in the United States.

(5) Establishing national immigration enforcement policies and priorities.

(6) Except as provided in sections 11211 through 11215 of this title, administering the customs laws of the United States.

(7) Conducting the inspection and related administrative functions of the Department of Agriculture transferred to the Secretary under subsection (b)(2).

(8) In carrying out the foregoing responsibilities, ensuring the speedy, orderly, and efficient flow of lawful traffic and commerce.

(b) FUNCTIONS TRANSFERRED.—

(1) IN GENERAL.—The Secretary succeeds to the functions, personnel, assets, and liabilities of—

(A) the United States Customs Service of the Department of the Treasury, including the functions of the Secretary of the Treasury relating thereto;

(B) the Transportation Security Administration of the Department of Transportation, including the functions of the Secretary of Transportation, and of the Under Secretary of Transportation for Security, relating thereto;

(C) the Federal Protective Service of the General Services Administration, including the functions of the Administrator of General Services relating thereto;

(D) the Federal Law Enforcement Training Center of the Department of the Treasury; and

(E) the Office for Domestic Preparedness of the Office of Justice Programs, including the functions of the Attorney General relating thereto.

(2) CERTAIN AGRICULTURAL INSPECTION FUNCTIONS OF THE DEPARTMENT OF AGRICULTURE.—

(A) EXCLUSION OF QUARANTINE ACTIVITIES.—In this section, the term ''functions'' does not include quarantine activities carried out under the laws specified in subparagraph (B).

(B) TRANSFER OF AGRICULTURAL IMPORT AND ENTRY INSPECTION FUNCTIONS.—The Secretary succeeds to the functions of the Secretary of Agriculture relating to agricultural import and entry inspection activities under the following laws:

(i) Section 1 of the Act of August 31, 1922 (known as the Honeybee Act) (7 U.S.C. 281).

(ii) Title III of the Federal Seed Act (7 U.S.C. 1581 et seq.).

(iii) The Plant Protection Act (7 U.S.C. 7701 et seq.).

(iv) The Animal Health Protection Act (7 U.S.C. 8301 et seq.).

(v) Section 11 of the Endangered Species Act of 1973 (16 U.S.C. 1540).

(vi) The Lacey Act Amendments of 1981 (16 U.S.C. 3371 et seq.).

(vii) The 8th paragraph under the heading ''Bureau of Animal Industry'' in the Act of March 4, 1913 (known as the Virus-Serum-Toxin Act) (21 U.S.C. 151 et seq.).

(C) EFFECT OF TRANSFER.—

(i) COMPLIANCE WITH DEPARTMENT OF AGRICULTURE REGULATIONS.—The authority transferred under subparagraph (B) shall be exercised by the Secretary in accordance with the regulations, policies, and procedures issued by the Secretary of Agriculture regarding the administration of the laws specified in subparagraph (B).

(ii) RULEMAKING COORDINATION.—The Secretary of Agriculture shall coordinate with the Secretary when the Secretary of Agriculture prescribes regulations, policies, or procedures for administering the functions transferred under subparagraph (B) under a law specified in subparagraph (B).

(iii) EFFECTIVE ADMINISTRATION.—The Secretary, in consultation with the Secretary of Agriculture, may issue directives and guidelines necessary to ensure the effective use of personnel of the Department to carry out the functions transferred under subparagraph (B).

(D) PERIODIC TRANSFER OF FUNDS TO DEPARTMENT.—Out of funds collected by fees authorized under sections 2508 and 2509 of the Food, Agriculture, Conservation, and Trade Act of 1990 (21 U.S.C. 136, 136a), the Secretary of Agriculture shall transfer, from time to time to the Secretary, funds for activities carried out by the Secretary for which fees were collected. The proportion of fees collected that are transferred to the Secretary under this subparagraph may not exceed the proportion of costs incurred by the Secretary to all costs incurred to carry out activities funded by the fees.

§ 11102. Commissioner of U.S. Customs and Border Protection

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

(b) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection (in this section referred to as the ''Commissioner'') shall—

(1) coordinate and integrate the security, trade facilitation, and trade enforcement functions of U.S. Customs and Border Protection;

(2) ensure the interdiction of individuals and goods illegally entering or exiting the United States;

(3) facilitate and expedite the flow of legitimate travelers and trade;

(4) direct and administer the commercial operations of U.S. Customs and Border Protection and the enforcement of the customs and trade laws of the United States;

(5) detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other individuals who may undermine the security of the United States, in cases in which the individuals are entering, or have recently entered, the United States;

(6) safeguard the borders of the United States to protect against the entry of dangerous goods;

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

(8) in coordination with U.S. Immigration and Customs Enforcement and United States Citizenship and Immigration Services, enforce and administer all immigration laws, as the term is defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)), including—

(A) the inspection, processing, and admission of individuals who seek to enter or depart the United States; and

(B) the detection, interdiction, removal, departure from the United States, short-term detention, and transfer of individuals unlawfully entering, or who have recently unlawfully entered, the United States;

(9) develop and implement screening and targeting capabilities, including the screening, reviewing, identifying, and prioritizing of passengers and cargo across all international modes of transportation, both inbound and outbound;

(10) in coordination with the Secretary, deploy technology to collect the data necessary for the Secretary to administer the biometric entry and exit data system pursuant to section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (8 U.S.C. 1365b);

(11) enforce and administer the laws relating to agricultural import and entry inspection referred to in section 11101(b)(2) of this title;

(12) in coordination with the Under Secretary for Management of the Department, ensure U.S. Customs and Border Protection complies with Federal law, the Federal Acquisition Regulation, and the Depart-

ment's acquisition management directives for major acquisition programs of U.S. Customs and Border Protection;

(13) ensure that the policies and regulations of U.S. Customs and Border Protection are consistent with the obligations of the United States pursuant to international agreements;

(14) enforce and administer—

(A) the Container Security Initiative program under section 30505 of this title; and

(B) the Customs-Trade Partnership Against Terrorism program under subchapter II of chapter 305 of this title;

(15) conduct polygraph examinations in accordance with section 11113(a)(1) of this title;

(16) establish the standard operating procedures described in subsection (c);

(17) carry out the training required under subsection (d);

(18) carry out section 11118 of this title relating to the issuance of Asia-Pacific Economic Cooperation Business Travel Cards; and

(19) carry out other duties and powers prescribed by law or delegated by the Secretary.

(c) STANDARD OPERATING PROCEDURES.—

(1) IN GENERAL.—The Commissioner shall establish—

(A) standard operating procedures for searching, reviewing, retaining, and sharing information contained in communication, electronic, or digital devices encountered by U.S. Customs and Border Protection personnel at United States ports of entry;

(B) standard use of force procedures that officers and agents of U.S. Customs and Border Protection may employ in the execution of their duties, including the use of deadly force;

(C) a uniform, standardized, and publicly available procedure for processing and investigating complaints against officers, agents, and employees of U.S. Customs and Border Protection for violations of professional conduct, including the timely disposition of complaints and a written notification to the complainant of the status or outcome, as appropriate, of the related investigation, in accordance with section 552a of title 5 (known as the Privacy Act of 1974);

(D) an internal, uniform reporting mechanism regarding incidents involving the use of deadly force by an officer or agent of U.S. Customs and Border Protection, including an evaluation of the degree to which the procedures required under subparagraph (B) were followed; and

(E) standard operating procedures, acting through the Assistant Commissioner for Air and Marine Operations and in coordination with the Office for Civil Rights and Civil Liberties and the Office of Privacy of the Department, to provide command, control, communication, surveillance, and reconnaissance assistance through the use of unmanned aerial systems, including the establishment of—

(i) a process for other Federal, State, and local law enforcement agencies to submit mission requests;

(ii) a formal procedure to determine whether to approve or deny a mission request;

(iii) a formal procedure to determine how mission requests are prioritized and coordinated; and

(iv) a process regarding the protection and privacy of data and images collected by U.S. Customs and Border Protection through the use of unmanned aerial systems.

(2) REQUIREMENTS REGARDING CERTAIN NOTIFICATIONS.—The standard operating procedures established pursuant to paragraph (1)(A) shall require—

(A) in the case of a search of information conducted on an electronic device by U.S. Customs and Border Protection personnel, the Commissioner to notify the individual subject to the search of the purpose and authority for the search and how the individual may obtain information on reporting concerns about the search; and

(B) in the case of information collected by U.S. Customs and Border Protection through a search of an electronic device, if the information is transmitted to another Federal agency for subject matter assistance, translation, or decryption, the Commissioner to notify the individual subject to the search of the transmission.

(3) EXCEPTIONS.—The Commissioner may withhold the notifications required under paragraphs (1)(C) and (2) if the Commissioner determines, in the sole and unreviewable discretion of the Commissioner, that the notifications would impair national security, law enforcement, or other operational interests.

(4) UPDATE AND REVIEW.—The Commissioner shall review and update every 3 years the standard operating procedures required under this subsection.

(5) AUDITS.—The Inspector General of the Department shall develop and annually administer, during 2017, 2018, and 2019, an auditing mechanism to review whether searches of electronic devices at or

between United States ports of entry are being conducted in conformity with the standard operating procedures required under paragraph (1)(A). Audits shall be submitted to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate and shall include the following:

(A) A description of the activities of officers and agents of U.S. Customs and Border Protection with respect to the searches.

(B) The number of searches.

(C) The number of instances in which information contained in devices that were subjected to searches was retained, copied, shared, or entered in an electronic database.

(D) The number of devices detained as the result of searches.

(E) The number of instances in which information collected from a device that was subjected to searches was transmitted to another Federal agency, including whether the transmission resulted in a prosecution or conviction.

(6) REQUIREMENTS REGARDING OTHER NOTIFICATIONS.—The standard operating procedures established pursuant to paragraph (1)(B) shall require—

(A) in the case of an incident of the use of deadly force by U.S. Customs and Border Protection personnel, the Commissioner to notify the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Commissioner to provide to those committees a copy of the evaluation pursuant to paragraph (1)(D) not later than 30 days after completion of the evaluation.

(7) REPORT ON UNMANNED AERIAL SYSTEMS.—The Commissioner shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, during 2017, 2018, and 2019, an annual report that reviews whether the use of unmanned aerial systems is being conducted in conformity with the standard operating procedures required under paragraph (1)(E). The report—

(A) shall be submitted with the President's annual budget;

(B) may be submitted in classified form if the Commissioner determines that it is appropriate; and

(C) shall include—

(i) a detailed description of how, where, and for how long data and images collected through the use of unmanned aerial

systems by U.S. Customs and Border Protection are collected and stored; and

(ii) a list of Federal, State, and local law enforcement agencies that submitted mission requests in the previous year and the disposition of the requests.

(d) TRAINING.—The Commissioner shall require all officers and agents of U.S. Customs and Border Protection to participate in a specified amount of continuing education (to be determined by the Commissioner) to maintain an understanding of Federal legal rulings, court decisions, and departmental policies, procedures, and guidelines.

(e) SHORT-TERM DETENTION STANDARDS.—

(1) DEFINITION OF SHORT-TERM DETENTION.—In this subsection, the term ''short-term detention'' means detention in a U.S. Customs and Border Protection processing center for 72 hours or less, before repatriation to a country of nationality or last habitual residence.

(2) ACCESS TO FOOD AND WATER.—The Commissioner shall make every effort to ensure that adequate access to food and water is provided to an individual apprehended and detained at or between a United States port of entry as soon as practicable following the time of the apprehension or during subsequent short-term detention.

(3) ACCESS TO INFORMATION ON DETAINEE RIGHTS AT BORDER PATROL PROCESSING CENTERS.—

(A) IN GENERAL.—The Commissioner shall ensure that an individual apprehended by a U.S. Border Patrol agent or an Office of Field Operations officer is provided with information concerning the individual's rights, including the right to contact a representative of the individual's government for purposes of United States treaty obligations.

(B) HOW INFORMATION IS TO BE PROVIDED.—The information referred to in subparagraph (A) may be provided either orally or in writing and shall be posted in the detention holding cell in which the individual is being held. The information shall be provided in a language understandable to the individual.

(4) DAYTIME REPATRIATION.—When practicable, repatriations shall be limited to daylight hours and avoid locations that are determined to have high indices of crime and violence.

(5) REPORT ON PROCUREMENT PROCESS AND STANDARDS.—Not later than 180 days after February 24, 2016, the Comptroller General shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the procurement process and

standards of entities with which U.S. Customs and Border Protection has contracts for the transportation and detention of individuals apprehended by agents or officers of U.S. Customs and Border Protection. The report should also consider the operational efficiency of contracting the transportation and detention of those individuals.

(6) REPORT ON INSPECTIONS OF SHORT-TERM CUSTODY FACILITIES.—The Commissioner shall—

(A) annually inspect all facilities utilized for short-term detention; and

(B) make publicly available information collected pursuant to the inspections, including information regarding the requirements under paragraphs (2) and (3), and, where appropriate, issue recommendations to improve the conditions of the facilities.

(f) WAIT TIMES TRANSPARENCY.—

(1) IN GENERAL.—The Commissioner shall—

(A) publish live wait times at the 20 United States airports that support the highest volume of international travel (as determined by available Federal flight data);

(B) make information about the wait times available to the public in real time through the U.S. Customs and Border Protection website;

(C) submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, during 2017, 2018, 2019, 2020, and 2021, a report that includes compilations of all those wait times and a ranking of those United States airports by wait times; and

(D) provide adequate staffing at the U.S. Customs and Border Protection information center to ensure timely access for travelers attempting to submit comments or speak with a representative about their entry experiences.

(2) CALCULATION.—The wait times referred to in paragraph (1)(A) shall be determined by calculating the time elapsed between an individual's entry into the U.S. Customs and Border Protection inspection area and the individual's clearance by a U.S. Customs and Border Protection officer.

(g) CONTINUED SUBMISSION OF REPORTS TO COMMITTEES.—The Commissioner shall continue to submit to the Committee on Homeland Security and the Committee on Ways and Means of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and

the Committee on Finance of the Senate any report required to be submitted on February 23, 2016, under any provision of law.

(h) AUTHORITY OF OTHER FEDERAL AGENCIES NOT AFFECTED.—Nothing in this section may be construed as affecting in any manner the authority, which existed on February 23, 2016, of any other Federal agency or component of the Department.

§ 11103. Limitation on reorganization of functions and units

The authority provided by section 1502 of the Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2308) may be used to reorganize functions or organizational units in U.S. Immigration and Customs Enforcement or U. S. Citizenship and Immigration Services, but may not be used to recombine U.S. Immigration and Customs Enforcement and U.S. Citizenship and Immigration Services into a single agency or otherwise to combine, join, or consolidate functions or organizational units of U.S. Immigration and Customs Enforcement and U.S. Citizenship and Immigration Services with each other.

§ 11104. Employee discipline

Notwithstanding another law, the Secretary may impose disciplinary action on an employee of U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection who willfully deceives Congress or agency leadership on any matter.

Subchapter II—Customs and Border Protection

Part A—In General

§ 11111. Separate budget request for U.S. Customs and Border Protection

(a) IN GENERAL.—The President shall include in each budget transmitted to Congress under section 1105 of title 31 a separate budget request for U.S. Customs and Border Protection.

(b) FIVE-YEAR PLAN FOR LAND BORDER PORT OF ENTRY PROJECTS.—The annual budget submission of U. S. Customs and Border Protection for ''Construction and Facilities Management'' shall, in consultation with the General Services Administration, include a detailed 5-year plan for all Federal land border port-of-entry projects, with a yearly update of total projected future funding needs delineated by Federal land border port of entry.

§ 11112. Allocation of resources by the Secretary

(a) DEFINITION OF CUSTOMS REVENUE SERVICES.—In this section, the term ''customs revenue services'' means those customs revenue functions described in section 11131(1) through (6) and (8) of this title.

(b) IN GENERAL.—The Secretary shall ensure that adequate staffing is provided to ensure that levels of customs revenue services provided on January 23, 2003, shall continue to be provided.

(c) NOTIFICATION OF CONGRESS.—The Secretary shall notify the Committee on Ways and Means of the House of Representatives and the Committee on Finance of the Senate at least 90 days prior to taking an action that would—

(1) result in a significant reduction in customs revenue services, including hours of operation, provided at an office within the Department or a port of entry;

(2) eliminate or relocate an office of the Department that provides customs revenue services; or

(3) eliminate a port of entry.

§ 11113. Polygraph and background examinations for law enforcement personnel of U.S. Customs and Border Protection

(a) IN GENERAL.—The Secretary shall ensure that—

(1) all applicants for law enforcement positions with U.S. Customs and Border Protection (except as provided in subsection (b)) receive polygraph examinations before being hired for a position; and

(2) U.S. Customs and Border Protection initiates all periodic background reinvestigations for all law enforcement personnel of U.S. Customs and Border Protection who should receive periodic background reinvestigations pursuant to relevant policies of U.S. Customs and Border Protection in effect on January 3, 2011.

(b) WAIVER.—The Commissioner of U.S. Customs and Border Protection may waive the polygraph examination requirement under subsection (a)(1) for any applicant who—

(1) is considered suitable for employment;

(2) holds a current, active Top Secret/Sensitive Compartmented Information Clearance;

(3) has a current Single Scope Background Investigation;

(4) was not granted any waivers to obtain his or her clearance; and

(5) is a veteran (as defined in section 2108 of title 5).

§ 11114. Fees authorized for Advanced Training Center

U.S. Customs and Border Protection's Advanced Training Center may charge fees for a service and/or thing of value it provides to Federal Government or non-government entities or individuals, so long as the fees charged do not exceed the full costs associated with the service or thing of value provided. Notwithstanding 31 U.S.C. 3302(b), fees collected by the Advanced Training Center—

(1) shall be deposited in a separate account entitled ''Advanced Training Center Revolving Fund'';

(2) shall be available, without further appropriations, for necessary expenses of the Advanced Training Center program; and

(3) shall remain available until expended.

§ 11115. Border security metrics

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

(B) the Committee on Homeland Security of the House of Representatives.

(2) CONSEQUENCE DELIVERY SYSTEM.—The term ''Consequence Delivery System'' means the series of consequences applied by the U.S. Border Patrol in collaboration with other Federal agencies to individuals unlawfully entering the United States, to prevent unlawful border crossing recidivism.

(3) GOT AWAY.—The term ''got away'' means an unlawful border crosser who—

(A) is directly or indirectly observed making an unlawful entry into the United States;

(B) is not apprehended; and

(C) is not a turn back.

(4) KNOWN MARITIME MIGRANT FLOW.—The term ''known maritime migrant flow'' means the sum of the number of undocumented migrants—

(A) interdicted in the waters over which the United States has jurisdiction;

(B) identified at sea either directly or indirectly, but not interdicted; or

(C) if not described in subparagraph (A) or (B), who were otherwise reported, with a significant degree of certainty, as having entered, or attempted to enter, the United States through the maritime border.

(5) MAJOR VIOLATOR.—The term ''major violator'' means a person or entity that has engaged in serious criminal activities at any land, air, or sea port of entry, including the following:

(A) Possession of illicit drugs.

(B) Smuggling of prohibited products.

(C) Human smuggling.

(D) Possession of illegal weapons.

(E) Use of fraudulent documents.

(F) Any other offense that is serious enough to result in an arrest.

(6) SITUATIONAL AWARENESS.—The term ''situational awareness'' means knowledge and understanding of current unlawful cross-border activity, including the following:

(A) Threats and trends concerning illicit trafficking and unlawful crossings.

(B) The ability to forecast future shifts in those threats and trends.

(C) The ability to evaluate those threats and trends at a level sufficient to create actionable plans.

(D) The operational capability to conduct persistent and integrated surveillance of the international borders of the United States.

(7) TRANSIT ZONE.—The term ''transit zone'' means the sea corridors of the western Atlantic Ocean, the Gulf of Mexico, the Caribbean Sea, and the eastern Pacific Ocean through which undocumented migrants and illicit drugs transit, either directly or indirectly, to the United States.

(8) TURN BACK.—The term ''turn back'' means an unlawful border crosser who, after making an unlawful entry into the United States, responds to United States enforcement efforts by returning promptly to the country from which the crosser entered.

(9) UNLAWFUL BORDER CROSSING EFFECTIVENESS RATE.—The term ''unlawful border crossing effectiveness rate'' means the percentage that results from dividing the number of apprehensions and turn backs by the sum of the number of apprehensions, estimated undetected unlawful entries, turn backs, and got aways.

(10) UNLAWFUL ENTRY.—The term ''unlawful entry'' means an unlawful border crosser who enters the United States and is not apprehended by a border security component of the Department.

(b) METRICS FOR SECURING THE BORDER BETWEEN PORTS OF ENTRY.—

(1) IN GENERAL.—Not later than 180 days after December 23, 2016, the Secretary shall develop metrics, informed by situational awareness, to measure the effectiveness of security between ports of entry. The Secretary shall annually implement the metrics developed under this subsection, which shall include the following:

(A) Estimates, using alternative methodologies where appropriate, including recidivism data, survey data, known-flow data, and technologically measured data, of the following:

(i) The rate of apprehension of attempted unlawful border crossers.

(ii) The number of detected unlawful entries.

(iii) The number of estimated undetected unlawful entries.

(iv) Turn backs.

(v) Got aways.

(B) A measurement of situational awareness achieved in each U.S. Border Patrol sector.

(C) An unlawful border crossing effectiveness rate in each U.S. Border Patrol sector.

(D) A probability of detection rate, which compares the estimated total unlawful border crossing attempts not detected by U.S. Border Patrol to the unlawful border crossing effectiveness rate under subparagraph (C), as informed by subparagraph (A).

(E) The number of apprehensions in each U.S. Border Patrol sector.

(F) The number of apprehensions of unaccompanied alien children, and the nationality of the children, in each U.S. Border Patrol sector.

(G) The number of apprehensions of family units, and the nationality of the family units, in each U.S. Border Patrol sector.

(H) An illicit drugs seizure rate for drugs seized by the U.S. Border Patrol between ports of entry, which compares the ratio of the amount and type of illicit drugs seized between ports of entry in any fiscal year to the average of the amount and type of illicit drugs seized between ports of entry in the immediately preceding 5 fiscal years.

(I) Estimates of the impact of the Consequence Delivery System on the rate of recidivism of unlawful border crossers over multiple fiscal years.

(J) An examination of each consequence under the Consequence Delivery System referred to in subparagraph (I), including the following:

(i) Voluntary return.

(ii) Warrant of arrest or notice to appear.

(iii) Expedited removal.

(iv) Reinstatement of removal.

(v) Alien transfer exit program.

(vi) Criminal consequence program.

(vii) Standard prosecution.

(viii) Operation Against Smugglers Initiative on Safety and Security.

(2) METRICS CONSULTATION.—To ensure that authoritative data sources are utilized in the development of the metrics described in paragraph (1), the Secretary shall—

(A) consult with the heads of the appropriate components of the Department; and

(B) where appropriate, consult with the heads of other agencies, including the Office of Refugee Resettlement of the Department of Health and Human Services and the Executive Office for Immigration Review of the Department of Justice.

(3) MANNER OF COLLECTION.—The data collected to inform the metrics developed in accordance with paragraph (1) shall be collected and reported in a consistent and standardized manner across all U.S. Border Patrol sectors, informed by situational awareness.

(c) METRICS FOR SECURING THE BORDER AT PORTS OF ENTRY.—

(1) IN GENERAL.—Not later than 180 days after December 23, 2016, the Secretary shall develop metrics, informed by situational awareness, to measure the effectiveness of security at ports of entry. The Secretary shall annually implement the metrics developed under this subsection, which shall include the following:

(A) Estimates, using alternative methodologies where appropriate, including recidivism data, survey data, and randomized secondary screening data, of the following:

(i) Total inadmissible travelers who attempt to enter or successfully enter the United States at a port of entry.

(ii) The rate of refusals and interdictions for travelers who attempt to enter or successfully enter the United States at a port of entry.

(iii) The number of unlawful entries at a port of entry.

(B) The amount and type of illicit drugs seized by the Office of Field Operations of U.S. Customs and Border Protection at ports of entry during the previous fiscal year.

(C) An illicit drugs seizure rate for drugs seized by the Office of Field Operations, which compares the ratio of the amount and type of illicit drugs seized by the Office of Field Operations in any fiscal year to the average of the amount and type of illicit drugs seized by the Office of Field Operations in the immediately preceding 5 fiscal years.

(D) The number of infractions related to travelers and cargo committed by major violators who are interdicted by the Office of Field Operations at ports of entry, and the estimated number of those infractions committed by major violators who are not so interdicted.

(E) In consultation with the heads of the Office of National Drug Control Policy and the United States Southern Command, a cocaine seizure effectiveness rate, which is the percentage resulting from dividing the amount of cocaine seized by the Office of Field Operations by the total estimated cocaine flow rate at ports of entry along the United States land border with Mexico and Canada.

(F) A measurement of how border security operations affect crossing times, including the following:

(i) A wait time ratio that compares the average wait times to total commercial and private vehicular traffic volumes at each land port of entry.

(ii) An infrastructure capacity utilization rate that measures traffic volume against the physical and staffing capacity at each land port of entry.

(iii) A secondary examination rate that measures the frequency of secondary examinations at each land port of entry.

(iv) An enforcement rate that measures the effectiveness of the secondary examinations at detecting major violators.

(G) A seaport scanning rate that includes the following:

(i) The number of all cargo containers that are considered potentially high-risk, as determined by the Executive Assistant Commissioner of the Office of Field Operations.

(ii) A comparison of the number of potentially high-risk cargo containers scanned by the Office of Field Operations at each sea port of entry during a fiscal year to the total number of high-risk cargo containers entering the United States at each such sea port of entry during the previous fiscal year.

(iii) The number of potentially high-risk cargo containers scanned on arrival at a United States sea port of entry.

(iv) The number of potentially high-risk cargo containers scanned before arrival at a United States sea port of entry.

(2) METRICS CONSULTATION.—To ensure that authoritative data sources are utilized in the development of the metrics described in paragraph (1), the Secretary shall—

(A) consult with the heads of the appropriate components of the Department; and

(B) where appropriate, work with heads of other appropriate agencies, including the Office of Refugee Resettlement of the Department of Health and Human Services and the Executive Office for Immigration Review of the Department of Justice.

(3) MANNER OF COLLECTION.—The data collected to inform the metrics developed in accordance with paragraph (1) shall be collected and reported in a consistent and standardized manner across all United States ports of entry, informed by situational awareness.

(d) METRICS FOR SECURING THE MARITIME BORDER.—

(1) IN GENERAL.—Not later than 180 days after December 23, 2016, the Secretary shall develop metrics, informed by situational awareness, to measure the effectiveness of security in the maritime environment. The Secretary shall annually implement the metrics developed under this subsection, which shall include the following:

(A) Situational awareness achieved in the maritime environment.

(B) A known maritime migrant flow rate.

(C) An illicit drugs removal rate for drugs removed inside and outside of a transit zone, which compares the amount and type of illicit drugs removed, including drugs abandoned at sea, by the maritime security components of the Department of Homeland Security in any fiscal year to the average of the amount and type of illicit drugs removed by the maritime components for the immediately preceding 5 fiscal years.

(D) In consultation with the heads of the Office of National Drug Control Policy and the United States Southern Command, a cocaine removal effectiveness rate for cocaine removed inside a transit zone and outside a transit zone, which compares the amount of cocaine removed by the maritime security components of the Department of Homeland Security to the total documented cocaine flow rate, as contained in Federal drug databases.

(E) A response rate, which compares the ability of the maritime security components of the Department of Homeland Security to respond to and resolve known maritime threats, whether inside or outside a transit zone, by placing assets on-scene, to the total number of events with respect to which the Department has known threat information.

(F) An intergovernmental response rate, which compares the ability of the maritime security components of the Department or

other United States Government entities to respond to and resolve actionable maritime threats, whether inside or outside a transit zone, with the number of those threats detected.

(2) METRICS CONSULTATION.—To ensure that authoritative data sources are utilized in the development of the metrics described in paragraph (1), the Secretary shall—

(A) consult with the heads of the appropriate components of the Department; and

(B) where appropriate, work with the heads of other agencies, including the Drug Enforcement Agency, the Department of Defense, and the Department of Justice.

(3) METHODS OF COLLECTION.—The data used by the Secretary shall be collected and reported in a consistent and standardized manner by the maritime security components of the Department, informed by situational awareness.

(e) AIR AND MARINE SECURITY METRICS IN THE LAND DOMAIN.—

(1) IN GENERAL.—Not later than 180 days after December 23, 2016, the Secretary shall develop metrics, informed by situational awareness, to measure the effectiveness of the aviation assets and operations of Air and Marine Operations of U.S. Customs and Border Protection. The Secretary shall annually implement the metrics developed under this subsection, which shall include the following:

(A) A flight hour effectiveness rate, which compares Air and Marine Operations flight hours requirements to the number of flight hours flown by Air and Marine Operations.

(B) A funded flight hour effectiveness rate, which compares the number of funded flight hours appropriated to Air and Marine Operations to the number of actual flight hours flown by Air and Marine Operations.

(C) A readiness rate, which compares the number of aviation missions flown by Air and Marine Operations to the number of aviation missions cancelled by Air and Marine Operations due to maintenance, operations, or other causes.

(D) The number of missions cancelled by Air and Marine Operations due to weather compared to the total planned missions.

(E) The number of individuals detected by Air and Marine Operations through the use of unmanned aerial systems and manned aircraft.

(F) The number of apprehensions assisted by Air and Marine Operations through the use of unmanned aerial systems and manned aircraft.

(G) The number and quantity of illicit drug seizures assisted by Air and Marine Operations through the use of unmanned aerial systems and manned aircraft.

(H) The number of times that actionable intelligence related to border security was obtained through the use of unmanned aerial systems and manned aircraft.

(2) METRICS CONSULTATION.—To ensure that authoritative data sources are utilized in the development of the metrics described in paragraph (1), the Secretary shall—

(A) consult with the heads of the appropriate components of the Department; and

(B) as appropriate, work with the heads of other departments and agencies, including the Department of Justice.

(3) MANNER OF COLLECTION.—The data collected to inform the metrics developed in accordance with paragraph (1) shall be collected and reported in a consistent and standardized manner by Air and Marine Operations, informed by situational awareness.

(f) DATA TRANSPARENCY.—The Secretary shall—

(1) in accordance with applicable privacy laws, make data relating to apprehensions, inadmissible aliens, drug seizures, and other enforcement actions available to the public, law enforcement communities, and academic research communities; and

(2) provide the Office of Immigration Statistics of the Department with unfettered access to the data referred to in paragraph (1).

(g) EVALUATIONS BY GOVERNMENT ACCOUNTABILITY OFFICE AND SECRETARY.—

(1) METRIC REPORT.—

(A) MANDATORY DISCLOSURES.—The Secretary shall submit to the appropriate congressional committees and the Comptroller General an annual report containing the metrics required under this section and the data and methodology used to develop the metrics.

(B) PERMISSIBLE DISCLOSURES.—The Secretary, for the purpose of validation and verification, may submit the annual report described in subparagraph (A) to—

(i) the Center for Borders, Trade, and Immigration Research of the Centers of Excellence network of the Department;

(ii) the head of a national laboratory in the Department laboratory network with prior expertise in border security; and

(iii) a federally funded research and development center.

(2) GOVERNMENT ACCOUNTABILITY OFFICE REPORT.—Not later than 270 days after receiving the first report under paragraph (1)(A) and biennially thereafter for the following 10 years with respect to every other report, the Comptroller General shall submit to the appropriate congressional committees a report that—

(A) analyzes the suitability and statistical validity of the data and methodology contained in each report; and

(B) includes recommendations on—

(i) the feasibility of other suitable metrics that may be used to measure the effectiveness of border security; and

(ii) improvements that need to be made to the metrics being used to measure the effectiveness of border security.

(3) STATE OF THE BORDER REPORT.—Not later than 60 days after the end of each fiscal year through fiscal year 2026, the Secretary shall submit to the appropriate congressional committees a State of the Border report that—

(A) provides trends for each metric under this section for the last 10 fiscal years, to the greatest extent possible;

(B) provides selected analysis into related aspects of illegal flow rates, including undocumented migrant flows and stock estimation techniques;

(C) provides selected analysis into related aspects of legal flow rates; and

(D) includes any other information that the Secretary determines appropriate.

(4) METRICS UPDATE.—

(A) IN GENERAL.—After submitting the 10th report to the Comptroller General under paragraph (1), the Secretary may re-evaluate and update any of the metrics developed in accordance with this section to ensure that the metrics are suitable to measure the effectiveness of border security.

(B) CONGRESSIONAL NOTIFICATION.—Not later than 30 days before updating the metrics pursuant to subparagraph (A), the Secretary shall notify the appropriate congressional committees of the updates.

§ 11116. Reports relating to border between United States and Mexico

(a) UNIDENTIFIED REMAINS.—

(1) ANNUAL REPORT.—Not later than 1 year after December 31, 2020, and annually thereafter, the Commissioner of U.S. Customs and

Border Protection shall submit a report to the appropriate committees of Congress regarding all unidentified remains discovered, during the reporting period, on or near the border between the United States and Mexico, including—

(A) for each deceased individual—

(i) the cause and manner of death, if known;

(ii) the sex, age (at time of death), and country of origin (if the information is determinable); and

(iii) the location of each unidentified remain;

(B) the total number of deceased individuals whose unidentified remains were discovered by U.S. Customs and Border Protection during the reporting period;

(C) to the extent the information is available to U.S. Customs and Border Protection, the total number of deceased individuals whose unidentified remains were discovered by Federal, State, local or Tribal law enforcement officers, military personnel, or medical examiner's offices;

(D) the efforts of U.S. Customs and Border Protection to engage with nongovernmental organizations, institutions of higher education, medical examiners and coroners, and law enforcement agencies—

(i) to identify and map the locations at which migrant deaths occur; and

(ii) to count the number of deaths that occur at those locations; and

(E) a detailed description of U.S. Customs and Border Protection's Missing Migrant Program, including how the program helps mitigate migrant deaths while maintaining border security.

(2) PUBLIC DISCLOSURE.—Not later than 30 days after each report required under paragraph (1) is submitted, the Commissioner of U.S. Customs and Border Protection shall publish on the website of the agency the information described in subparagraphs (A), (B), and (C) of paragraph (1) during each reporting period.

(b) RESCUE BEACONS.—Not later than 1 year after December 31, 2020, and annually thereafter, the Commissioner of U.S. Customs and Border Protection shall submit a report to the appropriate committees of Congress regarding the use of rescue beacons along the border between the United States and Mexico, including, for the reporting period—

(1) the number of rescue beacons in each border patrol sector;

(2) the specific location of each rescue beacon;

(3) the frequency with which each rescue beacon was activated by an individual in distress;

(4) a description of the nature of the distress that resulted in each rescue beacon activation (if the information is determinable); and

(5) an assessment, in consultation with local stakeholders, including elected officials, nongovernmental organizations, and landowners, of necessary additional rescue beacons and recommendations for locations for deployment to reduce migrant deaths.

(c) COMPTROLLER GENERAL REPORT.—Not later than 6 months after the report required under subsection (a) is submitted to the appropriate committees of Congress, the Comptroller General shall submit a report to the same committees that describes—

(1) how U.S. Customs and Border Protection collects and records border-crossing death data;

(2) the differences (if any) in U.S. Customs and Border Protection border-crossing death data collection methodology across its sectors;

(3) how U.S. Customs and Border Protection's data and statistical analysis on trends in the numbers, locations, causes, and characteristics of border-crossing deaths compare to other sources of data on these deaths, including border county medical examiners and coroners and the Centers for Disease Control and Prevention;

(4) how U.S. Customs and Border Protection measures the effectiveness of its programs to mitigate migrant deaths; and

(5) the extent to which U.S. Customs and Border Protection engages Federal, State, local, and Tribal governments, foreign diplomatic and consular posts, and nongovernmental organizations—

(A) to accurately identify deceased individuals;

(B) to resolve cases involving unidentified remains;

(C) to resolve cases involving unidentified individuals; and

(D) to share information on missing individuals and unidentified remains, specifically with the National Missing and Unidentified Persons System (NamUs).

§ 11117. Trusted traveler program

The Secretary may not enter into or renew an agreement with the government of a foreign country for a trusted traveler program administered by U.S. Customs and Border Protection unless the Secretary certifies in writing that the government—

(1) routinely submits to INTERPOL for inclusion in INTERPOL's Stolen and Lost Travel Documents database information about lost and stolen passports and travel documents of the citizens and nationals of the country; or

(2) makes available to the United States Government the information described in paragraph (1) through another means of reporting.

§ 11118. Asia-Pacific Economic Cooperation Business Travel Cards

(a) DEFINITION OF TRUSTED TRAVELER PROGRAM.—In this section, the term ''trusted traveler program'' means a voluntary program of the Department that allows U.S. Customs and Border Protection to expedite clearance of pre-approved, low-risk travelers arriving in the United States.

(b) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection (in this section referred to as the ''Commissioner'') may issue an Asia-Pacific Economic Cooperation Business Travel Card (referred to in this section as an ''ABT Card'') to an individual described in subsection (c).

(c) INDIVIDUALS WHO MAY RECEIVE ABT CARD.—An individual referred to in subsection (b) is an individual who—

(1) is a citizen of the United States;

(2) has been approved and is in good standing in an existing international trusted traveler program of the Department; and

(3) is—

(A) engaged in business in the Asia-Pacific region, as determined by the Commissioner; or

(B) a United States Government official actively engaged in Asia-Pacific Economic Cooperation business, as determined by the Commissioner.

(d) INTEGRATION WITH EXISTING TRAVEL PROGRAMS.—The Commissioner shall integrate application procedures for, and issuance, renewal, and revocation of, ABT Cards with existing international trusted traveler programs of the Department.

(e) COOPERATION WITH PRIVATE ENTITIES AND NONGOVERNMENTAL ORGANIZATIONS.—In carrying out this section, the Commissioner may consult with appropriate private-sector entities and nongovernmental organizations, including academic institutions.

(f) FEE.—

(1) IN GENERAL.—The Commissioner shall—

(A) prescribe and collect a fee for the issuance and renewal of ABT Cards; and

(B) adjust the fee to the extent the Commissioner determines necessary to comply with paragraph (2).

(2) LIMITATION.—The Commissioner shall ensure that the total amount of the fees collected under paragraph (1) during a fiscal year is sufficient to offset the direct and indirect costs associated with carrying out this section during that fiscal year, including the costs associ-

ated with operating and maintaining the ABT Card issuance and renewal processes.

(3) ACCOUNT FOR COLLECTIONS.—There is in the Treasury an Asia-Pacific Economic Cooperation Business Travel Card Account into which the fees collected under paragraph (1) shall be deposited as offsetting receipts.

(4) USE OF FUNDS.—Amounts deposited into the Asia-Pacific Economic Cooperation Business Travel Card Account shall—

(A) be credited to the appropriate account of U.S. Customs and Border Protection for expenses incurred in carrying out this section; and

(B) remain available until expended.

(g) NOTIFICATION.—The Commissioner shall notify the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate not later than 60 days after the expenditures of funds to operate and provide ABT Card services beyond the amounts collected under subsection (f)(1).

§ 11119. Hiring members of the armed forces separating from military service

(a) EXPEDITED HIRING.—The Secretary shall consider the expedited hiring of qualified candidates who have the ability to perform the essential functions of the position of a U.S. Customs and Border Protection officer and who are eligible for a veterans recruitment appointment authorized under section 4214 of title 38.

(b) ENHANCED RECRUITING EFFORTS.—The Secretary, in consultation with the Secretary of Defense, and acting through existing programs, authorities, and agreements, where applicable, shall enhance the efforts of the Department to recruit members of the armed forces who are separating from military service to serve as U.S. Customs and Border Protection officers. The enhanced recruiting efforts shall—

(1) include U.S. Customs and Border Protection officer opportunities in relevant job assistance efforts under the Transition Assistance Program;

(2) place U.S. Customs and Border Protection officials or other relevant Department officials at recruiting events and jobs fairs involving members of the armed forces who are separating from military service;

(3) provide opportunities for local U.S. Customs and Border Protection field offices to partner with military bases in the region;

(4) include outreach efforts to educate members of the armed forces with Military Occupational Specialty Codes and Officer Branches, Air Force Specialty Codes, Naval Enlisted Classifications and Officer Des-

ignators, and Coast Guard competencies that are transferable to the requirements, qualifications, and duties assigned to U.S. Customs and Border Protection officers of available hiring opportunities to become U.S. Customs and Border Protection officers;

(5) identify shared activities and opportunities for reciprocity related to steps in hiring U.S. Customs and Border Protection officers with the goal of minimizing the time required to hire qualified applicants;

(6) ensure the streamlined interagency transfer of relevant background investigations and security clearances; and

(7) include such other elements as may be necessary to ensure that members of the armed forces who are separating from military service are aware of opportunities to fill vacant U.S. Customs and Border Protection officer positions.

(c) REPORTS.—Not later than 180 days after October 16, 2015, and by December 31 of each of the next 3 years, the Secretary, in consultation with the Secretary of Defense, shall submit a report to the Committee on Homeland Security and the Committee on Armed Services of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services of the Senate that includes a description and assessment of the efforts of the Department under this section to hire members of the armed forces who are separating from military service as U.S. Customs and Border Protection officers. The report shall include—

(1) a detailed description of the efforts to implement subsection (b), including—

(A) elements of the enhanced recruiting efforts and the goals associated with those elements; and

(B) a description of how the elements and goals referred to in subparagraph (A) will assist in meeting statutorily mandated staffing levels and agency hiring benchmarks;

(2) a detailed description of the efforts that have been undertaken under subsection (b);

(3) the estimated number of separating service members made aware of U.S. Customs and Border Protection officer vacancies;

(4) the number of U.S. Customs and Border Protection officer vacancies filled with separating service members; and

(5) the number of U.S. Customs and Border Protection officer vacancies filled with separating service members under veterans recruitment appointments authorized under section 4214 of title 38.

(d) RULES OF CONSTRUCTION.—Nothing in this section may be construed—

(1) as superseding, altering, or amending existing Federal veterans' hiring preferences or Federal hiring authorities; or

(2) as authorizing the appropriation of additional amounts to carry out this section.

§ 11120. Protecting America's food and agriculture

(a) DEFINITIONS.—In this section:

(1) CBP.—The term ''CBP'' means U.S. Customs and Border Protection.

(2) COMMISSIONER.—The term ''Commissioner'' means Commissioner of U.S. Customs and Border Protection.

(b) ADDITIONAL PERSONNEL.—

(1) CBP AGRICULTURE SPECIALISTS.—The Commissioner may hire, train, and assign 240 new CBP Agriculture Specialists above the current attrition level during every fiscal year until the total number of CBP Agriculture Specialists equals and sustains the requirements identified each year in the Agriculture Resource Allocation Model.

(2) MISSION AND OPERATIONAL SUPPORT STAFF.—

(A) IN GENERAL.—The Commissioner may hire, train, and assign support staff to support CBP Agriculture Specialists.

(B) CBP AGRICULTURE TECHNICIANS.—The Commissioner may hire, train, and assign 200 new CBP Agriculture Technicians during each fiscal year until the total number of CBP Agriculture Technicians equals and sustains the requirements identified each year in the Mission and Operation Support Resource Allocation Model.

(3) CBP AGRICULTURE CANINE TEAMS.—The Commissioner may hire, train, and assign 20 new CBP agriculture canine teams during each of the first 3 fiscal years beginning after March 3, 2020.

(c) NUMBER OF CBP AGRICULTURE SPECIALISTS NEEDED AT EACH PORT OF ENTRY.—In calculating the number of CBP Agriculture Specialists needed at each port of entry through the Agriculture Resource Allocation Model, the Office of Field Operations shall—

(1) rely on data collected regarding the inspections and other activities conducted at each port of entry; and

(2) consider volume from seasonal surges, other projected changes in commercial and passenger volumes, the most current commercial forecasts, and other relevant information.

(d) AUTHORIZATION OF APPROPRIATIONS.—

(1) CBP AGRICULTURE SPECIALISTS.—There is authorized to be appropriated to carry out subsection (b)(1) $40,500,000 for fiscal year 2022.

(2) CBP AGRICULTURE TECHNICIANS.—There is authorized to be appropriated to carry out subsection (b)(2) $38,000,000 for fiscal year 2022.

(3) CBP AGRICULTURE CANINE TEAMS.—There is authorized to be appropriated to carry out subsection (b)(3) $12,200,000 for fiscal year 2022.

(4) TRAINING.—There is authorized to be appropriated for training costs associated with new CBP personnel and canine teams hired pursuant to paragraphs (1), (2), and (3) of subsection (b) $6,000,000 for fiscal year 2022.

§ 11121. Large-scale non-intrusive inspection scanning plan

(a) DEFINITIONS.—In this section

(1) LARGE-SCALE NON-INTRUSIVE INSPECTION SYSTEM.—The term ''large-scale, non-intrusive inspection system'' means a technology, including x-ray, gamma-ray, and passive imaging systems, capable of producing an image of the contents of a commercial or passenger vehicle or freight rail car in 1 pass of the vehicle or car.

(2)SCANNING.—The term ''scanning'' means utilizing nonintrusive imaging equipment, radiation detection equipment, or both, to capture data, including images of a commercial or passenger vehicle or freight rail car.

(b)IN GENERAL.—The Secretary shall submit a plan to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives for increasing to 100 percent the rate of high-throughput scanning of commercial and passenger vehicles and freight rail traffic entering the United States at land ports of entry and rail-border crossings along the border using large-scale non-intrusive inspection systems or similar technology to enhance border security.

(c)BASELINE INFORMATION.—The plan under subsection (b) shall include, at a minimum, the following information regarding large-scale non-intrusive inspection systems or similar technology operated by U.S. Customs and Border Protection at land ports of entry and rail-border crossings as of January 5, 2021:

(1) An inventory of large-scale non-intrusive inspection systems or similar technology in use at each land port of entry.

(2) For each system or technology identified in the inventory under paragraph (1)—

(A) the scanning method of the system or technology;

(B) the location of the system or technology at each land port of entry that specifies whether in use in pre-primary, primary, or secondary inspection area, or some combination of the areas;

(C) the percentage of commercial and passenger vehicles and freight rail traffic scanned by the system or technology;

(D) seizure data directly attributed to scanned commercial and passenger vehicles and freight rail traffic; and

(E) the number of personnel required to operate each system or technology.

(3) Information regarding the continued use of other technology and tactics used for scanning, such as canines and human intelligence in conjunction with large scale, nonintrusive inspection systems.

(d)ELEMENTS.—The plan under subsection (b) shall include the following information:

(1) Benchmarks for achieving incremental progress towards 100 percent high-throughput scanning by January 5, 2027, of commercial and passenger vehicles and freight rail traffic entering the United States at land ports of entry and rail-border crossings along the border with corresponding projected incremental improvements in scanning rates by fiscal year and rationales for the specified timeframes for each land port of entry.

(2) Estimated costs, together with an acquisition plan, for achieving the 100 percent high-throughput scanning rate within the timeframes specified in paragraph (1), including acquisition, operations, and maintenance costs for large-scale, nonintrusive inspection systems or similar technology, and associated costs for any necessary infrastructure enhancements or configuration changes at each port of entry. The acquisition plan shall promote, to the extent practicable, opportunities for entities that qualify as small business concerns (as defined under section 3(a) of the Small Business Act (15 U.S.C. 632(a)).

(3) Any projected impacts, as identified by the Commissioner of U.S. Customs and Border Protection, on the total number of commercial and passenger vehicles and freight rail traffic entering at land ports of entry and rail-border crossings where the systems are in use, and average wait times at peak and non-peak travel times, by lane type if applicable, as scanning rates are increased.

(4) Any projected impacts, as identified by the Commissioner of U.S. Customs and Border Protection, on land ports of entry and rail-border crossings border security operations as a result of implementation actions, including any changes to the number of U.S. Customs and Border Protection officers or their duties and assignments.

(e)ANNUAL REPORT.—Not later than 1 year after the submission of the plan under subsection (b), and biennially thereafter for the following 6 years, the Secretary of Homeland Security shall submit a report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives that describes the progress implementing the plan and includes—

(1) an inventory of large-scale, nonintrusive inspection systems or similar technology operated by U.S. Customs and Border Protection at each land port of entry;

(2) for each system or technology identified in the inventory required under paragraph (1)—

(A) the scanning method of the system or technology;

(B) the location of the system or technology at each land port of entry that specifies whether in use in pre-primary, primary, or secondary inspection area, or some combination of the areas;

(C) the percentage of commercial and passenger vehicles and freight rail traffic scanned by the system or technology; and

(D) seizure data directly attributed to scanned commercial and passenger vehicles and freight rail traffic;

(3) the total number of commercial and passenger vehicles and freight rail traffic entering at each land port of entry at which each system or technology is in use, and information on average wait times at peak and non-peak travel times, by lane type if applicable;

(4) a description of the progress towards reaching the benchmarks referred to in subsection (d)(1), and an explanation if any of the benchmarks are not achieved as planned;

(5) a comparison of actual costs (including information on any awards of associated contracts) to estimated costs set forth in subsection (d)(2);

(6) any realized impacts, as identified by the Commissioner of U.S. Customs and Border Protection, on land ports of entry and rail-border crossings operations as a result of implementation actions, including any changes to the number of U.S. Customs and Border Protection officers or their duties and assignments;

(7) any proposed changes to the plan and an explanation for the changes, including changes made in response to any Department research and development findings or changes in terrorist or transnational criminal organizations tactics, techniques, or procedures; and

(8) any challenges to implementing the plan or meeting the benchmarks, and plans to mitigate the challenges.

Part B—Customs Functions

§ 11131. Definition of customs revenue function

In this subchapter, the term ''customs revenue function'' means the following:

(1) Assessing and collecting customs duties (including antidumping and countervailing duties and duties imposed under safeguard provisions), excise taxes, fees, and penalties due on imported merchandise, including classifying and valuing merchandise for purposes of assessment.

(2) Processing and denial of entry of persons, baggage, cargo, and mail, with respect to the assessment and collection of import duties.

(3) Detecting and apprehending persons engaged in fraudulent practices designed to circumvent the customs laws of the United States.

(4) Enforcing section 337 of the Tariff Act of 1930 (19 U.S.C. 1337) and provisions relating to import quotas and the marking of imported merchandise, and providing Customs Recordations for copyrights, patents, and trademarks.

(5) Collecting accurate import data for compilation of international trade statistics.

(6) Enforcing reciprocal trade agreements.

(7) Functions performed by the following personnel, and associated support staff, of U. S. Customs and Border Protection on January 23, 2003:

(A) Import Specialists.

(B) Entry Specialists.

(C) Drawback Specialists.

(D) National Import Specialists.

(E) Fines and Penalties Specialists.

(F) Attorneys of the Office of Regulations and Rulings.

(G) Customs Auditors.

(H) International Trade Specialists.

(I) Financial Systems Specialists.

(8) Functions performed by the following offices, with respect to any function described in any of paragraphs (1) through (7), and associated support staff, of the United States Customs Service on January 23, 2003, and of U.S. Customs and Border Protection on February 23, 2016:

(A) Office of Information and Technology.

(B) Office of Laboratory Services.

(C) Office of the Chief Counsel.

(D) Office of Congressional Affairs.

(E) Office of International Affairs.

(F) Office of Training and Development.

§ 11132. Retention of customs revenue functions by Secretary of the Treasury

(a) RETENTION OF CUSTOMS REVENUE FUNCTIONS BY SECRETARY OF THE TREASURY.—

(1) RETENTION OF AUTHORITY.—Notwithstanding section 11101(b)(1) of this title, authority relating to customs revenue functions that was vested in the Secretary of the Treasury by law before January 24, 2003, under those provisions of law set forth in paragraph (2) shall not be transferred to the Secretary by reason of the Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2135) and, on and after January 24, 2003, the Secretary of the Treasury may delegate that authority to the Secretary at the discretion of the Secretary of the Treasury. The Secretary of the Treasury shall consult with the Secretary regarding the exercise of authority not delegated to the Secretary.

(2) STATUTES.—The provisions of law referred to in paragraph (1) are the following:

(A) Section 249 of the Revised Statutes of the United States (19 U.S.C. 3).

(B) Section 2 of the Act of March 4, 1923 (19 U.S.C. 6).

(C) Section 13031 of the Consolidated Omnibus Budget Reconciliation Act of 1985 (19 U.S.C. 58c).

(D) Section 251 of the Revised Statutes of the United States (19 U.S.C. 66).

(E) Section 1 of the Act of June 26, 1930 (19 U.S.C. 68).

(F) The Act of June 18, 1934 (known as the Foreign Trade Zones Act) (19 U.S.C. 81a et seq.).

(G) Section 1 of the Act of March 2, 1911 (19 U.S.C. 198).

(H) The Tariff Act of 1930 (19 U.S.C. 1202 et seq.).

(I) The Trade Act of 1974 (19 U.S.C. 2101 et seq.).

(J) The Trade Agreements Act of 1979 (19 U.S.C. 2501 et seq.).

(K) The Caribbean Basin Economic Recovery Act (19 U.S.C. 2701 et seq.).

(L) The Andean Trade Preference Act (19 U.S.C. 3201 et seq.).

(M) The North American Free Trade Agreement Implementation Act (19 U.S.C. 3311 et seq.).

(N) The Uruguay Round Agreements Act (19 U.S.C. 3501 et seq.).

(O) The African Growth and Opportunity Act (19 U.S.C. 3701 et seq.).

(P) Any other provision of law vesting customs revenue functions in the Secretary of the Treasury.

(b) MAINTENANCE OF CUSTOMS REVENUE FUNCTIONS.—

(1) MAINTENANCE OF FUNCTIONS.—Notwithstanding this subtitle, the Secretary may not consolidate, discontinue, or diminish those functions described in paragraph (2) performed by U.S. Customs and Border Protection on or after January 24, 2003, reduce the staffing level, or reduce the resources attributable to the functions, and the Secretary shall ensure that an appropriate management structure is implemented to carry out the functions.

(2) FUNCTIONS.—The functions referred to in paragraph (1) are those functions performed by the following personnel, and associated support staff, of U. S. Customs and Border Protection on January 23, 2003:

(A) Import Specialists.

(B) Entry Specialists.

(C) Drawback Specialists.

(D) National Import Specialists.

(E) Fines and Penalties Specialists.

(F) Attorneys of the Office of Regulations and Rulings.

(G) Customs Auditors.

(H) International Trade Specialists.

(I) Financial Systems Specialists.

(c) NEW PERSONNEL.—The Secretary of the Treasury may appoint up to 20 new personnel to work with personnel of the Department in performing customs revenue functions.

§ 11133. Preservation of customs funds

Notwithstanding this subtitle, no funds collected under section 13031(a)(1) through (8) of the Consolidated Omnibus Budget Reconciliation Act of 1985 (19 U.S.C. 58c(a)(1) through (8)) may be transferred for use by another agency or office in the Department.

Part C—Drug Interdiction

§ 11141. Methamphetamine and methamphetamine precursor chemicals

(a) DEFINITION OF METHAMPHETAMINE PRECURSOR CHEMICALS.—In this section, the term ''methamphetamine precursor chemicals'' means the chemicals ephedrine, pseudoephedrine, or phenylpropanolamine, including

each of the salts, optical isomers, and salts of optical isomers of the chemicals.

(b) COMPLIANCE WITH PERFORMANCE PLAN REQUIREMENTS.—As part of the annual performance plan required in the budget submission of U.S. Customs and Border Protection under section 1115 of title 31, the Commissioner of U.S. Customs and Border Protection (in this section referred to as the ''Commissioner'') shall establish performance indicators relating to the seizure of methamphetamine and methamphetamine precursor chemicals in order to evaluate the performance goals of U.S. Customs and Border Protection with respect to the interdiction of illegal drugs entering the United States.

(c) STUDY AND REPORT RELATING TO METHAMPHETAMINE AND METHAMPHETAMINE PRECURSOR CHEMICALS.—

(1) ANALYSIS.—The Commissioner shall, on an ongoing basis, analyze the movement of methamphetamine and methamphetamine precursor chemicals into the United States. In conducting the analysis, the Commissioner shall—

(A) consider the entry of methamphetamine and methamphetamine precursor chemicals through ports of entry, between ports of entry, through international mails, and through international courier services;

(B) examine the export procedures of each foreign country where the shipments of methamphetamine and methamphetamine precursor chemicals originate and determine if changes in the country's customs overtime provisions would alleviate the export of methamphetamine and methamphetamine precursor chemicals; and

(C) identify emerging trends in smuggling techniques and strategies.

(2) REPORT.—Not later than September 30 of each odd-numbered year, the Commissioner, in consultation with the Attorney General, United States Immigration and Customs Enforcement, the United States Drug Enforcement Administration, and the United States Department of State, shall submit a report to the Committee on Finance of the Senate, the Committee on Foreign Relations of the Senate, the Committee on the Judiciary of the Senate, the Committee on Ways and Means of the House of Representatives, the Committee on Foreign Affairs of the House of Representatives, and the Committee on the Judiciary of the House of Representatives that includes—

(A) a comprehensive summary of the analysis described in paragraph (1); and

(B) a description of how U.S. Customs and Border Protection utilized the analysis described in paragraph (1) to target shipments presenting a high risk for smuggling or circumvention of the Combat Methamphetamine Epidemic Act of 2005 (Public Law 109–177, title VII, 120 Stat. 256).

(3) AVAILABILITY OF ANALYSIS.—The Commissioner shall ensure that the analysis described in paragraph (1) is made available in a timely manner to the Secretary of State to facilitate the Secretary in fulfilling the Secretary's reporting requirements in section 722 of the Combat Methamphetamine Epidemic Act of 2005 (Public Law 109–177, title VII, 120 Stat. 268).

§ 11142. Protection against potential synthetic opioid exposure

(a) ISSUANCE OF POLICY.—The Commissioner of U.S. Customs and Border Protection (in this section referred to as the ''Commissioner'') shall issue a policy that specifies effective protocols and procedures—

(1) for the safe handling of potential synthetic opioids, including fentanyl, by U.S. Customs and Border Protection officers, agents, other personnel, and canines; and

(2) to reduce the risk of injury or death resulting from accidental exposure and enhance post-exposure management.

(b) TRAINING.—

(1) IN GENERAL.— Together with the issuance of the policy described in subsection (a), the Commissioner shall require mandatory and recurrent training on the following:

(A) The potential risk of opioid exposure and safe handling procedures for potential synthetic opioids, including precautionary measures such as the use of personal protective equipment during the handling of potential synthetic opioids.

(B) How to access and administer opioid receptor antagonists, including naloxone, post-exposure to potential synthetic opioids.

(C) How to use containment devices to prevent potential synthetic opioid exposure.

(2) INTEGRATION WITH OTHER TRAINING.— The training described in paragraph (1) may be integrated into existing training undersection 11102(d) of this titlefor U.S. Customs and Border Protection officers, agents, and other personnel.

(c) PERSONAL PROTECTIVE EQUIPMENT, CONTAINMENT DEVICES, AND OPIOID RECEPTOR ANTAGONISTS.— Together with the issuance of the policy described in subsection (a), the Commissioner shall ensure the availability of personal protective equipment and opioid receptor antagonists, in-

cluding naloxone and containment devices, to all U.S. Customs and Border Protection officers, agents, other personnel, and canines at risk of accidental exposure to synthetic opioids.

(d) OVERSIGHT.—To ensure the effectiveness of the policy described in subsection (a)—

(1) the Commissioner shall regularly monitor the efficacy of the implementation of the policy and adjust protocols and procedures, as necessary; and

(2) the Inspector General of the Department shall audit compliance with the requirements of this section not less than once during the 3-year period after December 27, 2020.

(e) APPLICABILITY TO OTHER COMPONENTS.—If the Secretary determines that other officers, agents, other personnel, or canines of a component of the Department other than U.S. Customs and Border Protection are at risk of potential synthetic opioid exposure in the course of their duties, the head of the component shall carry out the responsibilities under this section in the same manner and to the same manner as the Commissioner carries out the responsibilities.

§ 11143. Reports, evaluations, and research regarding drug interdiction at and between ports of entry

(a) DETECTION OF NARCOTICS AT VARIOUS PURITY LEVELS.—The Commissioner of U.S. Customs and Border Protection shall—

(1) implement a strategy to ensure deployed chemical screening devices are able to identify, in an operational environment, narcotics at purity levels less than or equal to 10 percent, or provide ports of entry with an alternate method for identifying narcotics at lower purity levels; and

(2) require testing of any new chemical screening devices to understand the abilities and limitations of the devices relating to identifying narcotics at various purity levels before CBP commits to the acquisition of the devices.

(b) DEVELOPMENT OF CENTRALIZED SPECTRAL DATABASE FOR CHEMICAL SCREENING DEVICES.—The Secretary shall implement a plan for the long-term development of a centralized spectral database for chemical screening devices. The plan shall address the following:

(1) How newly identified spectra will be collected, stored, and distributed to the devices in their operational environment, including at ports of entry.

(2) Identification of parties responsible for updates and maintenance of the database.

(c) RESEARCH ON ADDITIONAL TECHNOLOGIES TO DETECT FENTANYL.—Not later than December 23, 2023, the Secretary, in consultation with the Attorney General, the Secretary of Health and Human Services, and the Director of the Office of National Drug Control Policy, shall research additional technological solutions to—

(1) target and detect illicit fentanyl, fentanyl analogs, and precursor chemicals, including low-purity fentanyl, especially in counterfeit pressed tablets, and illicit pill press molds; and

(2) enhance detection of the counterfeit pressed tablets through non-intrusive, noninvasive, and other advanced screening technologies.

(d) EVALUATION OF CURRENT TECHNOLOGIES AND STRATEGIES IN ILLICIT DRUG INTERDICTION AND PROCUREMENT DECISIONS.—

(1) IN GENERAL.—The Secretary, in consultation with the Attorney General, the Secretary of Health and Human Services, and the Director of the Office of National Drug Control Policy, shall establish a program to collect available data and develop metrics to measure how technologies and strategies used by the Department, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and other relevant Federal agencies have helped detect trafficked illicit fentanyl, fentanyl analogs, and precursor chemicals or deter illicit fentanyl, fentanyl analogs, and precursor chemicals from being trafficked into the United States at and between land, air, and sea ports of entry.

(2) CONSIDERATIONS.—The data and metrics program established pursuant to paragraph (1) may consider

(A) the rate of detection of illicit fentanyl, fentanyl analogs, and precursor chemicals at land, air, and sea ports of entry;

(B) investigations and intelligence sharing into the origins of illicit fentanyl, fentanyl analogs, and precursor chemicals in the United States; and

(C) other data or metric the Secretary considers appropriate.

(3) UPDATES.—The Secretary, as appropriate and in the coordination with the officials referred to in paragraph (1), may update the data and metrics programs established pursuant to paragraph (1).

(4) REPORTS.—

(A) SECRETARY.— Not later than December 23, 2023, and biennially thereafter, the Secretary, in consultation with the Attorney General, the Secretary of Health and Human Services, and the Director of the Office of National Drug Control Policy, shall, based on the data collected and metrics developed pursuant to the program established pursuant to paragraph (1), submit to the

Committee on Homeland Security, the Committee on Energy and Commerce, the Committee on Science, Space, and Technology, and the Committee on the Judiciary of the House of Representatives and the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on the Judiciary of the Senate a report that—

(i) examines and analyzes current technologies, including pilot technologies, deployed at land, air, and sea ports of entry to assess how well the technologies detect, deter, and address illicit fentanyl, fentanyl analogs, and precursor chemicals; and

(ii) examines and analyzes current technologies, including pilot technologies, deployed between land ports of entry to assess how well and accurately the technologies detect, deter, and address illicit fentanyl, fentanyl analogs, and precursor chemicals.

(B) GOVERNMENT ACCOUNTABILITY OFFICE.——Not later than 1 year after the submission of each of the first 3 reports required under subparagraph (A), the Comptroller General shall submit to the Committee on Homeland Security, the Committee on Energy and Commerce, the Committee on Science, Space, and Technology, and the Committee on the Judiciary of the House of Representatives and the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on the Judiciary of the Senate a report that evaluates and as appropriate makes recommendations to improve the collection of data under the program established pursuant to paragraph (1) and metrics used in the subsequent reports required under that paragraph.

Subchapter III—Immigration Enforcement Functions

§ 11151. Transfer of functions

The Secretary succeeds to the functions, personnel, assets, and liabilities of the following programs of the Commissioner of Immigration and Naturalization:

(1) The Border Patrol program.

(2) The detention and removal program.

(3) The intelligence program.

(4) The investigations program.

(5) The inspections program.

§ 11152. Responsibilities of U.S. Immigration and Customs Enforcement officials

(a) DIRECTOR OF IMMIGRATION AND CUSTOMS ENFORCEMENT.—

(1) FUNCTIONS.—The Director of Immigration and Customs Enforcement—

(A) shall establish the policies for performing functions—

(i) transferred to the Secretary by section 11151 of this title and delegated to the Director of Immigration and Customs Enforcement by the Secretary; or

(ii) otherwise vested in the Director of Immigration and Customs Enforcement by law;

(B) shall oversee the administration of the policies; and

(C) shall advise the Secretary with respect to a policy or operation of U.S. Immigration and Customs Enforcement that may affect U.S. Citizenship and Immigration Services established under subchapter IV of this chapter, including potentially conflicting policies or operations.

(2) PROGRAM TO COLLECT INFORMATION RELATING TO FOREIGN STUDENTS.—The Director of Immigration and Customs Enforcement is responsible for administering the program to collect information relating to nonimmigrant foreign students and other exchange program participants described in section 641 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1372), including the Student and Exchange Visitor Information System established under that section, and shall use the information to carry out the enforcement functions of U.S. Immigration and Customs Enforcement.

(3) MANAGERIAL ROTATION PROGRAM.—The Director of Immigration and Customs Enforcement shall design and implement a managerial rotation program under which employees of U.S. Immigration 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.

§ 11153. 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.

§ 11154. 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;

(2) the Committee on the Judiciary of the Senate;

(3) the Committee on Appropriations of the Senate;

(4) the Committee on Homeland Security of the House of Representatives;

(5) the Committee on the Judiciary of the House of Representatives; and

(6) the Committee on Appropriations of the House of Representatives.

(b) CONTENT.—The Secretary shall submit an annual report to the congressional committees that includes a description of—

(1) the cross-border tunnels along the border between Mexico and the United States discovered during the preceding fiscal year; and

(2) the needs of the Department to effectively prevent, investigate, and prosecute border tunnel construction along the border between Mexico and the United States.

§ 11155. Illicit cross-border tunnel defense

(a) COUNTER ILLICIT CROSS-BORDER TUNNEL OPERATIONS STRATEGIC PLAN.—

(1) IN GENERAL.—Not later than 180 days after December 23, 2022, the Commissioner of U.S. Customs and Border Protection, in coordination with the Under Secretary for Science and Technology, and, as appropriate, other officials of the Department, shall develop an illicit cross-border tunnel operations strategic plan (in this section referred to as the ''strategic plan'') to address the following:

(A) Risk-based criteria to be used to prioritize the identification, breach, assessment, and remediation of illicit cross-border tunnels.

(B) Promote the use of innovative technologies to identify, breach, assess, and remediate illicit cross-border tunnels in a manner that, among other considerations, reduces the impact of those activities on surrounding communities.

(C) Processes to share relevant illicit cross-border tunnel locations, operations, and technical information.

(D) Indicators of specific types of illicit cross-border tunnels found in each U.S. Border Patrol sector identified through operations to be periodically disseminated to U.S. Border Patrol sector chiefs to education field personnel.

(E) A counter illicit cross-border tunnel operations resource needs assessment that includes consideration of the following:

(i) Technology needs.

(ii) Staffing needs including the following:

(I) A position description for counter illicit cross-border tunnel operations personnel.

(II) Any specialized skills required of the personnel.

(III) The number of the full time personnel disaggregated by U.S. Border Patrol sector.

(2) Report to congress on strategic plan.—Not later than 1 year after the development of the strategic plan, the Commissioner of U.S. Customs and Border Protection shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the implementation of the strategic plan.

(b) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Commissioner of U.S. Customs and Border Protection $1,000,000 for each of fiscal years 2023 and 2024 to carry out.—

(1) the development of the strategic plan; and

(2) remediation operations of illicit cross-border tunnels in accordance with the strategic plan to the maximum extent practicable.

Subchapter IV—Citizenship and Immigration Services

§ 11171. Transfer of functions to Director of U.S. Citizenship and Immigration Services

The Director of U.S. Citizenship and Immigration Services succeeds to the following functions of the Commissioner of Immigration and Naturalization, and all personnel, infrastructure, and funding provided to the Commissioner in support of the functions immediately before March 1, 2003:

(1) Adjudications of immigrant visa petitions.

(2) Adjudications of naturalization petitions.

(3) Adjudications of asylum and refugee applications.

(4) Adjudications performed at service centers.

(5) All other adjudications performed by the Immigration and Naturalization Service immediately before March 1, 2003.

§ 11172. Responsibilities of U.S. Citizenship and Immigration Services officials

(a) DIRECTOR.—

(1) FUNCTIONS.—The Director of U.S. Citizenship and Immigration Services—

(A) shall establish the policies for performing the functions transferred to the Director by section 11171 of this title or the Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2135) or otherwise vested in the Director by law;

(B) shall oversee the administration of the policies;

(C) shall advise the Deputy Secretary of Homeland Security with respect to a policy or operation of U.S. Citizenship and Immigration Services that may affect U.S. Immigration and Customs Enforcement, including potentially conflicting policies or operations;

(D) shall establish national immigration services policies and priorities;

(E) shall meet regularly with the Ombudsman described in section 11173 of this title to correct serious service problems identified by the Ombudsman; and

(F) shall establish procedures requiring a formal response to recommendations submitted in the Ombudsman's annual report to Congress within 3 months after its submission to Congress.

(2) MANAGERIAL ROTATION PROGRAM.—The Director of U.S. Citizenship and Immigration Services shall design and implement a managerial rotation program under which employees of U.S. Citizenship and Immigration Services 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. Citizenship and Immigration Services; and

(B) work in at least one field office and one service center of U.S. Citizenship and Immigration Services.

(3) PILOT INITIATIVES FOR BACKLOG ELIMINATION.—The Director of U.S. Citizenship and Immigration Services may implement innovative pilot initiatives to eliminate a remaining backlog in the processing of immigration benefit applications, and to prevent a backlog in the processing of applications from recurring, under section 204(a) of the Immigration Services and Infrastructure Improvements Act of 2000 (8 U.S.C. 1573(a)). Initiatives may include measures such as increasing personnel, transferring personnel to focus on areas with the largest potential for backlog, and streamlining paperwork.

(b) CHIEF OF POLICY AND STRATEGY.—

(1) IN GENERAL.—There is a Chief of Policy and Strategy for U.S. Citizenship and Immigration Services.

(2) FUNCTIONS.—In consultation with U.S. Citizenship and Immigration Services personnel in field offices, the Chief of Policy and Strategy is responsible for—

(A) making policy recommendations and performing policy research and analysis on immigration services issues; and

(B) coordinating immigration policy issues with the Chief of Policy and Strategy for U.S. Immigration and Customs Enforcement.

(c) LEGAL ADVISOR.—

(1) IN GENERAL.—There is a principal legal advisor to the Director of U.S. Citizenship and Immigration Services.

(2) FUNCTIONS.—The legal advisor is responsible for—

(A) providing specialized legal advice, opinions, determinations, regulations, and other assistance to the Director of U.S. Citizenship and Immigration Services with respect to legal matters affecting U.S. Citizenship and Immigration Services; and

(B) representing U.S. Citizenship and Immigration Services in visa petition appeal proceedings before the Executive Office for Immigration Review.

(d) BUDGET OFFICER.—

(1) IN GENERAL.—There is a Budget Officer for U.S. Citizenship and Immigration Services.

(2) FUNCTIONS.—The Budget Officer is responsible for—

(A) formulating and executing the budget of U.S. Citizenship and Immigration Services;

(B) managing the finances of U.S. Citizenship and Immigration Services; and

(C) collecting all payments, fines, and other debts for U.S. Citizenship and Immigration Services.

(e) CHIEF OF OFFICE OF CITIZENSHIP.—

(1) IN GENERAL.—There is a Chief of the Office of Citizenship for U.S. Citizenship and Immigration Services.

(2) FUNCTIONS.—The Chief of the Office of Citizenship for U.S. Citizenship and Immigration Services is responsible for promoting instruction and training on citizenship responsibilities for aliens interested in becoming naturalized citizens of the United States, including the development of educational materials.

§ 11173. Citizenship and Immigration Services Ombudsman

(a) IN GENERAL.—There is in the Department a Citizenship and Immigration Services Ombudsman (in this section referred to as the ''Ombudsman''). The Ombudsman shall report directly to the Deputy Secretary of Homeland Security. The Ombudsman shall have a background in customer service as well as immigration law.

(b) FUNCTIONS.—The Ombudsman—

(1) shall assist individuals and employers in resolving problems with U.S. Citizenship and Immigration Services;

(2) shall identify areas in which individuals and employers have problems in dealing with U.S. Citizenship and Immigration Services; and

(3) to the extent possible, shall propose changes in the administrative practices of U.S. Citizenship and Immigration Services to mitigate problems identified under paragraph (2).

(c) ANNUAL REPORT.—

(1) OBJECTIVES.—Not later than June 30 each year, the Ombudsman shall report to the Committees on the Judiciary of the House of Representatives and the Senate on the objectives of the Office of the Ombudsman for the fiscal year beginning in that year. The report shall

contain full and substantive analysis, in addition to statistical information, and—

(A) shall identify the recommendations the Office of the Ombudsman has made on improving the services and responsiveness of U.S. Citizenship and Immigration Services;

(B) shall contain a summary of the most pervasive and serious problems encountered by individuals and employers, including a description of the nature of the problems;

(C) shall contain an inventory of the items described in subparagraphs (A) and (B) for which action has been taken and the result of the action;

(D) shall contain an inventory of the items described in subparagraphs (A) and (B) for which action remains to be completed and the period during which each item has remained on the inventory;

(E) shall contain an inventory of the items described in subparagraphs (A) and (B) for which no action has been taken, the period during which each item has remained on the inventory, and the reasons for the inaction, and shall identify any official of U.S. Citizenship and Immigration Services who is responsible for the inaction;

(F) shall contain recommendations for administrative action appropriate to resolve problems encountered by individuals and employers, including problems created by excessive backlogs in the adjudication and processing of immigration benefit petitions and applications; and

(G) shall include other information the Ombudsman may deem advisable.

(2) REPORT TO BE SUBMITTED DIRECTLY TO COMMITTEES.—Each report required under this subsection shall be provided directly to the committees described in paragraph (1) without prior comment or amendment from the Secretary, the Deputy Secretary of Homeland Security, the Director of U.S. Citizenship and Immigration Services, or another officer or employee of the Department or the Office of Management and Budget.

(d) OTHER RESPONSIBILITIES.—The Ombudsman—

(1) shall monitor the coverage and geographic allocation of local offices of the Ombudsman;

(2) shall develop guidance to be distributed to all officers and employees of U.S. Citizenship and Immigration Services outlining the criteria for referral of inquiries to local offices of the Ombudsman;

(3) shall ensure that the local telephone number for each local office of the Ombudsman is published and available to individuals and employers served by the office; and

(4) shall meet regularly with the Director of U.S. Citizenship and Immigration Services to identify serious service problems and to present recommendations for administrative action appropriate to resolve problems encountered by individuals and employers.

(e) PERSONNEL ACTIONS.—

(1) IN GENERAL.—The Ombudsman has the responsibility and authority—

(A) to appoint local ombudsmen and make available at least one ombudsman for each State; and

(B) to evaluate and take personnel actions (including dismissal) with respect to an employee of a local office of the Ombudsman.

(2) CONSULTATION.—The Ombudsman may consult with the appropriate supervisory personnel of U.S. Citizenship and Immigration Services in carrying out the Ombudsman's responsibilities under this subsection.

(f) RESPONSIBILITIES OF DIRECTOR OF U.S. CITIZENSHIP AND IMMIGRATION SERVICES.—The Director of U.S. Citizenship and Immigration Services shall establish procedures requiring a formal response to all recommendations submitted to the Director by the Ombudsman within 3 months after submission.

(g) OPERATION OF LOCAL OFFICES.—

(1) IN GENERAL.—Each local ombudsman—

(A) shall report to the Ombudsman or the delegate of the Ombudsman;

(B) may consult with the appropriate supervisory personnel of U.S. Citizenship and Immigration Services regarding the daily operation of the local office of the Ombudsman;

(C) shall, at the initial meeting with an individual or employer seeking the assistance of the local office, notify the individual or employer that the local offices of the Ombudsman operate independently 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.

§ 11174. 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 any 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.

§ 11175. Employee discipline

Notwithstanding another law, 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.

§ 11176. 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 law, Executive order, rule, regulation, delegation of authority, or document of or pertaining to a component of government from which the function is transferred—

(1) to the head of the component is deemed to refer to the Director of U.S. Citizenship and Immigration Services; or

(2) to the component is deemed to refer to U.S. Citizenship and Immigration Services.

(b) EXERCISE OF AUTHORITIES.—Except as otherwise provided by law, a Federal official to whom a function is transferred by this subchapter may, for purposes of performing the function, exercise all authorities under any other provision of law that were available with respect to the performance of that function to the official responsible for the performance of the function immediately before March 1, 2003.

§ 11177. Application of Internet-based technologies

(a) ESTABLISHMENT OF TRACKING SYSTEM.—The Secretary, in consultation with the Technology Advisory Committee established under subsection (c), shall establish an Internet-based system that will permit a person, employer, immigrant, or nonimmigrant who has filings with the Secretary for a benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.), access to online information about the processing status of the filing involved.

(b) FEASIBILITY STUDY FOR ONLINE FILING AND IMPROVED PROCESSING.—

(1) ONLINE FILING.—The Secretary, in consultation with the Technology Advisory Committee established under subsection (c), shall conduct a feasibility study on the online filing of the filings described in subsection (a). The study shall include a review of computerization and technology of U.S. Immigration and Customs Enforcement relating to immigration services and the processing of filings relating to immigrant services. The study shall also include an estimate of the time frame and cost and shall consider other factors in implementing the filing system, including the feasibility of fee payment online.

(2) REPORT.—A report on the study under this subsection shall be submitted to the Committees on the Judiciary of the House of Representatives and the Senate not later than January 24, 2004.

(c) TECHNOLOGY ADVISORY COMMITTEE.—

(1) ESTABLISHMENT.—The Secretary shall establish the Technology Advisory Committee to assist the Secretary in—

(A) establishing the tracking system under subsection (a); and

(B) conducting the study under subsection (b).

(2) CONSULTATION.—The Technology Advisory Committee shall be established after consultation with the Committees on the Judiciary of the House of Representatives and the Senate.

(3) COMPOSITION.—The Technology Advisory Committee shall be composed of representatives from high technology companies capable of establishing and implementing the tracking system described in subsection (a) in an expeditious manner, and representatives of persons

who may use the tracking system described in subsection (a) and the online filing system described in subsection (b)(1).

Subchapter V—General Immigration Provisions

§ 11191. Director of Shared Services

(a) IN GENERAL.—There is in the Office of the Deputy Secretary of Homeland Security a Director of Shared Services.

(b) FUNCTIONS.—The Director of Shared Services is responsible for the coordination of resources for U.S. Immigration and Customs Enforcement and U.S. Citizenship and Immigration Services, including—

(1) information resources management, including computer databases and information technology;

(2) records and file management; and

(3) forms management.

§ 11192. Separation of funding

(a) IN GENERAL.—There are in the Treasury separate accounts for appropriated funds and other deposits available for U.S. Citizenship and Immigration Services and U.S. Immigration and Customs Enforcement.

(b) SEPARATE BUDGETS.—To ensure that U.S. Citizenship and Immigration Services and U.S. Immigration and Customs Enforcement are funded to the extent necessary to fully carry out their respective functions, the Director of the Office of Management and Budget shall separate the budget requests for each entity.

(c) FEES.—Fees imposed for a particular service, application, or benefit shall be deposited in the account established under subsection (a) that is for whichever of U.S. Immigration and Customs Enforcement or U.S. Citizenship and Immigration Services has jurisdiction over the function to which the fee relates.

(d) FEES NOT TRANSFERABLE.—A fee may not be transferred between U.S. Citizenship and Immigration Services and U.S. Immigration and Customs Enforcement for purposes not authorized by section 286 of the Immigration and Nationality Act (8 U.S.C. 1356).

§ 11193. Annual immigration functions report

(a) ANNUAL REPORT.—The Secretary shall submit a report annually to the President, to the Committee on the Judiciary and the Committee on Oversight and Government Reform of the House of Representatives, and to the Committee on the Judiciary and the Committee on Homeland Security and Governmental Affairs of the Senate, on the impact the transfers made by Subtitle F of Title IV of the Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2205) have had on immigration functions.

(b) CONTENT.—The report shall address the following with respect to the period covered by the report:

(1) The aggregate number of all immigration applications and petitions received, and processed, by the Department.

(2) Region-by-region statistics on the aggregate number of immigration applications and petitions filed by an alien (or filed on behalf of an alien) and denied, disaggregated by category of denial and application or petition type.

(3) The quantity of backlogged immigration applications and petitions that have been processed, the aggregate number awaiting processing, and a detailed plan for eliminating the backlog.

(4) The average processing period for immigration applications and petitions, disaggregated by application or petition type.

(5) The number and types of immigration-related grievances filed with an official of the Department of Justice, and if those grievances were resolved.

(6) Plans to address grievances and improve immigration services.

(7) Whether immigration-related fees were used consistent with legal requirements regarding their use.

(8) Whether immigration-related questions conveyed by customers to the Department (whether conveyed in person, by telephone, or by means of the Internet) were answered effectively and efficiently.

Subchapter VI—U.S. Customs and Border Protection Public-Private Partnerships

§ 11201. Definitions

In this subchapter:

(1) DONOR.—The term ''donor'' means an entity that is proposing to make a donation under this title (except chapters 113 and 409).

(2) ENTITY.—The term ''entity'' means—

(A) a person;

(B) a partnership, corporation, trust, estate, cooperative, association, or other organized group of persons;

(C) the Federal Government or a State or local government (including a subdivision, agency, or instrumentality of the Federal Government or a State or local government); or

(D) another private person or governmental entity.

§ 11202. Fee agreements for certain services at ports of entry

(a) IN GENERAL.—Notwithstanding section 13031(e) of the Consolidated Omnibus Budget Reconciliation Act of 1985 (19 U.S.C. 58c(e)) and section 451 of the Tariff Act of 1930 (19 U.S.C. 1451), the Commissioner of U.S.

Customs and Border Protection, on request of any entity, may enter into a fee agreement with the entity under which—

(1) U. S. Customs and Border Protection shall provide services described in subsection (b) at a United States port of entry or any other facility at which U.S. Customs and Border Protection provides the services;

(2) the entity shall remit to U.S. Customs and Border Protection a fee imposed under subsection (h) in an amount equal to the full costs that are incurred or will be incurred in providing the services; and

(3) if space is provided by the entity, each facility at which U.S. Customs and Border Protection services are performed shall be maintained and equipped by the entity, without cost to the Federal Government, in accordance with U.S. Customs and Border Protection specifications.

(b) SERVICES DESCRIBED.—The services referred to in subsection (a) are activities of an employee or Office of Field Operations contractor of U.S. Customs and Border Protection (except employees of U.S. Border Patrol, as established under section 10306(e) of this title) pertaining to, or in support of, customs, agricultural processing, border security, or immigration inspection-related matters at a port of entry or other facility at which U.S. Customs and Border Protection provides or will provide the services.

(c) MODIFICATION OF PRIOR AGREEMENTS.—The Commissioner of U.S. Customs and Border Protection, at the request of an entity that has previously entered into an agreement with U.S. Customs and Border Protection for the reimbursement of fees in effect on December 16, 2016, may modify the agreement to implement provisions of this section.

(d) LIMITATIONS.—

(1) IMPACTS OF SERVICES.—The Commissioner of U.S. Customs and Border Protection—

(A) may enter into fee agreements under this section only for services that—

(i) will increase or enhance the operational capacity of U.S. Customs and Border Protection based on available staffing and workload; and

(ii) will not shift the cost of services funded in an appropriations Act, or provided from an account in the Treasury derived by the collection of fees, to entities under this title (except chapters 113 and 409); and

(B) may not enter into a fee agreement under this section if the agreement would unduly and permanently impact services funded

in an appropriations Act, or provided from an account in the Treasury, derived by the collection of fees.

(2) NO LIMIT.—There shall be no limit to the number of fee agreements that the Commissioner of U.S. Customs and Border Protection may enter into under this section.

(e) AIR PORTS OF ENTRY.—

(1) IN GENERAL.—Except as otherwise provided in this subsection, a fee agreement for U.S. Customs and Border Protection services at an air port of entry may only provide for the payment of overtime costs of U.S. Customs and Border Protection officers and salaries and expenses of U.S. Customs and Border Protection employees to support U.S. Customs and Border Protection officers in performing services described in subsection (b).

(2) SMALL AIRPORTS.—Notwithstanding paragraph (1), U.S. Customs and Border Protection may receive reimbursement in addition to overtime costs if the fee agreement is for services at an air port of entry that has fewer than 100,000 arriving international passengers annually.

(3) COVERED SERVICES.—In addition to costs described in paragraph (1), a fee agreement for U.S. Customs and Border Protection services at an air port of entry referred to in paragraph (2) may provide for the reimbursement of—

(A) salaries and expenses of not more than 5 fulltime equivalent U.S. Customs and Border Protection officers beyond the number of officers assigned to the port of entry on the date on which the fee agreement was signed;

(B) salaries and expenses of employees of U.S. Customs and Border Protection, other than the officers referred to in subparagraph (A), to support U.S. Customs and Border Protection officers in performing law enforcement functions; and

(C) other costs incurred by U.S. Customs and Border Protection relating to services described in subparagraph (B), such as temporary placement or permanent relocation of employees, including incentive pay for relocation, as appropriate.

(f) PORT OF ENTRY SIZE NOT A FACTOR.—The Commissioner of U.S. Customs and Border Protection shall ensure that each fee agreement proposal is given equal consideration regardless of the size of the port of entry.

(g) DENIED APPLICATION.—

(1) IN GENERAL.—If the Commissioner of U.S. Customs and Border Protection denies a proposal for a fee agreement under this section, the

Commissioner shall provide the entity submitting the proposal with the reason for the denial unless—

(A) the reason for the denial is law enforcement sensitive; or

(B) withholding the reason for the denial is in the national security interests of the United States.

(2) JUDICIAL REVIEW.—Decisions of the Commissioner of U.S. Customs and Border Protection under paragraph (1) are in the discretion of the Commissioner of U.S. Customs and Border Protection and are not subject to judicial review.

(h) FEE.—

(1) IN GENERAL.—The amount of the fee to be charged under an agreement authorized under subsection (a) shall be paid by each entity requesting U.S. Customs and Border Protection services, and shall be for the full cost of providing the services, including the salaries and expenses of employees and contractors of U.S. Customs and Border Protection, to provide the services and other costs incurred by U.S. Customs and Border Protection relating to the services, such as temporary or permanent relocation of the employees and contractors.

(2) TIMING.—The Commissioner of U.S. Customs and Border Protection may require that the fee referred to in paragraph (1) be paid by each entity that has entered into a fee agreement under subsection (a) with U.S. Customs and Border Protection in advance of the performance of U.S. Customs and Border Protection services.

(3) OVERSIGHT.—The Commissioner of U.S. Customs and Border Protection shall develop a process to oversee the services for which fees are charged pursuant to an agreement under subsection (a), including—

(A) a determination and report on the full costs of providing the services, and a process for increasing the fees, as necessary;

(B) the establishment of a periodic remittance schedule to replenish appropriations, accounts, or funds, as necessary; and

(C) the identification of costs paid by the fees.

(i) DEPOSIT OF FUNDS.—

(1) ACCOUNT.—Funds collected pursuant to an agreement entered into pursuant to subsection (a)—

(A) shall be deposited as offsetting collections;

(B) shall remain available until expended without fiscal year limitation; and

(C) shall be credited to the applicable appropriation, account, or fund for the amount paid out of the appropriation, account, or fund for any expenses incurred or to be incurred by U.S. Customs

and Border Protection in providing U.S. Customs and Border Protection services under the agreement and for any other costs incurred or to be incurred by U.S. Customs and Border Protection relating to the services.

(2) RETURN OF UNUSED FUNDS.—The Commissioner of U.S. Customs and Border Protection shall return any unused funds collected and deposited in the account described in paragraph (1) if a fee agreement entered into pursuant to subsection (a) is terminated for any reason or the terms of the fee agreement change by mutual agreement to cause a reduction of U.S. Customs and Border Protection services. No interest shall be owed on the return of the unused funds.

(j) TERMINATION.—

(1) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection shall terminate the services provided pursuant to a fee agreement entered into under subsection (a) with an entity that, after receiving notice from the Commissioner of U.S. Customs and Border Protection that a fee under subsection (h) is due, fails to pay the fee in a timely manner. If the services are terminated, all costs incurred by U.S. Customs and Border Protection that have not been paid shall become immediately due and payable. Interest on unpaid fees shall accrue based on the rate and amount established under sections 6621 and 6622 of the Internal Revenue Code of 1986 (26 U.S.C. 6621, 6622).

(2) PENALTY.—An entity that, after notice and demand for payment of a fee under subsection (h), fails to pay the fee in a timely manner shall be liable for a penalty or liquidated damage equal to 2 times the amount of the fee. The amount collected under this paragraph shall be deposited into the appropriate account specified under subsection (i) and shall be available as described in subsection (i).

(3) TERMINATION BY THE ENTITY.—An entity that has previously entered into an agreement with U.S. Customs and Border Protection for the reimbursement of fees in effect on December 16, 2016, or under this section, may request that the agreement be amended to provide for termination on advance notice, length, and terms that are negotiated between the entity and U.S. Customs and Border Protection.

(k) ANNUAL REPORT.—The Commissioner of U.S. Customs and Border Protection shall—

(1) submit an annual report identifying the activities undertaken and the agreements entered into pursuant to this section to—

(A) the Committee on Appropriations of the Senate;

(B) the Committee on Finance of the Senate;

(C) the Committee on Homeland Security and Governmental Affairs of the Senate;

(D) the Committee on the Judiciary of the Senate;

(E) the Committee on Appropriations of the House of Representatives;

(F) the Committee on Homeland Security of the House of Representatives;

(G) the Committee on the Judiciary of the House of Representatives; and

(H) the Committee on Ways and Means of the House of Representatives; and

(2) not later than 15 days before entering into a fee agreement, notify the members of Congress who represent the State or congressional district in which the affected port of entry or facility is located of the agreement.

(l) RULE OF CONSTRUCTION.—Nothing in this section may be construed as imposing on U.S. Customs and Border Protection any responsibilities, duties, or authorities relating to real property.

§ 11203. Port of entry donation authority

(a) PERSONAL PROPERTY, MONEY, OR NONPERSONAL SERVICES.—

(1) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection, in consultation with the Administrator of General Services, may enter into an agreement with an entity to accept a donation of personal property, money, or nonpersonal services for the uses described in paragraph (3) only with respect to the following locations at which U.S. Customs and Border Protection performs or will be performing inspection services:

(A) A new or existing sea or air port of entry.

(B) An existing Federal Government-owned or -leased land port of entry.

(C) A new Federal Government-owned or -leased land port of entry if—

(i) the fair market value of the donation is $75,000,000 or less; and

(ii) the fair market value of donations with respect to the land port of entry total $75,000,000 or less over the preceding 5 years.

(2) LIMITATION ON MONETARY DONATIONS.—A monetary donation accepted pursuant to this subsection may not be used to pay the salaries of U.S. Customs and Border Protection employees performing inspection services.

(3) USES.—Donations accepted pursuant to this subsection may be used for activities of the Office of Field Operations, set forth in subparagraphs (A) through (F) of section 10306(g)(3) of this title, that are related to a new or existing sea or air port of entry or a new or existing Federal Government-owned or -leased land port of entry described in paragraph (1), including expenses relating to—

(A) furniture, fixtures, equipment, or technology, including the installation or deployment of those items; and

(B) the operation and maintenance of the furniture, fixtures, equipment, or technology.

(b) REAL PROPERTY OR MONEY.—

(1) IN GENERAL.—Subject to paragraph (3), the Commissioner of U.S. Customs and Border Protection, and the Administrator of General Services, as applicable, may enter into an agreement with an entity to accept a donation of real property or money for uses described in paragraph (2) only with respect to the following locations at which U.S. Customs and Border Protection performs or will be performing inspection services:

(A) A new or existing sea or air port of entry.

(B) An existing Federal Government-owned land port of entry.

(C) A new Federal Government-owned land port of entry if—

(i) the fair market value of the donation is $75,000,000 or less; and

(ii) the fair market value with respect to the land port of entry total $75,000,000 or less over the preceding 5 years.

(2) USES.—Donations accepted pursuant to this subsection may be used for activities of the Office of Field Operations set forth in section 10306(g) of this title that are related to the construction, alteration, operation, or maintenance of a new or existing sea or air port of entry or a new or existing Federal Government-owned land port of entry described in paragraph (1), including expenses related to—

(A) land acquisition, design, construction, repair, or alteration; and

(B) operation and maintenance of the port of entry facility.

(3) LIMITATION ON REAL PROPERTY DONATIONS.—A donation of real property under this subsection at an existing land port of entry owned by the General Services Administration may only be accepted by the Administrator of General Services.

(4) SUNSET.—

(A) IN GENERAL.—The authority to enter into an agreement under this subsection shall terminate on December 31, 2026.

(B) RULE OF CONSTRUCTION.—The termination date referred to in subparagraph (A) shall not apply to a proposal accepted for consideration by U.S. Customs and Border Protection or the General Services Administration pursuant to this section or a prior pilot program prior to December 31, 2026.

(c) GENERAL PROVISIONS.—

(1) DURATION.—An agreement entered into under subsection (a) or (b) (and in the case of subsection (b), in accordance with paragraph (4) of subsection (b)) may last as long as required to meet the terms of the agreement.

(2) CRITERIA.—In carrying out an agreement entered into under subsection (a) or (b), the Commissioner of U.S. Customs and Border Protection, in consultation with the Administrator of General Services, shall establish criteria regarding—

(A) the selection and evaluation of donors;

(B) the identification of roles and responsibilities between U.S. Customs and Border Protection, the General Services Administration, and donors;

(C) the identification, allocation, and management of explicit and implicit risks of partnering between the Federal Government and donors;

(D) decision-making and dispute resolution processes; and

(E) processes for U.S. Customs and Border Protection, and the General Services Administration, as applicable, to terminate agreements if selected donors are not meeting the terms of the agreement, including the security standards established by U.S. Customs and Border Protection.

(3) EVALUATION PROCEDURES.—

(A) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection, in consultation with the Administrator of General Services, as applicable, shall—

(i) establish criteria for evaluating a proposal to enter into an agreement under subsection (a) or (b); and

(ii) make the criteria publicly available.

(B) CONSIDERATIONS.—Criteria established pursuant to subparagraph (A) shall consider—

(i) the impact of a proposal referred to in subparagraph (A) on the land, sea, or air port of entry at issue and other ports of entry or similar facilities or other infrastructure near the location of the proposed donation;

(ii) the proposal's potential to increase trade and travel efficiency through added capacity;

(iii) the proposal's potential to enhance the security of the port of entry at issue;

(iv) the impact of the proposal on reducing wait times at the port of entry or facility and other ports of entry on the same border;

(v) for a donation under subsection (b)—

(I) whether the donation satisfies the requirements of the proposal or whether additional real property would be required; and

(II) how the donation was acquired, including if eminent domain was used;

(vi) the funding available to complete the intended use of the donation;

(vii) the costs of maintaining and operating the donation;

(viii) the impact of the proposal on U.S. Customs and Border Protection staffing requirements; and

(ix) other factors that the Commissioner of U.S. Customs and Border Protection or the Administrator of General Services determines to be relevant.

(C) DETERMINATION AND NOTIFICATION.—

(i) INCOMPLETE PROPOSALS.—

(I) IN GENERAL.—Not later than 60 days after receiving the proposals for a donation agreement from an entity, the Commissioner of U.S. Customs and Border Protection shall notify the entity as to whether the proposal is complete or incomplete.

(II) RESUBMISSION.—If the Commissioner of U.S. Customs and Border Protection determines that a proposal is incomplete, the Commissioner shall—

(aa) notify the appropriate entity and provide the entity with a description of all information or material that is needed to complete review of the proposal; and

(bb) allow the entity to resubmit the proposal with additional information and material described in item (aa) to complete the proposal.

(ii) COMPLETE PROPOSAL.—Not later than 180 days after receiving a completed proposal to enter into an agreement under subsection (a) or (b), the Commissioner of U.S. Cus-

toms and Border Protection, with the concurrence of the Administrator of General Services, as applicable, shall—

(I) determine whether to approve or deny the proposal; and

(II) notify the entity that submitted the proposal of the determination.

(4) SUPPLEMENTAL FUNDING.—Except as required under section 3307 of title 40, real property donations to the Administrator of General Services made pursuant to subsection (b) at a GSA-owned land port of entry may be used in addition to any other funding for the port of entry, including appropriated funds, property, or services.

(5) RETURN OF DONATIONS.—The Commissioner of U.S. Customs and Border Protection, or the Administrator of General Services, as applicable, may return a donation made pursuant to subsection (a) or (b). No interest shall be owed to the donor with respect to any donation provided under subsection (a) or (b) that is returned pursuant to this subsection.

(6) PROHIBITION ON CERTAIN FUNDING.—

(A) IN GENERAL.—Except as provided in subsections (a) and (b) regarding the acceptance of donations, the Commissioner of U.S. Customs and Border Protection and the Administrator of General Services, as applicable, may not, with respect to an agreement entered into under subsection (a) or (b), obligate or expend amounts in excess of amounts that have been appropriated pursuant to any appropriations Act for purposes specified in subsection (a) or (b) or otherwise made available for those purposes.

(B) CERTIFICATION REQUIREMENT.—Before accepting any donations pursuant to an agreement under subsection (a) or (b), the Commissioner of U.S. Customs and Border Protection shall certify to the congressional committees set forth in paragraph (7) that—

(i) the donation will not be used for the construction of a detention facility or a border fence or wall; or

(ii) the donor will be notified in the Donations Acceptance Agreement that the donor shall be financially responsible for all costs and operating expenses related to the operation, maintenance, and repair of the donated real property until such time as U.S. Customs and Border Protection provides the donor written notice otherwise.

(7) REPORTS BY COMMISSIONER OF U.S. CUSTOMS AND BORDER PROTECTION AND ADMINISTRATOR OF GENERAL SERVICES.—The Commissioner of U.S. Customs and Border Protection, in collaboration with

the Administrator of General Services, as applicable, shall submit an annual report identifying the activities undertaken and agreements entered into pursuant to subsections (a) and (b) to—

(A) the Committee on Appropriations of the Senate;

(B) the Committee on Environment and Public Works of the Senate;

(C) the Committee on Finance of the Senate;

(D) the Committee on Homeland Security and Governmental Affairs of the Senate;

(E) the Committee on the Judiciary of the Senate;

(F) the Committee on Appropriations of the House of Representatives;

(G) the Committee on Homeland Security of the House of Representatives;

(H) the Committee on the Judiciary of the House of Representatives;

(I) the Committee on Transportation and Infrastructure of the House of Representatives; and

(J) the Committee on Ways and Means of the House of Representatives.

(d) REPORT BY COMPTROLLER GENERAL.—The Comptroller General shall submit a biennial report to the congressional committees referred to in subsection (c)(7) that evaluates—

(1) fee agreements entered into pursuant to section 11202 of this title;

(2) donation agreements entered into pursuant to subsections (a) and (b); and

(3) the fees and donations received by U. S. Customs and Border Protection pursuant to the agreements.

(e) JUDICIAL REVIEW.—Decisions of the Commissioner of U.S. Customs and Border Protection and the Administrator of General Services under this section regarding the acceptance of real or personal property are in the discretion of the Commissioner of U.S. Customs and Border Protection and the Administrator of General Services, and are not subject to judicial review.

(f) RULE OF CONSTRUCTION.—Except as otherwise provided in this section, nothing in this section may be construed as affecting in any manner the responsibilities, duties, or authorities of U.S. Customs and Border Protection or the General Services Administration.

§ 11204. Current and proposed agreements

Nothing in this subchapter or in section 4 of the Cross-Border Trade Enhancement Act of 2016 (Public Law 114–279, 130 Stat. 1422) may be construed as affecting—

(1) any agreement entered into pursuant to section 560 of the Department of Homeland Security Appropriations Act, 2013 (Public Law 113–6, 127 Stat. 378) or section 559 of the Department of Homeland Security Appropriations Act, 2014 (Public Law 113–76, 128 Stat. 279) as in existence on December 15, 2016, and the agreement shall continue to have full force and effect on and after December 15, 2016; or

(2) a proposal accepted for consideration by U.S. Customs and Border Protection pursuant to section 559 of the Department of Homeland Security Appropriations Act, 2014 (Public Law 113–76, 128 Stat. 279) as in existence on December 15, 2016.

Subchapter VII—Miscellaneous Provisions

§ 11211. Coordination of information and information technology

(a) DEFINITION OF AFFECTED AGENCY.—In this section, the term ''affected agency'' means—

(1) the Department;

(2) the Department of Agriculture;

(3) the Department of Health and Human Services; and

(4) any other department or agency determined to be appropriate by the Secretary.

(b) COORDINATION.—The Secretary, in coordination with the Secretary of Agriculture, the Secretary of Health and Human Services, and the head of each other department or agency determined to be appropriate by the Secretary, shall ensure that appropriate information (as determined by the Secretary) concerning inspections of articles that are imported or entered into the United States, and are inspected or regulated by one or more affected agencies, is timely and efficiently exchanged between the affected agencies.

§ 11212. Visa issuance

(a) DEFINITION OF CONSULAR OFFICER.—In this section, the term ''consular officer'' has the meaning given the term under section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)).

(b) IN GENERAL.—Notwithstanding section 104(a) of the Immigration and Nationality Act (8 U.S.C. 1104(a)) or any other law, and except as provided in subsection (c) of this section, the Secretary—

(1) shall be vested exclusively with all authorities to issue regulations with respect to, to administer, and to enforce the Immigration and Na-

tionality Act (8 U.S.C. 1101 et seq.), and of all other immigration and nationality laws, relating to the functions of consular officers of the United States in connection with the granting or refusal of visas, and shall have the authority to refuse visas in accordance with law and to develop programs of homeland security training for consular officers (in addition to consular training provided by the Secretary of State), which authorities shall be exercised through the Secretary of State, except that the Secretary shall not have authority to alter or reverse the decision of a consular officer to refuse a visa to an alien; and

(2) shall have authority to confer or impose upon an officer or employee of the United States, with the consent of the head of the executive agency under whose jurisdiction the officer or employee is serving, any of the functions specified in paragraph (1).

(c) AUTHORITY OF THE SECRETARY OF STATE.—

(1) IN GENERAL.—Notwithstanding subsection (b), the Secretary of State may direct a consular officer to refuse a visa to an alien if the Secretary of State deems the refusal necessary or advisable in the foreign policy or security interests of the United States.

(2) CONSTRUCTION REGARDING AUTHORITY.—Nothing in this section, consistent with the Secretary of Homeland Security's authority to refuse visas in accordance with law, shall be construed as affecting the authorities of the Secretary of State under the following provisions of law:

(A) Section 101(a)(15)(A) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)(A)).

(B) Section 204(d)(2) of the Immigration and Nationality Act (8 U.S.C. 1154(d)(2)) (as it will take effect upon the entry into force of the Convention on Protection of Children and Cooperation in Respect to Inter-Country adoption).

(C) Section 212(a)(3)(B)(i)(IV)(bb) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(i)(IV)(bb)).

(D) Section 212(a)(3)(B)(i)(VI) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(i)(VI)).

(E) Section 212(a)(3)(B)(vi)(II) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(vi)(II)).

(F) Section 212(a)(3)(C) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(C)).

(G) Section 212(a)(10)(C) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(10)(C)).

(H) Section 212(f) of the Immigration and Nationality Act (8 U.S.C. 1182(f)).

(I) Section 801 of the Admiral James W. Nance and Meg Donovan Foreign Relations Authorization Act, Fiscal Years 2000 and 2001 (8 U.S.C. 1182e).

(J) Section 219(a) of the Immigration and Nationality Act (8 U.S.C. 1189(a)).

(K) Section 237(a)(4)(C) of the Immigration and Nationality Act (8 U.S.C. 1227(a)(4)(C)).

(L) Section 51 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2723).

(M) Section 401 of the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996 (22 U.S.C. 6091).

(N) Section 103(f) of the Chemical Weapons Convention Implementation Act of 1998 (22 U.S.C. 6713(f)).

(O) Section 616 of the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 1999 (section 101(b) of division A of the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Public Law 105–277, 112 Stat. 2681–114).

(P) Section 568 of the Foreign Operations, Export Financing, and Related Programs Appropriations Act, 2002 (Public Law 107–115, 115 Stat. 2166).

(d) CONSULAR OFFICERS AND CHIEFS OF MISSIONS.—

(1) IN GENERAL.—Nothing in this section may be construed to alter or affect—

(A) the employment status of consular officers as employees of the Department of State; or

(B) the authority of a chief of mission under section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927).

(2) CONSTRUCTION REGARDING DELEGATION OF AUTHORITY.—Nothing in this section shall be construed to affect any delegation of authority to the Secretary of State by the President pursuant to any proclamation issued under section 212(f) of the Immigration and Nationality Act (8 U.S.C. 1182(f)), consistent with the Secretary of Homeland Security's authority to refuse visas in accordance with law.

(e) ASSIGNMENT OF DEPARTMENT EMPLOYEES TO DIPLOMATIC AND CONSULAR POSTS.—

(1) IN GENERAL.—The Secretary may assign employees of the Department to each diplomatic and consular post at which visas are issued, unless the Secretary determines that an assignment at a particular post would not promote homeland security.

(2) FUNCTIONS.—Employees assigned under paragraph (1) shall—

(A) provide expert advice and training to consular officers regarding specific security threats relating to the adjudication of individual visa applications or classes of applications;

(B) review applications, either on the initiative of the employee of the Department or upon request by a consular officer or other person charged with adjudicating applications; and

(C) conduct investigations with respect to consular matters under the jurisdiction of the Secretary.

(3) EVALUATION OF CONSULAR OFFICERS.—The Secretary of State shall evaluate, in consultation with the Secretary, as considered appropriate by the Secretary, the performance of consular officers with respect to the processing and adjudication of applications for visas in accordance with performance standards developed by the Secretary for these procedures.

(4) REPORT.—The Secretary shall, on an annual basis, submit a report to Congress that describes the basis for each determination under paragraph (1) that the assignment of an employee of the Department at a particular diplomatic post would not promote homeland security.

(5) PERMANENT ASSIGNMENT; PARTICIPATION IN TERRORIST LOOKOUT COMMITTEE.—When appropriate, employees of the Department assigned to perform functions described in paragraph (2) may be assigned permanently to overseas diplomatic or consular posts with country-specific or regional responsibility. If the Secretary so directs, an employee, when present at an overseas post, shall participate in the terrorist lookout committee established under section 304 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (8 U.S.C. 1733).

(6) TRAINING AND HIRING.—

(A) IN GENERAL.—The Secretary shall ensure, to the extent possible, that employees of the Department assigned to perform functions under paragraph (2) and, as appropriate, consular officers, shall be provided the necessary training to enable them to carry out the functions, including training in foreign languages, interview techniques, and fraud detection techniques, in conditions in the particular country where each employee is assigned, and in other appropriate areas of study.

(B) USE OF CENTER.—The Secretary may use the George P. Shultz National Foreign Affairs Training Center, on a reimbursable basis, to obtain the training described in subparagraph (A).

(f) NO CREATION OF PRIVATE RIGHT OF ACTION.—Nothing in this section shall be construed to create or authorize a private right of action to

challenge a decision of a consular officer or other United States official or employee to grant or deny a visa.

(g) VISA ISSUANCE PROGRAM FOR SAUDI ARABIA.—On-site personnel of the Department shall review all visa applications for Saudi Arabia prior to adjudication.

§ 11213. Information on visa denials required to be entered into electronic data system

(a) IN GENERAL.—Whenever a consular officer of the United States denies a visa to an applicant, the consular officer shall enter the fact and the basis of the denial and the name of the applicant into the interoperable electronic data system implemented under section 202(a) of the Enhanced Border Security and Visa Entry Reform Act of 2002 (8 U.S.C. 1722(a)).

(b) PROHIBITION.—In the case of an alien with respect to whom a visa has been denied under subsection (a)—

(1) no subsequent visa may be issued to the alien unless the consular officer considering the alien's visa application has reviewed the information concerning the alien placed in the interoperable electronic data system, has indicated on the alien's application that the information has been reviewed, and has stated for the record why the visa is being issued or a waiver of visa ineligibility recommended in spite of that information; and

(2) the alien may not be admitted to the United States without a visa issued in accordance with the procedures described in paragraph (1).

§ 11214. Purpose and responsibilities of Office of Cargo Security Policy

(a) PURPOSES.—The Office of Cargo Security Policy—

(1) coordinates all Department policies relating to cargo security; and

(2) consults with stakeholders and coordinates with other Federal agencies in the establishment of standards and regulations and the promotion of best practices.

(b) RESPONSIBILITIES OF DIRECTOR.—The Director of the Office of Cargo Security Policy—

(1) advises the Assistant Secretary for Policy in the development of Department-wide policies regarding cargo security;

(2) coordinates all policies relating to cargo security among the agencies and offices within the Department relating to cargo security; and

(3) coordinates the cargo security policies of the Department with the policies of other executive agencies.

(c) RELATIONSHIP WITH COAST GUARD.—Nothing in this section shall be construed to affect—

(1) the authorities, functions, or capabilities of the Coast Guard to perform its missions; or

(2) the requirement under section 10312 of this title that those authorities, functions, and capabilities be maintained intact.

§ 11215. Purpose, composition, and operation of Border Enforcement Security Task Force

(a) PURPOSE.—The purpose of the Border Enforcement Security Task Force (in this section referred to as "BEST") is to establish units to enhance border security by addressing and reducing border security threats and violence by—

(1) facilitating collaboration among Federal, State, local, tribal, and foreign law enforcement agencies to execute coordinated activities in furtherance of border security, and homeland security; and

(2) enhancing information sharing, including the dissemination of homeland security information among these agencies.

(b) COMPOSITION AND ESTABLISHMENT OF UNITS.—

(1) COMPOSITION.—BEST units may be comprised of personnel from—

(A) U.S. Immigration and Customs Enforcement;

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

(C) the Coast Guard;

(D) other Department personnel, as appropriate;

(E) other Federal agencies, as appropriate;

(F) appropriate State law enforcement agencies;

(G) foreign law enforcement agencies, as appropriate;

(H) local law enforcement agencies from affected border cities and communities; and

(I) appropriate tribal law enforcement agencies.

(2) ESTABLISHMENT.—The Secretary may establish BEST units in jurisdictions in which the units can contribute to BEST missions, as appropriate. Before establishing a BEST unit, the Secretary shall consider—

(A) whether the area in which the BEST unit would be established is significantly impacted by cross-border threats;

(B) the availability of Federal, State, local, tribal, and foreign law enforcement resources to participate in the BEST unit;

(C) the extent to which border security threats are having a significant harmful impact in the jurisdiction in which the BEST

unit is to be established, and in other jurisdictions in the country; and

(D) whether or not an Integrated Border Enforcement Team already exists in the area in which the BEST unit would be established.

(3) DUPLICATION OF EFFORTS.—In determining whether to establish a new BEST unit or to expand an existing BEST unit in a given jurisdiction, the Secretary shall ensure that the BEST unit under consideration does not duplicate the efforts of other existing interagency task forces or centers within that jurisdiction.

(c) OPERATION.—After determining the jurisdictions in which to establish BEST units under subsection (b)(2), and in order to provide Federal assistance to the jurisdictions, the Secretary may—

(1) direct the assignment of Federal personnel to BEST, subject to the approval of the head of the department or agency that employs such personnel; and

(2) take other actions to assist Federal, State, local, and tribal entities to participate in BEST, including providing financial assistance, as appropriate, for operational, administrative, salary reimbursement, and technological costs associated with the participation of Federal, State, local, and tribal law enforcement agencies in BEST

(d) REPORT.—Not later than June 6, 2017, and 2018, the Secretary shall submit a report to Congress that describes the effectiveness of BEST in enhancing border security and reducing the drug trafficking, arms smuggling, illegal alien trafficking and smuggling, violence, and kidnapping along and across the international borders of the United States, as measured by crime statistics, including violent deaths, incidents of violence, and drug-related arrests.

§ 11216. Cyber Crimes Center

(a) IN GENERAL.—

(1) ESTABLISHMENT.—The Secretary shall operate, in U.S. Immigration and Customs Enforcement, Homeland Security Investigations, a Cyber Crimes Center (in this section referred to as the ''Center'').

(2) PURPOSE.—The Center shall provide investigative assistance, training, and equipment to support domestic and international investigations of cyber-related crimes by the Department.

(b) CHILD EXPLOITATION INVESTIGATIONS UNIT

(1) IN GENERAL.—The Secretary shall operate, in the Center, a Child Exploitation Investigations Unit (in this subsection referred to as the ''CEIU'').

(2) FUNCTIONS.—The CEIU—

(A) shall coordinate all U.S. Immigration and Customs Enforcement child exploitation initiatives, including investigations into—

(i) child exploitation;

(ii) child pornography;

(iii) child victim identification;

(iv) traveling child sex offenders; and

(v) forced child labor, including the sexual exploitation of minors;

(B) shall, among other things, focus on—

(i) child exploitation prevention;

(ii) investigative capacity building;

(iii) enforcement operations; and

(iv) training for Federal, State, local, tribal, and foreign law enforcement agency personnel, on request;

(C) shall provide training, technical expertise, support, or coordination of child exploitation investigations, as needed, to cooperating law enforcement agencies and personnel, which shall include participating in training for Homeland Security Investigations personnel conducted by Internet Crimes Against Children Task Force;

(D) shall provide psychological support and counseling services for U.S. Immigration and Customs Enforcement personnel engaged in child exploitation prevention initiatives, including making available other existing services to assist employees who are exposed to child exploitation material during investigations;

(E) may collaborate with the Department of Defense and the National Association to Protect Children for the purpose of the recruiting, training, equipping and hiring of wounded, ill, and injured veterans and transitioning service members, through the Human Exploitation Rescue Operative (HERO) Child-Rescue Corps Program; and

(F) shall collaborate with other governmental, nongovernmental, and nonprofit entities approved by the Secretary for the sponsorship of, and participation in, outreach and training activities.

(3) DATA COLLECTION.—The CEIU shall collect and maintain data concerning—

(A) the total number of suspects identified by U.S. Immigration and Customs Enforcement;

(B) the number of arrests by U.S. Immigration and Customs Enforcement in child exploitation investigations, disaggregated by type, including—

(i) the number of child victims identified through investigations carried out by U.S. Immigration and Customs Enforcement; and

(ii) the number of suspects arrested who were in positions of trust or authority over children;

(C) the number of child exploitation cases opened for investigation by U.S. Immigration and Customs Enforcement; and

(D) the number of child exploitation cases resulting in a Federal, State, foreign, or military prosecution.

(4) AVAILABILITY OF DATA TO CONGRESS.—In addition to submitting the reports required under paragraph (7), the CEIU shall make the data collected and maintained under paragraph (3) available to the committees of Congress described in paragraph (7).

(5) COOPERATIVE AGREEMENTS.—The CEIU may enter into cooperative agreements to accomplish the functions set forth in paragraphs (2) and (3).

(6) ACCEPTANCE OF GIFTS.—

(A) IN GENERAL.—The Secretary may accept money and in-kind donations from the Virtual Global Taskforce, national laboratories, Federal agencies, not-for-profit organizations, and educational institutions to create and expand public awareness campaigns in support of the functions of the CEIU.

(B) EXEMPTION FROM FEDERAL ACQUISITION REGULATION.—Gifts authorized under subparagraph (A) are not subject to the Federal Acquisition Regulation for competition when the services provided by the entities referred to in subparagraph (A) are donated or of minimal cost to the Department.

(7) REPORTS.—Not later than May 29, 2017, 2018, 2019, and 2020, the CEIU shall—

(A) submit a report containing a summary of the data collected pursuant to paragraph (3) during the previous year to—

(i) the Committee on Homeland Security and Governmental Affairs of the Senate;

(ii) the Committee on the Judiciary of the Senate;

(iii) the Committee on Appropriations of the Senate;

(iv) the Committee on Homeland Security of the House of Representatives;

(v) the Committee on the Judiciary of the House of Representatives; and

(vi) the Committee on Appropriations of the House of Representatives; and

(B) make a copy of each report submitted under subparagraph (A) publicly available on the website of the Department.

(c) COMPUTER FORENSICS UNIT.—

(1) IN GENERAL.—The Secretary shall operate, in the Center, a Computer Forensics Unit (in this subsection referred to as the ''CFU'').

(2) FUNCTIONS.—The CFU—

(A) shall provide training and technical support in digital forensics and administer the Digital Forensics and Document and Media Exploitation program to—

(i) U.S. Immigration and Customs Enforcement personnel; and

(ii) Federal, State, local, tribal, military, and foreign law enforcement agency personnel engaged in the investigation of crimes within their respective jurisdictions, on request and subject to the availability of funds;

(B) shall provide computer hardware, software, and forensic licenses for all computer forensics personnel in U.S. Immigration and Customs Enforcement;

(C) shall participate in research and development in the area of digital forensics and emerging technologies, in coordination with appropriate components of the Department; and

(D) may collaborate with the Department of Defense, the National Association to Protect Children, and other governmental entities for the purpose of recruiting, training, equipping, and hiring wounded, ill, and injured veterans and transitioning service members, through the Human Exploitation Rescue Operative (HERO) Child-Rescue Corps Program.

(3) COOPERATIVE AGREEMENTS.—The CFU may enter into cooperative agreements to accomplish the functions set forth in paragraph (2).

(4) ACCEPTANCE OF GIFTS.—

(A) IN GENERAL.—The Secretary may accept money and in-kind donations from the Virtual Global Task Force, national laboratories, Federal agencies, not-for-profit organizations, and educational institutions to create and expand public awareness campaigns in support of the functions of the CFU.

(B) EXEMPTION FROM FEDERAL ACQUISITION REGULATION.—Gifts authorized under subparagraph (A) are not subject to the Federal Acquisition Regulation for competition when the services provided by the entities referred to in subparagraph (A) are donated or of minimal cost to the Department.

(d) CYBER CRIMES UNIT.—

(1) IN GENERAL.—The Secretary shall operate, in the Center, a Cyber Crimes Unit (in this subsection referred to as the ''CCU'').

(2) FUNCTIONS.—The CCU—

(A) shall oversee the cyber security strategy and cyber-related operations and programs for U.S. Immigration and Customs Enforcement;

(B) shall enhance U.S. Immigration and Customs Enforcement's ability to combat criminal enterprises operating on or through the Internet, with specific focus in the areas of—

(i) cyber economic crime;

(ii) digital theft of intellectual property;

(iii) illicit e-commerce (including hidden marketplaces);

(iv) Internet-facilitated proliferation of arms and strategic technology; and

(v) cyber-enabled smuggling and money laundering;

(C) shall provide training and technical support in cyber investigations to—

(i) U.S. Immigration and Customs Enforcement personnel; and

(ii) Federal, State, local, tribal, military, and foreign law enforcement agency personnel engaged in the investigation of crimes within their respective jurisdictions, on request and subject to the availability of funds;

(D) shall participate in research and development in the area of cyber investigations, in coordination with appropriate components of the Department; and

(E) may recruit participants of the Human Exploitation Rescue Operative (HERO) Child-Rescue Corps Program for investigative and forensic positions in support of the functions of the CCU.

(3) COOPERATIVE AGREEMENTS.—The CCU may enter into cooperative agreements to accomplish the functions set forth in paragraph (2).

(e) HUMAN EXPLOITATION RESCUE OPERATIVE CHILD-RESCUE CORPS PROGRAM.—

(1) ESTABLISHMENT.—

(A) IN GENERAL.—There is in the Center a Human Exploitation Rescue Operative Child-Rescue Corps Program (in this subsection referred to as the ''HERO Child-Rescue Corps Program''), which shall be a Department-wide program, in collaboration with the Department of Defense and the National Association to Protect Children.

(B) PRIVATE-SECTOR COLLABORATION.—As part of the HERO Child-Rescue Corps Program, the National Association to Protect Children shall provide logistical support for program participants.

(2) PURPOSE.—The purpose of the HERO Child-Rescue Corps Program shall be to recruit, train, equip, and employ members of the Armed Forces on active duty and wounded, ill, and injured veterans to combat and prevent child exploitation, through serving in investigative, intelligence, analyst, inspection, and forensic positions or in any other positions determined appropriate by the employing agency.

(3) FUNCTIONS.—The HERO Child-Rescue Corps Program shall—

(A) provide, recruit, train, and equip participants of the HERO Child-Rescue Corps Program in the areas of digital forensics, investigation, analysis, intelligence, and victim identification, as determined by the Center and the needs of the Department; and

(B) ensure that during the internship period, participants in the HERO Child-Rescue Corps Program are assigned to investigate and analyze——

(i) child exploitation;

(ii) child pornography;

(iii) unidentified child victims;

(iv) human trafficking;

(v) traveling child sex offenders; and

(vi) forced child labor, including the sexual exploitation of minors.

(f) PAID INTERNSHIP AND HIRING PROGRAM.—

(1) IN GENERAL.—The Secretary shall establish a paid internship and hiring program for the purpose of placing participants of the HERO Child-Rescue Corps Program (in this subsection referred to as ''participants'') into paid internship positions, for the subsequent appointment of the participants to permanent positions, as described in the guidelines promulgated under paragraph (3).

(2) INTERNSHIP POSITIONS.—Under the paid internship and hiring program required to be established under paragraph (1), the Secretary shall assign or detail participants to positions in United States Immigration and Customs Enforcement or any other Federal agency in accordance with the guidelines promulgated under paragraph (3).

(3) PLACEMENT.—

(A) IN GENERAL.—The Secretary shall promulgate guidelines for assigning or detailing participants to positions in United States Immigration and Customs Enforcement and other Federal agencies, which shall include requirements for internship duties

and agreements regarding the subsequent appointment of the participants to permanent positions.

(B) PREFERENCE.—The Secretary shall give a preference to Homeland Security Investigations in assignments or details under the guidelines promulgated under subparagraph (A).

(4) TERM OF INTERNSHIP.—An appointment to an internship position under this subsection shall be for a term not to exceed 12 months.

(5) RATE AND TERM OF PAY.—After completion of initial group training and on beginning work at an assigned office, a participant appointed to an internship position under this subsection who is not receiving monthly basic pay as a member of the Armed Forces on active duty shall receive compensation at a rate that is—

(A) not less than the minimum rate of basic pay payable for a position at level GS–5 of the General Schedule; and

(B) not more than the maximum rate of basic pay payable for a position at level GS–7 of the General Schedule.

(6) ELIGIBILITY.—In establishing the paid internship and hiring program required under paragraph (1), the Secretary shall ensure that the eligibility requirements for participation in the internship program are the same as the eligibility requirements for participation in the HERO Child-Rescue Corps Program.

(7) HERO CHILD-RESCUE CORPS HIRING.—The Secretary shall establish in Homeland Security Investigations positions, which shall be in addition to positions in existence on December 21, 2018, for the hiring and permanent employment of graduates of the paid internship program required to be established under paragraph (1).

(g) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There are authorized to be appropriated to the Secretary such sums as are necessary to carry out this section.

(2) ALLOCATION.—Of the amounts made available pursuant to paragraph (1) in each of fiscal years 2023 through 2027, not more than $10,000,000 shall be used to carry out subsection (e) and not less than $2,000,000 shall be used to carry out subsection (f).

§ 11217. Human trafficking

(a) CENTER FOR COUNTERING HUMAN TRAFFICKING.—

(1) IN GENERAL.—

(A) ESTABLISHMENT.—The Secretary shall operate, within U.S. Immigration and Customs Enforcement's Homeland Security Investigations, the Center for Countering Human Trafficking (referred to in this section as ''CCHT'').

(B) PURPOSE.—The purpose of CCHT shall be to serve at the forefront of the Department's unified global efforts to counter human trafficking through law enforcement operations and victim protection, prevention, and awareness programs.

(C) ADMINISTRATION.—Homeland Security Investigations shall—

(i) maintain a concept of operations that identifies CCHT participants, funding, core functions, and personnel; and

(ii) update the concept of operations, as needed, to accommodate its mission and the threats to the mission.

(D) PERSONNEL.—

(i) DIRECTOR.—The Secretary shall appoint a CCHT Director, who shall—

(I) be a member of the Senior Executive Service; and

(II) serve as the Department's representative on human trafficking.

(ii) MINIMUM CORE PERSONNEL REQUIREMENTS.—Subject to appropriations, the Secretary shall ensure that CCHT is staffed with at least 45 employees in order to maintain continuity of effort, subject matter expertise, and necessary support to the Department, including—

(I) employees who are responsible for the Continued Presence Program and other victim protection duties;

(II) employees who are responsible for training, including curriculum development, and public awareness and education;

(III) employees who are responsible for stakeholder engagement, Federal interagency coordination, multilateral partnerships, and policy;

(IV) employees who are responsible for public relations, human resources, evaluation, data analysis and reporting, and information technology;

(V) special agents and criminal analysts necessary to accomplish its mission of combating human trafficking and the importation of goods produced with forced labor; and

(VI) managers.

(2) OPERATIONS UNIT.—The CCHT Director shall operate, in CCHT, an Operations Unit, that shall, at a minimum—

(A) support criminal investigations of human trafficking (including sex trafficking and forced labor)—

(i) by developing, tracking, and coordinating leads; and

(ii) by providing subject matter expertise;

(B) augment the enforcement of the prohibition on the importation of goods produced with forced labor through civil and criminal authorities;

(C) coordinate a Department-wide effort to conduct procurement audits and enforcement actions, including suspension and debarment, to mitigate the risk of human trafficking throughout Department acquisitions and contracts; and

(D) support all CCHT enforcement efforts with intelligence by conducting lead development, lead validation, case support, strategic analysis, and data analytics.

(3) PROTECTION AND AWARENESS PROGRAMS UNIT.—The CCHT Director shall operate, in CCHT, an Operations Unit, that shall—

(A) incorporate a victim-centered approach throughout Department policies, training, and practices;

(B) operate a comprehensive Continued Presence program;

(C) conduct, review, and assist with Department human trafficking training, screening, and identification tools and efforts;

(D) operate the Blue Campaign's nationwide public awareness effort and any other awareness efforts needed to encourage victim identification and reporting to law enforcement and to prevent human trafficking; and

(E) coordinate external engagement, including training and events, regarding human trafficking with critical partners, including survivors, nongovernmental organizations, corporations, multilateral entities, law enforcement agencies, and other interested parties.

(4) Investigation of labor trafficking.—

(A) IN GENERAL.—Not later than January 5, 2025, the Secretary shall establish a team of not fewer than 10 agents in CCHT to be assigned to exclusively investigate labor trafficking.

(B) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out subparagraph (A) $2,000,000 for each of fiscal years 2023 through 2027, to remain available until expended.

(b) BLUE CAMPAIGN.—

(1) DEFINITION OF HUMAN TRAFFICKING.—In this subsection, the term ''human trafficking'' means an act or practice described in paragraph (11) or (12) of section 103 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7102(11), (12)).

(2) ESTABLISHMENT.—There is in CCHT a program that shall be known as the ''Blue Campaign''. The Blue Campaign shall be headed by a Director, who shall be appointed by the Secretary.

(3) PURPOSE.—The purpose of the Blue Campaign shall be to unify and coordinate Department efforts to address human trafficking.

(4) RESPONSIBILITIES.—The Secretary, working through the Director, shall, in accordance with paragraph (5)—

(A) issue Department-wide guidance to appropriate Department personnel;

(B) develop training programs for the personnel;

(C) coordinate departmental efforts, including training for the personnel; and

(D) provide guidance and training on trauma-informed practices to ensure that human trafficking victims are afforded prompt access to victim support service providers, in addition to the assistance required under section 107 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7105), to address their immediate and long-term needs.

(5) GUIDANCE AND TRAINING.—The Blue Campaign shall provide guidance and training to Department personnel and other Federal, State, tribal, and law enforcement personnel, as appropriate, regarding—

(A) programs to help identify instances of human trafficking;

(B) the types of information that should be collected and recorded in information technology systems utilized by the Department to help identify individuals suspected or convicted of human trafficking;

(C) systematic and routine information sharing in the Department and among Federal, State, tribal, and local law enforcement agencies regarding—

(i) individuals suspected or convicted of human trafficking; and

(ii) patterns and practices of human trafficking;

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

(E) methods to be used by the Transportation Security Administration and personnel from other appropriate agencies to train employees of the Transportation Security Administration to—

(i) identify suspected victims of trafficking; and

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

(F) the development and utilization, in consultation with the Blue Campaign Advisory Board established pursuant to paragraph (7), of resources, such as indicator cards, fact sheets, pamphlets, posters, brochures, and radio and television campaigns to—

(i) educate partners and stakeholders; and

(ii) increase public awareness of human trafficking;

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

(H) any other activities the Secretary determines necessary to carry out the Blue Campaign.

(6) WEB-BASED TRAINING PROGRAMS.—To enhance training opportunities, the Director of the Blue Campaign shall develop web-based interactive training videos that utilize a learning management system to provide online training opportunities. During the 10-year period beginning on the date that is 90 days after December 27, 2021, the training opportunities shall be made available to the following individuals:

(A) Federal, State, local, Tribal, and territorial law enforcement officers.

(B) Non-Federal correction system personnel.

(C) Such other individuals as the Director determines appropriate.

(7) BLUE CAMPAIGN ADVISORY BOARD.—

(A) IN GENERAL.—There is in the Department a Blue Campaign Advisory Board, which shall be comprised of representatives assigned by the Secretary from—

(i) the Office for Civil Rights and Civil Liberties of the Department;

(ii) the Privacy Office of the Department; and

(iii) not fewer than 4 other separate components or offices of the Department.

(B) CHARTER.—The Secretary may issue a charter for the Blue Campaign Advisory Board. The charter shall specify the following:

(i) The Board's mission and goals and the scope of its activities.

(ii) The duties of the Board's representatives.

(iii) The frequency of the Board's meetings.

(C) CONSULTATION.—The Director shall consult the Blue Campaign Advisory Board and, as appropriate, experts from other components and offices of the CCHT regarding the following:

(i) Recruitment tactics used by human traffickers to inform the development of training and materials by the Blue Campaign.

(ii) The development of effective awareness tools for distribution to Federal and non-Federal officials to identify and prevent instances of human trafficking.

(iii) Identification of additional persons or entities that may be uniquely positioned to recognize signs of human trafficking and the development of materials for those persons.

(8) CONSULTATION.—With regard to the development of programs under the Blue Campaign and the implementation of the programs, the Director may consult with State, local, Tribal, and territorial agencies, non-governmental organizations, private sector organizations, and experts.

(c) TRANSFER OF FUNCTIONS AND RESOURCES.—

(1) AUTHORIZATION.—Not later than 180 days after December 27, 2022, the Secretary may transfer the functions and resources of any component, directorate, or other office of the Department related to combating human trafficking to the CCHT.

(2) NOTIFICATION.—Not later than 30 days before executing any transfer authorized under paragraph (1), the Secretary shall notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of the planned transfer.

(d) INFORMATION SHARING TO FACILITATE REPORTS AND ANALYSIS.—Each subagency of the Department shall share with CCHT—

(1) any information needed by CCHT to develop the strategy and proposal required under section 4(a) of the Countering Human Trafficking Act of 2021 (Public Law 117–322 136 Stat. 4435);and

(2) any additional data analysis to help CCHT better understand the issues surrounding human trafficking.

(e) REPORTS TO CONGRESS.—

(1) IDENTIFYING NEEDED LEGISLATION.—Not later than December 27, 2023, the CCHT Director shall submit a report to Congress that identifies any legislation that is needed to facilitate the Department's mission to end human trafficking.

(2) POTENTIAL HUMAN TRAFFICKING VICTIMS.—Not later than December 27, 2023, and annually thereafter, the Secretary shall submit a report to Congress that includes—

(1) the numbers of screened and identified potential victims of trafficking (as defined insection 103 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7102) at or near the international border between the United States and Mexico, including a summary of the age ranges of the victims and their countries of origin; and

(2) an update on the Department's efforts to establish protocols and methods for personnel to report human trafficking, pursuant to the Department of Homeland Security Strategy to Combat Human Trafficking, the Importation of Goods Produced with Forced Labor, and Child Sexual Exploitation, published in January 2020.

Chapter 113—National Emergency Management

Subchapter I—General

Subchapter II—Fire Prevention and Control

Subchapter I—General

§ 11301. Definitions

In this subchapter:

(1) ADMINISTRATOR.—the term ''Administrator'' means the Administrator of the Agency.

(2) AGENCY.—The term ''Agency'' means the Federal Emergency Management Agency.

(3) CATASTROPHIC INCIDENT.—The term ''catastrophic incident'' means a natural disaster, act of terrorism, or other man-made disaster that results in extraordinary levels of casualties or damage or disruption severely affecting the population (including mass evacuations), infrastructure, environment, economy, national morale, or government functions in an area.

(4) CREDENTIALED; CREDENTIALING.—The terms ''credentialed'' and ''credentialing'' mean having provided, or providing, respectively, documentation that identifies personnel and authenticates and verifies the qualifications of the personnel by ensuring that the personnel pos-

sess a minimum common level of training, experience, physical and medical fitness, and capability appropriate for a particular position in accordance with standards created under section 11310 of this title.

(5) FEDERAL COORDINATING OFFICER.—The term ''Federal coordinating officer'' means a Federal coordinating officer as described in section 302 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5143).

(6) INTEROPERABLE COMMUNICATIONS.—The term ''interoperable communications'' has the meaning given that term in section 10912(a) of this title.

(7) NATIONAL INCIDENT MANAGEMENT SYSTEM.—The term ''National Incident Management System'' means a system to enable effective, efficient, and collaborative incident management.

(8) NATIONAL RESPONSE PLAN.—The term ''National Response Plan'' means the National Response Plan or a successor plan prepared under section 11303(a)(6) of this title.

(9) NUCLEAR INCIDENT RESPONSE TEAM.—The term ''Nuclear Incident Response Team'' means a resource that includes—

(A) those entities of the Department of Energy that perform nuclear or radiological emergency support functions (including accident response, search response, advisory, and technical operations functions), radiation exposure functions at the medical assistance facility known as the Radiation Emergency Assistance Center/Training Site (REAC/TS), radiological assistance functions, and related functions; and

(B) those entities of the Environmental Protection Agency that perform such support functions (including radiological emergency response functions) and related functions.

(10) REGIONAL ADMINISTRATOR.—The term ''Regional Administrator'' means a Regional Administrator appointed under section 11307 of this title.

(11) REGIONAL OFFICE.—The term ''Regional Office'' means a Regional Office established under section 11307 of this title.

(12) RESOURCES.—The term ''resources'' means personnel and major items of equipment, supplies, and facilities available or potentially available for responding to a natural disaster, act of terrorism, or other man-made disaster.

(13) SURGE CAPACITY.—The term ''surge capacity'' means the ability to rapidly and substantially increase the provision of search and rescue capabilities, food, water, medicine, shelter and housing, medical care, evacuation capacity, staffing (including disaster assistance em-

ployees), and other resources necessary to save lives and protect property during a catastrophic incident.

(14) TRIBAL GOVERNMENT.—The term ''tribal government'' means the government of an entity described in section 10101(13)(B) of this title.

(15) TYPED; TYPING.—The terms ''typed'' and ''typing'' mean having evaluated, or evaluating, respectively, a resource in accordance with standards created under section 11310 of this title.

§ 11302. Federal Emergency Management Agency

(a) MISSION.—

(1) PRIMARY MISSION.—The primary mission of the Agency is to reduce the loss of life and property and protect the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters, by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation.

(2) SPECIFIC ACTIVITIES.—In support of the primary mission of the Agency, the Administrator shall—

(A) lead the Nation's efforts to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents;

(B) partner with State, local, and tribal governments and emergency response providers, with other Federal agencies, with the private sector, and with nongovernmental organizations to build a national system of emergency management that can effectively and efficiently utilize the full measure of the Nation's resources to respond to natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents;

(C) develop a Federal response capability that, when necessary and appropriate, can act effectively and rapidly to deliver assistance essential to saving lives or protecting or preserving property or public health and safety in a natural disaster, act of terrorism, or other man-made disaster;

(D) integrate the Agency's emergency preparedness, protection, response, recovery, and mitigation responsibilities to confront effectively the challenges of a natural disaster, act of terrorism, or other man-made disaster;

(E) develop and maintain robust Regional Offices that will work with State, local, and tribal governments, emergency response pro-

viders, and other appropriate entities to identify and address regional priorities;

(F) under the leadership of the Secretary, coordinate with the Commandant of the Coast Guard, the Commissioner of U.S. Customs and Border Protection, the Director of Immigration and Customs Enforcement, the National Operations Center, and other agencies and offices in the Department to take full advantage of the substantial range of resources in the Department;

(G) provide funding, training, exercises, technical assistance, planning, and other assistance to build tribal, local, State, regional, and national capabilities (including communications capabilities) necessary to respond to a natural disaster, act of terrorism, or other man-made disaster; and

(H) develop and coordinate the implementation of a risk-based, all-hazards strategy for preparedness that builds those common capabilities necessary to respond to natural disasters, acts of terrorism, and other man-made disasters while also building the unique capabilities necessary to respond to specific types of incidents that pose the greatest risk to our Nation.

(I) identify, integrate, and implement the needs of children, including children within under-served communities, into activities to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other disasters, including catastrophic incidents, including by appointing a technical expert, who may consult with relevant outside organizations and experts, as necessary, to coordinate the integration, as necessary.

(b) ADMINISTRATOR.—

(1) REPORTING.—The Administrator shall report to the Secretary, without being required to report through another official of the Department.

(2) PRINCIPAL ADVISOR ON EMERGENCY MANAGEMENT.—

(A) IN GENERAL.—The Administrator is the principal advisor to the President, the Homeland Security Council, and the Secretary for all matters relating to emergency management in the United States.

(B) ADVICE AND RECOMMENDATIONS.—

(i) RANGE OF OPTIONS.—In presenting advice with respect to a matter to the President, the Homeland Security Council, or the Secretary, the Administrator shall, as the Administrator considers appropriate, inform the President, the Home-

land Security Council, or the Secretary, as the case may be, of the range of emergency preparedness, protection, response, recovery, and mitigation options with respect to that matter.

(ii) ADVICE ON A PARTICULAR MATTER.—The Administrator, as the principal advisor on emergency management, shall provide advice to the President, the Homeland Security Council, or the Secretary on a particular matter when the President, the Homeland Security Council, or the Secretary requests advice.

(iii) RECOMMENDATIONS.—After informing the Secretary, the Administrator may make recommendations to Congress relating to emergency management the Administrator considers appropriate.

(3) CABINET STATUS.—

(A) IN GENERAL.—The President may designate the Administrator to serve as a member of the Cabinet in the event of natural disasters, acts of terrorism, or other man-made disasters.

(B) RETENTION OF AUTHORITY.—Nothing in this paragraph shall be construed as affecting the authority of the Secretary under this subtitle.

§ 11303. Authority and responsibilities

(a) IN GENERAL.—The Administrator shall provide Federal leadership necessary to prepare for, protect against, respond to, recover from, or mitigate against a natural disaster, act of terrorism, or other man-made disaster, including—

(1) helping to ensure the effectiveness of emergency response providers to terrorist attacks, major disasters, and other emergencies;

(2) with respect to the Nuclear Incident Response Team (regardless of whether it is operating as an organizational unit of the Department pursuant to this subchapter)—

(A) establishing standards and certifying when those standards have been met;

(B) conducting joint and other exercises, and training and evaluating performance; and

(C) providing funds to the Department of Energy and the Environmental Protection Agency, as appropriate, for homeland security planning, exercises and training, and equipment;

(3) providing the Federal Government's response to terrorist attacks and major disasters, including—

(A) managing the response;

(B) directing the Domestic Emergency Support Team and (when operating as an organizational unit of the Department pursuant to this subchapter) the Nuclear Incident Response Team;

(C) overseeing the Metropolitan Medical Response System; and

(D) coordinating other Federal response resources, including requiring deployment of the Strategic National Stockpile, in the event of a terrorist attack or major disaster;

(4) aiding the recovery from terrorist attacks and major disasters;

(5) building a comprehensive national incident management system with Federal, State, and local government personnel, agencies, and authorities, to respond to attacks and disasters;

(6) consolidating existing Federal Government emergency response plans into a single, coordinated national response plan;

(7) helping ensure the acquisition of operable and interoperable communications capabilities by Federal, State, local, and tribal governments and emergency response providers;

(8) assisting the President in carrying out the functions under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) and carrying out all functions and authorities given to the Administrator under that Act;

(9) carrying out the mission of the Agency to reduce the loss of life and property and protect the Nation from all hazards by leading and supporting the Nation in a risk-based, comprehensive emergency management system of—

(A) mitigation, by taking sustained actions to reduce or eliminate long-term risks to people and property from hazards and their effects;

(B) preparedness, by planning, training, and building the emergency management profession to prepare effectively for, mitigate against, respond to, and recover from a hazard;

(C) response, by conducting emergency operations to save lives and property through positioning emergency equipment, personnel, and supplies, through evacuating potential victims, through providing food, water, shelter, and medical care to those in need, and through restoring critical public services; and

(D) recovery, by rebuilding communities so individuals, businesses, and governments can function on their own, return to normal life, and protect against future hazards;

(10) increasing efficiencies, by coordinating efforts relating to preparedness, protection, response, recovery, and mitigation;

(11) helping to ensure the effectiveness of emergency response providers in responding to a natural disaster, act of terrorism, or other man-made disaster;

(12) supervising grant programs administered by the Agency;

(13) administering and ensuring the implementation of the National Response Plan, including coordinating and ensuring the readiness of each emergency support function under the National Response Plan;

(14) coordinating with the National Advisory Council established under section 11308 of this title;

(15) preparing and implementing the plans and programs of the Federal Government for—

(A) continuity of operations;

(B) continuity of government; and

(C) continuity of plans;

(16) minimizing, to the extent practicable, overlapping planning and reporting requirements applicable to State, local, and tribal governments and the private sector;

(17) maintaining and operating within the Agency the National Response Coordination Center or its successor;

(18) developing a national emergency management system that is capable of preparing for, protecting against, responding to, recovering from, and mitigating against catastrophic incidents;

(19) assisting the President in carrying out the functions under the national preparedness goal and the national preparedness system and carrying out all functions and authorities of the Administrator under the national preparedness system;

(20) carrying out all authorities of the Federal Emergency Management Agency and the Directorate of Preparedness of the Department as transferred under section 11305 of this title; and

(21) otherwise carrying out the mission of the Agency as described in section 11302(a) of this title.

(b) ALL-HAZARDS APPROACH.—In carrying out the responsibilities under this section, the Administrator shall coordinate the implementation of a risk-based, all-hazards strategy that builds those common capabilities necessary to prepare for, protect against, respond to, recover from, or mitigate against natural disasters, acts of terrorism, and other man-made disasters, while also building the unique capabilities necessary to prepare for, protect against, respond to, recover from, or mitigate against the risks of specific types of incidents that pose the greatest risk to the Nation.

§ 11304. Preparedness programs

The Administrator is responsible for the radiological emergency preparedness program and the chemical stockpile emergency preparedness program.

§ 11305. Functions transferred

(a) IN GENERAL.—Except as provided in subsection (b), there are transferred to the Agency the following:

(1) All functions of the Agency, including existing responsibilities for emergency alert systems and continuity of operations and continuity of government plans and programs as constituted on June 1, 2006, including all of its personnel, assets, components, authorities, grant programs, and liabilities, and including the functions of the former Under Secretary for Federal Emergency Management relating to the Agency.

(2) The former Directorate of Preparedness, as constituted on June 1, 2006, including all of its functions, personnel, assets, components, authorities, grant programs, and liabilities, and including the functions of the Under Secretary for Preparedness relating to the Directorate.

(b) EXCEPTIONS.—The following in the former Directorate of Preparedness shall not be transferred:

(1) The Office of Infrastructure Protection.

(2) The National Communications System.

(3) The National Cybersecurity Division.

(4) The functions, personnel, assets, components, authorities, and liabilities of each component described under paragraphs (1) through (3).

§ 11306. Preserving the Federal Emergency Management Agency

(a) REORGANIZATION.—Section 10341(b) of this title shall not apply to the Agency, including any function or organizational unit of the Agency.

(b) PROHIBITION ON CHANGES TO MISSIONS.—

(1) IN GENERAL.—The Secretary may not substantially or significantly reduce, including through a Joint Task Force established under section 11708 of this title, the authorities, responsibilities, or functions of the Agency or the capability of the Agency to perform those authorities, responsibilities, or functions, except as otherwise specifically provided in an Act enacted after October 4, 2006.

(2) CERTAIN TRANSFERS PROHIBITED.—No asset, function, or mission of the Agency may be diverted to the principal and continuing use of another organization, unit, or entity of the Department, including a Joint Task Force established under section 11708 of this title, except for details or assignments that do not reduce the capability of the Agency to perform its missions.

(c) REPROGRAMMING AND TRANSFER OF FUNDS.—In reprogramming or transferring funds, the Secretary shall comply with applicable provisions of any Act making appropriations for the Department for any fiscal year relating to the reprogramming or transfer of funds.

§ 11307. Regional Offices

(a) IN GENERAL.—There are in the Agency 10 regional offices, as identified by the Administrator.

(b) MANAGEMENT OF REGIONAL OFFICES.—

(1) REGIONAL ADMINISTRATOR.—Each Regional Office shall be headed by a Regional Administrator, who shall be appointed by the Administrator, after consulting with State, local, and tribal government officials in the region. Each Regional Administrator shall report directly to the Administrator and be in the Senior Executive Service.

(2) QUALIFICATIONS.—

(A) IN GENERAL.—Each Regional Administrator shall be appointed from among individuals who have a demonstrated ability in and knowledge of emergency management and homeland security.

(B) CONSIDERATIONS.—In selecting a Regional Administrator for a Regional Office, the Administrator shall consider the familiarity of an individual with the geographical area and demographic characteristics of the population served by the Regional Office.

(c) RESPONSIBILITIES.—

(1) IN GENERAL.—The Regional Administrator shall work in partnership with State, local, and tribal governments, emergency managers, emergency response providers, medical providers, the private sector, nongovernmental organizations, multijurisdictional councils of governments, and regional planning commissions and organizations in the geographical area served by the Regional Office to carry out the responsibilities of a Regional Administrator under this section.

(2) SPECIFIC RESPONSIBILITIES.—The responsibilities of a Regional Administrator include—

(A) ensuring effective, coordinated, and integrated regional preparedness, protection, response, recovery, and mitigation activities and programs for natural disasters, acts of terrorism, and other man-made disasters (including planning, training, exercises, and professional development);

(B) assisting in the development of regional capabilities needed for a national catastrophic response system;

(C) coordinating the establishment of effective regional operable and interoperable emergency communications capabilities;

(D) staffing and overseeing one or more strike teams within the region under subsection (f), to serve as the focal point of the Federal Government's initial response efforts for natural disasters, acts of terrorism, and other man-made disasters within that region, and otherwise building Federal response capabilities to respond to natural disasters, acts of terrorism, and other man-made disasters within that region;

(E) designating an individual responsible for the development of strategic and operational regional plans in support of the National Response Plan;

(F) fostering the development of mutual aid and other cooperative agreements;

(G) identifying critical gaps in regional capabilities to respond to populations with special needs;

(H) maintaining and operating a Regional Response Coordination Center or its successor;

(I) coordinating with the private sector to help ensure private-sector preparedness for natural disasters, acts of terrorism, and other man-made disasters;

(J) assisting State, local, and tribal governments, where appropriate, to pre-identify and evaluate suitable sites where a multi-jurisdictional incident command system may quickly be established and operated from, if the need for a system arises; and

(K) performing any other duties relating to these responsibilities that the Administrator may require.

(3) TRAINING AND EXERCISE REQUIREMENTS.—

(A) TRAINING.—The Administrator shall require each Regional Administrator to undergo specific training periodically to complement the qualifications of the Regional Administrator. The training, as appropriate, shall include training with respect to the National Incident Management System, the National Response Plan, and other subjects determined by the Administrator.

(B) EXERCISES.—The Administrator shall require each Regional Administrator to participate as appropriate in regional and national exercises.

(d) AREA OFFICES.—

(1) IN GENERAL.—There is an Area Office for the Pacific and an Area Office for the Caribbean, as components in the appropriate Regional Offices.

(2) ALASKA.—The Administrator shall establish an Area Office in Alaska, as a component in the appropriate Regional Office.

(e) REGIONAL ADVISORY COUNCIL.—

(1) ESTABLISHMENT.—Each Regional Administrator shall establish a Regional Advisory Council.

(2) NOMINATIONS.—A State, local, or tribal government located in the geographic area served by the Regional Office may nominate officials, including Adjutants General and emergency managers, to serve as members of the Regional Advisory Council for that region.

(3) RESPONSIBILITIES.—Each Regional Advisory Council shall—

(A) advise the Regional Administrator on emergency management issues specific to that region;

(B) identify geographic, demographic, or other characteristics peculiar to a State, local, or tribal government within the region that might make preparedness, protection, response, recovery, or mitigation more complicated or difficult; and

(C) advise the Regional Administrator of weaknesses or deficiencies in preparedness, protection, response, recovery, and mitigation for a State, local, and tribal government within the region of which the Regional Advisory Council is aware.

(f) REGIONAL OFFICE STRIKE TEAMS.—

(1) IN GENERAL.—In coordination with other relevant Federal agencies, each Regional Administrator shall oversee multi-agency strike teams authorized under section 303 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5144) that shall consist of—

(A) a designated Federal coordinating officer;

(B) personnel trained in incident management;

(C) public affairs, response and recovery, and communications support personnel;

(D) a defense coordinating officer;

(E) liaisons to other Federal agencies;

(F) other personnel the Administrator or Regional Administrator determines appropriate; and

(G) individuals from the agencies with primary responsibility for each of the emergency support functions in the National Response Plan.

(2) OTHER DUTIES TO BE CONSISTENT.—The duties of an individual assigned to a Regional Office strike team from another relevant agency when the individual is not functioning as a member of the strike team shall be consistent with the emergency preparedness activities of the agency that employs the individual.

(3) LOCATION OF MEMBERS.—The members of each Regional Office strike team, including representatives from agencies other than the Department, shall be based primarily within the region that corresponds to that strike team.

(4) COORDINATION.—Each Regional Office strike team shall coordinate the training and exercises of that strike team with the State, local, and tribal governments and private-sector and nongovernmental entities that the strike team shall support when a natural disaster, act of terrorism, or other man-made disaster occurs.

(5) PREPAREDNESS.—Each Regional Office strike team shall be trained as a unit on a regular basis and equipped and staffed to be well prepared to respond to natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents.

(6) AUTHORITIES.—If the Administrator determines that statutory authority is inadequate for the preparedness and deployment of individuals in strike teams under this subsection, the Administrator shall report to Congress regarding the additional statutory authorities that the Administrator determines are necessary.

§ 11308. National Advisory Council

(a) ESTABLISHMENT.—There is in the Department the National Advisory Council, established as an advisory body under section 10391(a) of this title to ensure effective and ongoing coordination of Federal preparedness, protection, response, recovery, and mitigation for natural disasters, acts of terrorism, and other man-made disasters.

(b) RESPONSIBILITIES.—

(1) IN GENERAL.—The National Advisory Council shall advise the Administrator on all aspects of emergency management. The National Advisory Council shall incorporate State, local, and tribal government and private-sector input in the development and revision of the national preparedness goal, the national preparedness system, the National Incident Management System, the National Response Plan, and other related plans and strategies.

(2) CONSULTATION ON GRANTS.—To ensure input from and coordination with State, local, and tribal governments and emergency response providers, the Administrator shall regularly consult and work with the National Advisory Council on the administration and assessment of grant programs administered by the Department, including with respect to the development of program guidance and the development and evaluation of risk-assessment methodologies, as appropriate.

(c) MEMBERSHIP.—

(1) IN GENERAL.—The members of the National Advisory Council shall be appointed by the Administrator, and shall, to the extent practicable, represent a geographic (including urban and rural) and substantive cross section of officials, emergency managers, and emergency response providers from State, local, and tribal governments, the private sector, and nongovernmental organizations, including as appropriate—

(A) members selected from the emergency management field and emergency response providers, including fire service, law enforcement, hazardous materials response, emergency medical services, and emergency management personnel, or organizations representing these individuals;

(B) health scientists, emergency and inpatient medical providers, and public health professionals;

(C) experts from Federal, State, local, and tribal governments, and the private sector, representing standards-setting and accrediting organizations, including representatives from the voluntary consensus codes and standards development community, particularly those with expertise in the emergency preparedness and response field;

(D) State, local, and tribal government officials with expertise in preparedness, protection, response, recovery, and mitigation, including Adjutants General;

(E) elected State, local, and tribal government executives;

(F) experts in public- and private-sector infrastructure protection, cybersecurity, and communications;

(G) representatives of individuals with disabilities and other populations with special needs; and

(H) other individuals the Administrator determines to be appropriate.

(2) COORDINATION WITH DEPARTMENTS OF HEALTH AND HUMAN SERVICES AND TRANSPORTATION.—In the selection of members of the National Advisory Council who are health or emergency medical services professionals, the Administrator shall work with the Secretary of Health and Human Services and the Secretary of Transportation.

(3) EX OFFICIO MEMBERS.—The Administrator shall designate one or more officers of the Federal Government to serve as ex officio members of the National Advisory Council.

(4) TERM OF OFFICE.—The term of office of each member of the National Advisory Council shall be 3 years.

(d) RESPONSE SUBCOMMITTEE.—

(1) ESTABLISHMENT.—The Administrator shall establish the Railroad Emergency Services Preparedness, Operational Needs, and Safety Evaluation Subcommittee (in this subsection referred to as the ''RESPONSE Subcommittee'').

(2) MEMBERSHIP.—Notwithstanding subsection (c), the RESPONSE Subcommittee is composed of the following:

(A) the Deputy Administrator, Protection and National Preparedness of the Federal Emergency Management Agency, or designee.

(B) The Chief Safety Officer of the Pipeline and Hazardous Materials Safety Administration, or designee.

(C) The Associate Administrator for Hazardous Materials Safety of the Pipeline and Hazardous Materials Safety Administration, or designee.

(D) The Assistant Director for Emergency Communications, or designee.

(E) The Director of the Office of Railroad, Pipeline and Hazardous Materials Investigations of the National Transportation Safety Board, or designee.

(F) The Chief Safety Officer and Associate Administrator for Railroad Safety of the Federal Railroad Administration, or designee.

(G) The Assistant Administrator for Security Policy and Industry Engagement of the Transportation Security Administration, or designee.

(H) The Assistant Commandant for Response Policy of the Coast Guard, or designee.

(I) The Assistant Administrator for the Office of Solid Waste and Emergency Response of the Environmental Protection Agency, or designee.

(J) Such other qualified individuals as the co-chairpersons shall jointly appoint as soon as practicable from among the following:

(i) Members of the National Advisory Council who have the requisite technical knowledge and expertise to address rail emergency response issues, including members for the following disciplines:

(I) Emergency management and emergency response providers, including fire service, law enforcement, hazardous materials response, and emergency medical services.

(II) State, local, and tribal government officials.

(ii) Individuals who have the requisite technical knowledge and expertise to serve on the RESPONSE Subcommittee, including at least 1 representative from each of the following:

(I) The rail industry.

(II) Rail labor.

(III) Persons that offer oil for transportation by rail.

(IV) The communications industry.

(V) Emergency response providers, including individuals nominated by national organizations representing State and local governments and emergency responders.

(VI) Emergency response training providers.

(VII) Representatives from tribal organizations.

(VIII) Technical experts.

(IX) Vendors, developers, and manufacturers of systems, facilities, equipment, and capabilities for emergency responder services.

(iii) Representatives of such other stakeholders and interested and affected parties as the co-chairpersons consider appropriate.

(3) CO-CHAIRPERSONS.—The members described in subparagraphs (A) and (B) of paragraph (2) shall serve as the co-chairpersons of the RESPONSE Subcommittee.

(4) CONSULTATION WITH NONMEMBERS.—The RESPONSE Subcommittee and the program offices for emergency responder training and resources shall consult with other relevant agencies and groups, including entities engaged in federally funded research and academic institutions engaged in relevant work and research, that are not represented on the RESPONSE Subcommittee to consider new and developing technologies and methods that may be beneficial to preparedness and response to rail hazardous materials incidents.

(5) RECOMMENDATIONS.—The RESPONSE Subcommittee shall develop recommendations, as appropriate, for improving emergency responder training and resource allocation for hazardous materials incidents involving railroads after evaluating the following topics:

(A) The quality and application of training for State and local emergency responders relating to rail hazardous materials incidents, including training for emergency responders serving small communities near railroads, including the following:

(i) Ease of access to relevant training for State and local emergency responders, including an analysis of—

(I) the number of individual being trained;

(II) the number of individuals who are applying;

(III) whether current demand is being met;

(IV) current challenges; and

(V) projected needs.

(ii) Modernization of training course content relating to rail hazardous materials incidents, with a particular focus on fluctuations in oil shipments by rail, including regular and ongoing evaluation of course opportunities, adaptation to emerging trends, agency and private-sector outreach, effectiveness, and ease of access for State and local emergency responders.

(iii) Identification of overlap in training content and identification of opportunities to develop complementary courses and materials among governmental and nongovernmental entities.

(iv) Online training platforms, train-the-trainer, and mobile training options.

(B) The availability and effectiveness of Federal, State, local, and nongovernmental funding levels related to training emergency responders for rail hazardous materials incidents, including emergency responders serving small communities near railroads, including—

(i) identifying overlap in resource allocation;

(ii) identifying cost-saving measures that can be implemented to increase training opportunities;

(iii) leveraging government funding with nongovernmental funding to enhance training opportunities and fill existing training gaps;

(iv) adapting priority settings for agency funding allocations in response to emerging trends;

(v) identifying historic levels of funding across Federal agencies for rail hazardous materials incident response and training, including funding provided by the private sector to public entities or in conjunction with Federal programs; and

(vi) identifying current funding resources across agencies.

(C) The strategy for integrating commodity flow studies, mapping, and rail and hazardous materials databases for State and local emergency responders and for increasing the rate of access to the individual responder in existing or emerging communications technology.

(6) REPORT.—

(A) IN GENERAL.—Not later than December 16, 2017, the RESPONSE Subcommittee shall submit a report to the National Advisory Council that—

(i) includes the recommendations developed under paragraph (5);

(ii) specifies the time frames for implementing the recommendations that do not require congressional action; and

(iii) identifies the recommendations that do require congressional action.

(B) REVIEW.—Not later than 30 days after receiving the report under subparagraph (A), the National Advisory Council shall begin a review of the report. The National Advisory Council may ask for additional clarification, changes, or other information from the RESPONSE Subcommittee to assist in the approval of the recommendations.

(C) RECOMMENDATIONS.—Once the National Advisory Council approves the recommendations of the RESPONSE Subcommittee, the National Advisory Council shall submit the report to—

(i) the co-chairpersons of the RESPONSE Subcommittee;

(ii) the head of each other agency represented on the RESPONSE Subcommittee;

(iii) the Committee on Homeland Security and Governmental Affairs of the Senate;

(iv) the Committee on Commerce, Science, and Transportation of the Senate;

(v) the Committee on Homeland Security of the House of Representatives; and

(vi) the Committee on Transportation and Infrastructure of the House of Representatives.

(7) INTERIM ACTIVITY.—

(A) UPDATES AND OVERSIGHT.—After the submission of the report by the National Advisory Council under paragraph (6), the Administrator shall—

(i) provide annual updates to the congressional committees referred to in paragraph (6)(C) regarding the status of the implementation of the recommendations developed under paragraph (5); and

(ii) coordinate the implementation of the recommendations described in paragraph (5)(A)(i), as appropriate.

(B) SUNSET.—The requirements of subparagraph (A) shall terminate on the date that is 2 years after the date of the submission of the report required under paragraph (6)(A).

(8) TERMINATION.—The RESPONSE Subcommittee shall terminate not later than 90 days after the submission of the report required under paragraph (6))(C).

(e) APPLICABILITY OF CHAPTER 10 OF TITLE 5.—

(1) IN GENERAL.—Notwithstanding section 10391(a) of this title and subject to paragraph (2), chapter 10 of title 5, including subsections (a), (b), and (d) of section 1009 of title 5, and section 552b(c) of title 5, apply to the National Advisory Council.

(2) TERMINATION.—Section 1013(a)(2) of title 5 does not apply to the National Advisory Council.

§ 11309. National Integration Center

(a) IN GENERAL.—There is in the Agency the National Integration Center.

(b) RESPONSIBILITIES.—

(1) IN GENERAL.—The Administrator, through the National Integration Center, and in consultation with other Federal departments and agencies and the National Advisory Council, shall ensure ongoing management and maintenance of the National Incident Management System, the National Response Plan, and a successor to the system or plan.

(2) REVIEW AND REVISION OF SYSTEM AND PLAN.—The National Integration Center shall periodically review, and revise as appropriate, the National Incident Management System and the National Response Plan, including—

(A) establishing, in consultation with the Director of the Corporation for National and Community Service, a process to better use volunteers and donations;

(B) improving the use of Federal, State, local, and tribal resources and ensuring the effective use of emergency response providers at emergency scenes; and

(C) revising the Catastrophic Incident Annex, finalizing and releasing the Catastrophic Incident Supplement to the National Response Plan, and ensuring that both effectively address response requirements in the event of a catastrophic incident.

(c) INCIDENT MANAGEMENT.—

(1) IN GENERAL.—

(A) NATIONAL RESPONSE PLAN.—The Administrator shall ensure that the National Response Plan provides for a clear chain

of command to lead and coordinate the Federal response to a natural disaster, act of terrorism, or other man-made disaster.

(B) ADMINISTRATOR.—The chain of the command specified in the National Response Plan shall provide for a role for—

(i) the Administrator consistent with the role of the Administrator as the principal emergency management advisor to the President, the Homeland Security Council, and the Secretary under section 11302(b)(2) of this title and the responsibility of the Administrator under the Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109–295, 120 Stat. 1394), and the amendments made by that Act, relating to natural disasters, acts of terrorism, and other man-made disasters; and

(ii) the Federal Coordinating Officer consistent with the responsibilities under section 302(b) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5143(b)).

(2) PRINCIPAL FEDERAL OFFICIAL OR DIRECTOR OF A JOINT TASK FORCE.—The Principal Federal Official (or the successor to the Official) or a Director of a Joint Task Force established under section 11708 of this title shall not—

(A) direct or replace the incident command structure established at the incident; or

(B) have directive authority over the Senior Federal Law Enforcement Official, Federal Coordinating Officer, or other Federal and State officials.

§ 11310. Credentialing and typing

(a) IN GENERAL.—The Administrator shall enter into a memorandum of understanding with the administrators of the Emergency Management Assistance Compact, State, local, and tribal governments, and organizations that represent emergency response providers, to collaborate on developing standards for deployment capabilities, including for credentialing and typing of incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to natural disasters, acts of terrorism, and other man-made disasters.

(b) DISTRIBUTION.—

(1) IN GENERAL.—The Administrator shall provide the standards developed under subsection (a), including detailed written guidance, to—

(A) each Federal agency that has responsibilities under the National Response Plan to aid that agency with credentialing and typing incident management personnel, emergency response pro-

viders, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other man-made disaster; and

(B) State, local, and tribal governments, to aid the governments with credentialing and typing of State, local, and tribal incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other man-made disaster.

(2) ASSISTANCE.—The Administrator shall provide expertise and technical assistance to aid Federal, State, local, and tribal government agencies with credentialing and typing incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other man-made disaster.

(c) CREDENTIALING AND TYPING OF PERSONNEL.—Each Federal agency with responsibilities under the National Response Plan shall ensure that incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other manmade disaster are credentialed and typed under this section.

(d) CONSULTATION ON HEALTH CARE STANDARDS.—In developing standards for credentialing health care professionals under this section, the Administrator shall consult with the Secretary of Health and Human Services.

§ 11311. National Infrastructure Simulation and Analysis Center

(a) IN GENERAL.—There is in the Department the National Infrastructure Simulation and Analysis Center established under the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(d)), which shall serve as a source of national expertise to address critical infrastructure protection and continuity through support for activities related to—

(1) counterterrorism, threat assessment, and risk mitigation; and

(2) a natural disaster, act of terrorism, or other man-made disaster.

(b) INFRASTRUCTURE MODELING.—

(1) PARTICULAR SUPPORT.—The support provided under subsection (a) includes modeling, simulation, and analysis of the systems and assets comprising critical infrastructure, to enhance preparedness, protection, response, recovery, and mitigation activities.

(2) RELATIONSHIP WITH OTHER AGENCIES.—Each Federal agency and department with critical infrastructure responsibilities under

Homeland Security Presidential Directive–7, or a successor to the Directive, shall establish a formal relationship, including an agreement regarding information sharing, between the elements of the agency or department and the National Infrastructure Simulation and Analysis Center, through the Department.

(3) PURPOSE.—The purpose of the relationship under paragraph (2) is to permit each Federal agency and department described in paragraph (2) to take full advantage of the capabilities of the National Infrastructure Simulation and Analysis Center (particularly vulnerability and consequence analysis), consistent with its work load capacity and priorities, for real-time response to reported and projected natural disasters, acts of terrorism, and other man-made disasters.

(4) RECIPIENT OF CERTAIN SUPPORT.—Modeling, simulation, and analysis provided under this subsection shall be provided to relevant Federal agencies and departments, including Federal agencies and departments with critical infrastructure responsibilities under Homeland Security Presidential Directive–7, or a successor to the Directive.

§ 11312. Evacuation plans and exercises

(a) IN GENERAL.—Notwithstanding another law, and subject to subsection (d), grants made to States or local or tribal governments by the Department through the State Homeland Security Grant Program or the Urban Area Security Initiative may be used to—

(1) establish programs for the development and maintenance of mass evacuation plans under subsection (b) in the event of a natural disaster, act of terrorism, or other man-made disaster;

(2) prepare for the execution of the plans, including the development of evacuation routes and the purchase and stockpiling of necessary supplies and shelters; and

(3) conduct exercises of the plans.

(b) PLAN DEVELOPMENT.—In developing the mass evacuation plans authorized under subsection (a), each State, local, or tribal government shall, to the maximum extent practicable—

(1) establish incident command and decision-making processes;

(2) ensure that State, local, and tribal government plans, including evacuation routes, are coordinated and integrated;

(3) identify primary and alternative evacuation routes and methods to increase evacuation capabilities along the routes, such as conversion of two-way traffic to one-way evacuation routes;

(4) identify evacuation transportation modes and capabilities, including the use of mass and public transit capabilities, and coordinating and integrating evacuation plans for all populations including for those

individuals located in hospitals, nursing homes, and other institutional living facilities;

(5) develop procedures for informing the public of evacuation plans before and during an evacuation, including individuals—

(A) with disabilities or other special needs, including the elderly;

(B) with limited English proficiency; or

(C) who might otherwise have difficulty in obtaining information; and

(6) identify shelter locations and capabilities.

(c) ASSISTANCE.—

(1) IN GENERAL.—The Administrator may establish guidelines, standards, or requirements determined appropriate to administer this section and to ensure effective mass evacuation planning for State, local, and tribal areas.

(2) REQUESTED ASSISTANCE.—The Administrator shall make assistance available upon request of a State, local, or tribal government to assist hospitals, nursing homes, and other institutions that house individuals with special needs to establish, maintain, and exercise mass evacuation plans that are coordinated and integrated into the plans developed by that State, local, or tribal government under this section.

(d) MULTIPURPOSE FUNDS.—Nothing in this section may be construed to preclude a State, local, or tribal government from using grant funds in a manner that enhances preparedness for a natural or man-made disaster unrelated to an act of terrorism, if the use assists the government in building capabilities for terrorism preparedness.

§ 11313. Disability Coordinator

(a) IN GENERAL.—After consultation with organizations representing individuals with disabilities, the National Council on Disability, and the Interagency Coordinating Council on Emergency Preparedness and Individuals with Disabilities, established under Executive Order No. 13347 (July 22, 2004, 69 Fed. Reg. 44573), the Administrator shall appoint a Disability Coordinator. The Disability Coordinator shall report directly to the Administrator, in order to ensure that the needs of individuals with disabilities are being properly addressed in emergency preparedness and disaster relief.

(b) RESPONSIBILITIES.—The Disability Coordinator is responsible for—

(1) providing guidance and coordination on matters related to individuals with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

(2) interacting with the staff of the Agency, the National Council on Disability, the Interagency Coordinating Council on Emergency Pre-

paredness and Individuals with Disabilities established under Executive Order No. 13347 (July 22, 2004, 69 Fed. Reg. 44573), other agencies of the Federal Government, and State, local, and tribal government authorities regarding the needs of individuals with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

(3) consulting with organizations that represent the interests and rights of individuals with disabilities about the needs of individuals with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

(4) ensuring the coordination and dissemination of best practices and model evacuation plans for individuals with disabilities;

(5) ensuring the development of training materials and a curriculum for training of emergency response providers, State, local, and tribal government officials, and others on the needs of individuals with disabilities;

(6) promoting the accessibility of telephone hotlines and websites regarding emergency preparedness, evacuations, and disaster relief;

(7) working to ensure that video programming distributors, including broadcasters, cable operators, and satellite television services, make emergency information accessible to individuals with hearing and vision disabilities;

(8) ensuring the availability of accessible transportation options for individuals with disabilities in the event of an evacuation;

(9) providing guidance and implementing policies to ensure that the rights and wishes of individuals with disabilities regarding post-evacuation residency and relocation are respected;

(10) ensuring that meeting the needs of individuals with disabilities is included in the components of the national preparedness system established under section 644 of the Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109–295, 120 Stat. 1425); and

(11) carrying out other duties assigned by the Administrator.

§ 11314. National Operations Center

(a) DEFINITION OF SITUATIONAL AWARENESS.—In this section, the term ''situational awareness'' means information gathered from a variety of sources that, when communicated to emergency managers, decision makers, and other appropriate officials, can form the basis for incident management decision-making and steady-state activity.

(b) ESTABLISHMENT.—The National Operations Center is the principal operations center for the Department and shall—

(1) provide situational awareness and a common operating picture for the entire Federal Government, and for State, local, tribal, and territorial governments, the private sector, and international partners as appropriate, for events, threats, and incidents involving a natural disaster, act of terrorism, or other man-made disaster;

(2) ensure that critical terrorism and disaster-related information reaches government decision-makers; and

(3) enter into agreements with other Federal operations centers and other homeland security partners, as appropriate, to facilitate the sharing of information.

(c) STATE AND LOCAL EMERGENCY RESPONDER REPRESENTATION.—

(1) ESTABLISHMENT OF EMERGENCY RESPONDER POSITION.—The Secretary shall establish a position, on a rotating basis, for a representative of State and local emergency responders at the National Operations Center established under subsection (b) to ensure the effective sharing of information between the Federal Government and State and local emergency response services.

(2) MANAGEMENT.—The Secretary shall manage the position established under paragraph (1) in accordance with the rules, regulations, and practices that govern other similar rotating positions at the National Operations Center.

§ 11315. 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 subchapter 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 this subchapter) from exercising direction, authority, and control over them when they are not operating as a unit of the Department.

§ 11316. 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, biological, radiological, and nuclear and other emerging terrorist threats carried out by the Department of Health and Human Services (including the Public Health Service), the Secretary of Health and Human Services shall

set priorities and preparedness goals and further develop a coordinated strategy for these activities in collaboration with the Secretary.

(b) EVALUATION OF PROGRESS.—In carrying out subsection (a), the Secretary of Health and Human Services shall collaborate with the Secretary in developing specific benchmarks and outcome measurements for evaluating progress toward achieving the priorities and goals described in subsection (a).

§ 11317. Use of national private-sector networks in emergency response

To the maximum extent practicable, the Secretary shall use national private-sector networks and infrastructure for emergency response to chemical, biological, radiological, nuclear, or explosive disasters, and other major disasters.

§ 11318. Model standards and guidelines for critical infrastructure workers

(a) IN GENERAL.—In coordination with appropriate national professional organizations, Federal, State, local, and tribal government agencies, and private-sector and nongovernmental entities, the Administrator shall establish model standards and guidelines for credentialing critical infrastructure workers that may be used by a State to credential critical infrastructure workers that may respond to a natural disaster, act of terrorism, or other man-made disaster.

(b) DISTRIBUTION AND ASSISTANCE.—The Administrator shall provide the standards developed under subsection (a), including detailed written guidance, to State, local, and tribal governments, and provide expertise and technical assistance to aid the governments with credentialing critical infrastructure workers that may respond to a natural disaster, act of terrorism, or other man-made disaster.

§ 11319. Guidance and recommendations

(a) IN GENERAL.—Consistent with their responsibilities and authorities under law, as of August 2, 2007, the Administrator and the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the private sector, may develop guidance or recommendations and identify best practices to assist or foster action by the private sector in—

(1) identifying potential hazards and assessing risks and impacts;

(2) mitigating the impact of a wide variety of hazards, including weapons of mass destruction;

(3) managing necessary emergency preparedness and response resources;

(4) developing mutual aid agreements;

(5) developing and maintaining emergency preparedness and response plans, and associated operational procedures;

(6) developing and conducting training and exercises to support and evaluate emergency preparedness and response plans and operational procedures;

(7) developing and conducting training programs for security guards to implement emergency preparedness and response plans and operations procedures; and

(8) developing procedures to respond to requests for information from the media or the public.

(b) ISSUANCE AND PROMOTION.—Any guidance or recommendations developed or best practices identified under subsection (a) shall be—

(1) issued through the Administrator; and

(2) promoted by the Secretary to the private sector.

(c) SMALL BUSINESS CONCERNS.—In developing guidance or recommendations or identifying best practices under subsection (a), the Administrator and the Director of the Cybersecurity and Infrastructure Security Agency shall take into consideration small business concerns (under the meaning given that term in section 3 of the Small Business Act (15 U.S.C. 632)), including a need for separate guidance or recommendations or best practices, as necessary and appropriate.

(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed to supersede a requirement established under any other provision of law.

§ 11320. Voluntary private-sector preparedness accreditation and certification program

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Secretary, acting through the officer designated under paragraph (2), shall establish and implement the voluntary private-sector preparedness accreditation and certification program under this section.

(2) DESIGNATION OF OFFICER.—The Secretary shall designate an officer responsible for the accreditation and certification program under this section. The officer (in this section referred to as the ''designated officer'') shall be one of the following:

(A) The Administrator, based on consideration of—

(i) the expertise of the Administrator in emergency management and preparedness in the United States; and

(ii) the responsibilities of the Administrator as the principal advisor to the President for all matters relating to emergency management in the United States.

(B) The Assistant Director for Infrastructure Security, based on consideration of the expertise of the Assistant Director in, and responsibilities for—

(i) protection of critical infrastructure;

(ii) risk assessment methodologies; and

(iii) interaction with the private sector on the issues described in clauses (i) and (ii).

(C) The Under Secretary for Science and Technology, based on consideration of the expertise of the Under Secretary in, and responsibilities associated with, standards.

(3) COORDINATION.—In carrying out the accreditation and certification program under this section, the designated officer shall coordinate with—

(A) the other officers of the Department referred to in paragraph (2), using the expertise and responsibilities of the officers; and

(B) the Special Assistant to the Secretary for the private sector, based on consideration of the expertise of the Special Assistant in, and responsibilities for, interacting with the private sector.

(b) VOLUNTARY PRIVATE-SECTOR PREPAREDNESS STANDARDS; VOLUNTARY ACCREDITATION AND CERTIFICATION PROGRAM FOR THE PRIVATE SECTOR.—

(1) ACCREDITATION AND CERTIFICATION PROGRAM.—The designated officer shall—

(A) begin supporting the development and updating, as necessary, of voluntary preparedness standards through appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards and voluntary consensus standards development organizations; and

(B) in consultation with representatives of appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards, appropriate voluntary consensus standards development organizations, each private-sector advisory council created under section 10320(4) of this title, appropriate representatives of State and local governments, including emergency management officials, and appropriate private-sector advisory groups, such as sector coordinating councils and information sharing and analysis centers—

(i) develop and promote a program to certify the preparedness of private-sector entities that voluntarily choose to seek certification under the program; and

(ii) implement the program under this subsection through an entity with which the designated officer enters into an agreement under paragraph (3)(A), which shall accredit third parties to carry out the certification process under this section.

(2) PROGRAM ELEMENTS.—

(A) IN GENERAL.—

(i) The program developed and implemented under this subsection shall assess whether a private-sector entity complies with voluntary preparedness standards.

(ii) In developing the program under this subsection, the designated officer shall develop guidelines for the accreditation and certification processes established under this subsection.

(B) STANDARDS.—The designated officer, in consultation with representatives of appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards, representatives of appropriate voluntary consensus standards development organizations, each private-sector advisory council created under section 10320(4) of this title, appropriate representatives of State and local governments, including emergency management officials, and appropriate private-sector advisory groups such as sector coordinating councils and information sharing and analysis centers—

(i) shall adopt one or more appropriate voluntary preparedness standards that promote preparedness, which may be tailored to address the unique nature of various sectors in the private sector, as necessary and appropriate, that shall be used in the accreditation and certification program under this subsection; and

(ii) after the adoption of one or more standards under clause (i), may adopt additional voluntary preparedness standards or modify or discontinue the use of voluntary preparedness standards for the accreditation and certification program, as necessary and appropriate to promote preparedness.

(C) SUBMISSION OF RECOMMENDATIONS.—In adopting one or more standards under subparagraph (B), the designated officer may receive recommendations from an entity described in that subparagraph relating to appropriate voluntary preparedness

standards, including appropriate sector-specific standards, for adoption in the program.

(D) SMALL BUSINESS CONCERNS.—The designated officer and an entity with which the designated officer enters into an agreement under paragraph (3)(A) shall establish separate classifications and methods of certification for small business concerns (under the meaning given that term in section 3 of the Small Business Act (15 U.S.C. 632)) for the program under this subsection.

(E) CONSIDERATIONS.—In developing and implementing the program under this subsection, the designated officer shall—

(i) consider the unique nature of various sectors in the private sector, including preparedness standards, business continuity standards, or best practices, established—

(I) under any other provision of Federal law; or

(II) by a Sector Risk Management Agency, as defined under Homeland Security Presidential Directive–7; and

(ii) coordinate the program, as appropriate, with—

(I) other Department private-sector-related programs; and

(II) preparedness and business continuity programs in other Federal agencies.

(3) ACCREDITATION AND CERTIFICATION PROCESSES.—

(A) AGREEMENT.—

(i) The designated officer shall enter into one or more agreements with a highly qualified nongovernmental entity with experience or expertise in coordinating and facilitating the development and use of voluntary consensus standards and in managing or implementing accreditation and certification programs for voluntary consensus standards, or a similarly qualified private-sector entity, to carry out accreditations and oversee the certification process under this subsection. An entity entering into an agreement with the designated officer under this clause (in this section referred to as a ''selected entity'') shall not perform certifications under this subsection.

(ii) A selected entity shall manage the accreditation process and oversee the certification process in accordance with the program established under this subsection and accredit qualified third parties to carry out the certification program established under this subsection.

(B) PROCEDURES AND REQUIREMENTS FOR ACCREDITATION AND CERTIFICATION.—

(i) COLLABORATION.—A selected entity shall collaborate to develop procedures and requirements for the accreditation and certification processes under this subsection, in accordance with the program established under this subsection and guidelines developed under paragraph (2)(A)(ii).

(ii) REASONABLE UNIFORMITY; USE.—The procedures and requirements developed under clause (i) shall—

(I) ensure reasonable uniformity in accreditation and certification processes if there is more than one selected entity; and

(II) be used by a selected entity in conducting accreditations and overseeing the certification process under this subsection.

(iii) RESOLUTION OF DISAGREEMENT.—A disagreement among selected entities in developing procedures under clause (i) shall be resolved by the designated officer.

(C) DESIGNATION.—A selected entity may accredit a qualified third party to carry out the certification process under this subsection.

(D) DISADVANTAGED BUSINESS INVOLVEMENT.—In accrediting qualified third parties to carry out the certification process under this subsection, a selected entity shall ensure, to the extent practicable, that the third parties include qualified small, minority, women-owned, or disadvantaged business concerns when appropriate. 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 of title 13, Code of Federal Regulations.

(E) TREATMENT OF OTHER CERTIFICATIONS.—At the request of an entity seeking certification, a selected entity may consider, as appropriate, other relevant certifications acquired by the entity seeking certification. If the selected entity determines that the other certifications are sufficient to meet the certification requirement or aspects of the certification requirement under this section, the selected entity may give credit to the entity seeking certification, as appropriate, to avoid unnecessarily duplicative certification requirements.

(F) THIRD PARTIES.—To be accredited under subparagraph (C), a third party shall—

(i) demonstrate that the third party has the ability to certify private-sector entities in accordance with the procedures and requirements developed under subparagraph (B);

(ii) agree to perform certifications in accordance with the procedures and requirements;

(iii) agree not to have a beneficial interest in or direct or indirect control over—

(I) a private-sector entity for which that third party conducts a certification under this subsection; or

(II) an organization that provides preparedness consulting services to private-sector entities;

(iv) agree not to have any other conflict of interest with respect to a private-sector entity for which the third party conducts a certification under this subsection;

(v) maintain liability insurance coverage at policy limits in accordance with the requirements developed under subparagraph (B); and

(vi) enter into an agreement with the selected entity accrediting that third party to protect proprietary information of a private-sector entity obtained under this subsection.

(G) MONITORING.—

(i) ENSURE COMPLIANCE.—The designated officer and a selected entity shall regularly monitor and inspect the operations of a third party conducting certifications under this subsection to ensure that the third party is complying with the procedures and requirements established under subparagraph (B) and all other applicable requirements.

(ii) PROCEDURES OR REQUIREMENTS NOT MET.—If the designated officer or a selected entity determines that a third party is not following the procedures or meeting the requirements established under subparagraph (B), the selected entity shall—

(I) revoke the accreditation of that third party to conduct certifications under this subsection; and

(II) review the certifications conducted by that third party, as necessary and appropriate.

(4) ANNUAL REVIEW.—

(A) IN GENERAL.—The designated officer, in consultation with representatives of appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards, appropriate voluntary consensus standards development organiza-

tions, appropriate representatives of State and local governments, including emergency management officials, and each private-sector advisory council created under section 10320(4) of this title, shall annually review the voluntary accreditation and certification program established under this subsection to ensure the effectiveness of the program (including the operations and management of the program by a selected entity and the selected entity's inclusion of qualified disadvantaged business concerns under paragraph (3)(D)) and make improvements and adjustments to the program as necessary and appropriate.

(B) REVIEW OF STANDARDS.—Each review under subparagraph (A) shall include an assessment of the voluntary preparedness standard or standards used in the program under this subsection.

(5) VOLUNTARY PARTICIPATION.—Certification under this subsection shall be voluntary for a private-sector entity.

(6) PUBLIC LISTING.—The designated officer shall maintain and make public a listing of any private-sector entity certified as being in compliance with the program established under this subsection, if that private-sector entity consents to the listing.

(c) RULE OF CONSTRUCTION.—Nothing in this section may be construed as—

(1) a requirement to replace preparedness, emergency response, or business continuity standards, requirements, or best practices established—

(A) under any other provision of federal law; or

(B) by a Sector Risk Management Agency, as defined under Homeland Security Presidential Directive–7; or

(2) an exemption of a private-sector entity seeking certification or meeting certification requirements under subsection (b) from compliance with all applicable statutes, regulations, directives, policies, and industry codes of practice.

§ 11321. Acceptance of gifts

(a) AUTHORITY.—The Secretary may accept and use gifts of property, both real and personal, and may accept gifts of services, including from guest lecturers, for otherwise authorized activities of the Center for Domestic Preparedness that are related to efforts to prevent, prepare for, protect against, or respond to a natural disaster, act of terrorism, or other man-made disaster, including the use of a weapon of mass destruction.

(b) PROHIBITION.—The Secretary may not accept a gift under this section if the Secretary determines that the use of the property or services would compromise the integrity or appearance of integrity of—

(1) a program of the Department; or

(2) an individual involved in a program of the Department.

(c) REPORT.—

(1) IN GENERAL.—The Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an annual report disclosing—

(A) gifts that were accepted under this section during the year covered by the report;

(B) how the gifts contribute to the mission of the Center for Domestic Preparedness; and

(C) the amount of Federal savings that were generated from the acceptance of the gifts.

(2) PUBLICATION.—Each report required under paragraph (1) shall be made publicly available.

§ 11322. Integrated public alert and warning system modernization

(a) IN GENERAL.—To provide timely and effective warnings regarding natural disasters, acts of terrorism, and other man-made disasters or threats to public safety, the Administrator shall—

(1) modernize the integrated public alert and warning system of the United States (in this section referred to as the ''public alert and warning system'') to help ensure that under all conditions the President and, except to the extent the public alert and warning system is in use by the President, Federal agencies and State, tribal, and local governments can alert and warn the civilian population in areas endangered by natural disasters, acts of terrorism, and other man-made disasters or threats to public safety; and

(2) implement the public alert and warning system to disseminate timely and effective warnings regarding natural disasters, acts of terrorism, and other man-made disasters or threats to public safety.

(b) IMPLEMENTATION REQUIREMENTS.—In carrying out subsection (a), the Administrator shall—

(1) establish or adopt, as appropriate, common alerting and warning protocols, standards, terminology, and operating procedures for the public alert and warning system;

(2) include in the public alert and warning system the capability to adapt the distribution and content of communications on the basis of geographic location, risks, and multiple communication systems and technologies, as appropriate and to the extent technically feasible;

(3) include in the public alert and warning system the capability to alert, warn, and provide equivalent information to individuals with disabilities, individuals with access and functional needs, and individuals with limited-English proficiency, to the extent technically feasible;

(4) ensure that training, tests, and exercises are conducted for the public alert and warning system, including by—

(A) incorporating the public alert and warning system into other training and exercise programs of the Department, as appropriate;

(B) establishing and integrating into the National Incident Management System a comprehensive and periodic training program to instruct and educate Federal, State, tribal, and local government officials in the use of the Common Alerting Protocol enabled Emergency Alert System; and

(C) conducting, not less than once every 3 years, periodic nationwide tests of the public alert and warning system;

(5) to the extent practicable, ensure that the public alert and warning system is resilient and secure and can withstand acts of terrorism and other external attacks;

(6) conduct public education efforts so that State, tribal, and local governments, private entities, and the people of the United States reasonably understand the functions of the public alert and warning system and how to access, use, and respond to information from the public alert and warning system through a general market awareness campaign;

(7) consult, coordinate, and cooperate with the appropriate private-sector entities and Federal, State, tribal, and local governmental authorities, including the Regional Administrators and emergency response providers;

(8) consult and coordinate with the Federal Communications Commission, taking into account rules and regulations promulgated by the Federal Communications Commission; and

(9) coordinate with and consider the recommendations of the Integrated Public Alert and Warning System Subcommittee established under section 2(b) of the Integrated Public Alert and Warning System Modernization Act of 2015 (Public Law 114–143, 130 Stat. 329).

(c) SYSTEM REQUIREMENTS.—The public alert and warning system shall—

(1) to the extent determined appropriate by the Administrator, incorporate multiple communications technologies;

(2) be designed to adapt to, and incorporate, future technologies for communicating directly with the public;

(3) to the extent technically feasible, be designed—

(A) to provide alerts to the largest portion of the affected population feasible, including nonresident visitors and tourists, individuals with disabilities, individuals with access and functional needs, and individuals with limited-English proficiency; and

(B) to improve the ability of remote areas to receive alerts;

(4) promote local and regional public and private partnerships to enhance community preparedness and response;

(5) provide redundant alert mechanisms where practicable so as to reach the greatest number of people; and

(6) to the extent feasible, include a mechanism to ensure the protection of individual privacy.

(d) USE OF SYSTEM.—Except to the extent necessary for testing the public alert and warning system, the public alert and warning system shall not be used to transmit a message that does not relate to a natural disaster, act of terrorism, or other man-made disaster or threat to public safety.

(e) PERFORMANCE REPORTS.—

(1) IN GENERAL.—Not later than April 11, 2017, and 2018, the Administrator shall make available on the public website of the Agency a performance report, which shall—

(A) establish performance goals for the implementation of the public alert and warning system by the Agency;

(B) describe the performance of the public alert and warning system, including—

(i) the type of technology used for alerts and warnings issued under the system;

(ii) the measures taken to alert, warn, and provide equivalent information to individuals with disabilities, individuals with access and functional needs, and individuals with limited-English proficiency; and

(iii) the training, tests, and exercises performed and the outcomes obtained by the Agency;

(C) identify significant challenges to the effective operation of the public alert and warning system and any plans to address the challenges;

(D) identify other necessary improvements to the system; and

(E) provide an analysis comparing the performance of the public alert and warning system with the performance goals established under subparagraph (A).

(2) SUBMISSION TO CONGRESS.—The Administrator shall submit to the Committee on Homeland Security and Governmental Affairs and

the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives each report required under paragraph (1).

§ 11323. Integrated public alert and warning system

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term ''appropriate congressional committees'' means—

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

(B) the Committee on Transportation and Infrastructure of the House of Representatives; and

(C) the Committee on Homeland Security of the House of Representatives.

(2) PUBLIC ALERT AND WARNING SYSTEM.—The term ''public alert and warning system'' means the integrated public alert and warning system of the United States described in section 11322 of this title.

(3) STATE.—The term ''State'' means a State, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any possession of the United States.

(b) INTEGRATED PUBLIC ALERT AND WARNING SYSTEM.—

(1) MINIMUM REQUIREMENTS.—Not later than 1 year after December 20, 2019, the Administrator shall develop minimum requirements for State, Tribal, and local governments to participate in the public alert and warning system and that are necessary to maintain the integrity of the public alert and warning system, including—

(A) guidance on the categories of public emergencies and appropriate circumstances that warrant an alert and warning from State, Tribal, and local governments using the public alert and warning system;

(B) the procedures for State, Tribal, and local government officials to authenticate civil emergencies and initiate, modify, and cancel alerts transmitted through the public alert and warning system, including protocols and technology capabilities for—

(i) the initiation, or prohibition on the initiation, of alerts by a single authorized or unauthorized individual;

(ii) testing a State, Tribal, or local government incident management and warning tool without accidentally initiating an alert through the public alert and warning system; and

(iii) steps a State, Tribal, or local government official should take to mitigate the possibility of the issuance of a false alert through the public alert and warning system;

(C) the standardization, functionality, and interoperability of incident management and warning tools used by State, Tribal, and local governments to notify the public of an emergency through the public alert and warning system;

(D) the annual training and recertification of emergency management personnel on requirements for originating and transmitting an alert through the public alert and warning system;

(E) the procedures, protocols, and guidance concerning the protective action plans that State, Tribal, and local governments shall issue to the public following an alert issued under the public alert and warning system;

(F) the procedures, protocols, and guidance concerning the communications that State, Tribal, and local governments shall issue to the public following a false alert issued under the public alert and warning system;

(G) a plan by which State, Tribal, and local government officials may, during an emergency, contact each other as well as Federal officials and participants in the Emergency Alert System and the Wireless Emergency Alert System, when appropriate and necessary, by telephone, text message, or other means of communication regarding an alert that has been distributed to the public; and

(H) any other procedure the Administrator considers appropriate for maintaining the integrity of and providing for public confidence in the public alert and warning system.

(2) COORDINATION WITH NATIONAL ADVISORY COUNCIL REPORT.—The Administrator shall ensure that the minimum requirements developed under paragraph (1) do not conflict with recommendations made for improving the public alert and warning system provided in the report submitted by the National Advisory Council under section 2(b)(7)(B) of the Integrated Public Alert and Warning System Modernization Act of 2015 (Public Law 114–143, 130 Stat. 332).

(3) PUBLIC CONSULTATION.—In developing the minimum requirements under paragraph (1), the Administrator shall ensure appropriate public consultation and, to the extent practicable, coordinate the development of the requirements with stakeholders of the public alert and warning system, including—

(A) appropriate personnel from Federal agencies, including the National Institute of Standards and Technology, the Agency, and the Federal Communications Commission;

(B) representatives of State and local governments and emergency services personnel, who shall be selected from among individuals nominated by national organizations representing those governments and personnel;

(C) representatives of Federally recognized Indian tribes and national Indian organizations;

(D) communications service providers;

(E) vendors, developers, and manufacturers of systems, facilities, equipment, and capabilities for the provision of communications services;

(F) third-party service bureaus;

(G) the national organization representing the licensees and permittees of noncommercial broadcast television stations;

(H) technical experts from the broadcasting industry;

(I) educators from the Emergency Management Institute; and

(J) other individuals with technical expertise as the Administrator determines appropriate.

(4) ADVICE TO THE ADMINISTRATOR.—In accordance with the chapter 10 of title 5, the Administrator may obtain advice from an individual or non-consensus advice from each of the several members of a group without invoking that Act.

(c) INCIDENT MANAGEMENT AND WARNING TOOL VALIDATION.—

(1) ESTABLISHMENT.—The Administrator shall establish a process to ensure that an incident management and warning tool used by a State, Tribal, or local government to originate and transmit an alert through the public alert and warning system meets the requirements developed by the Administrator under subsection (b)(1).

(2) REQUIREMENTS.—The process required to be established under paragraph (1) shall include—

(A) the ability to test an incident management and warning tool in the public alert and warning system lab;

(B) the ability to certify that an incident management and warning tool complies with the applicable cyber frameworks of the Department and the National Institute of Standards and Technology;

(C) a process to certify developers of emergency management software; and

(D) requiring developers to provide the Administrator with a copy of, and rights of use for, ongoing testing of each version of incident management and warning tool software before the software is first used by a State, Tribal, or local government.

(d) REVIEW AND UPDATE OF MEMORANDA OF UNDERSTANDING.—The Administrator shall review the memoranda of understanding between the Agency and State, Tribal, and local governments with respect to the public alert and warning system to ensure that all agreements ensure compliance with the requirements developed by the Administrator under subsection (b)(1).

(e) FUTURE MEMORANDA.—On and after the date that is 60 days after the date on which the Administrator issues the requirements developed under subsection (b)(1), any new memorandum of understanding entered into between the Agency and a State, Tribal, or local government with respect to the public alert and warning system shall comply with those requirements.

(f) MISSILE ALERT AND WARNING AUTHORITIES.—

(1) IN GENERAL.—

(A) AUTHORITY.—The authority to originate an alert warning the public of a missile launch directed against a State using the public alert and warning system shall reside primarily with the Federal Government.

(B) DELEGATION OF AUTHORITY.—The Secretary may delegate the authority described in subparagraph (A) to a State, Tribal, or local entity if, not later than 180 days after December 20, 2019, the Secretary submitted a report to the appropriate congressional committees that—

(i) it is not feasible for the Federal Government to alert the public of a missile threat against a State; or

(ii) it is not in the national security interest of the United States for the Federal Government to alert the public of a missile threat against a State.

(C) ACTIVATION OF SYSTEM.—On verification of a missile threat, the President, utilizing established authorities, protocols and procedures, may activate the public alert and warning system.

(D) CONSTRUCTION.—Nothing in this paragraph shall be construed to change the command and control relationship between entities of the Federal Government with respect to the identification, dissemination, notification, or alerting of information of missile threats against the United States that was in effect on the day before December 20, 2019.

(2) NOTIFICATION PROCESS.—The Secretary, acting through the Administrator, shall establish a process to promptly notify a State warning point, and any State entities that the Administrator determines appropriate, following the issuance of an alert described in paragraph (1)(A) so the State may take appropriate action to protect the health, safety, and welfare of the residents of the State.

(3) WORK WITH GOVERNOR.—The Secretary, acting through the Administrator, shall work with the Governor of a State warning point to develop and implement appropriate protective action plans to respond to an alert described in paragraph (1)(A) for that State.

(4) STUDY AND REPORT.—Not later than 1 year after December 20, 2019, the Secretary shall—

(A) examine the feasibility of establishing an alert designation under the public alert and warning system that would be used to alert and warn the public of a missile threat while concurrently alerting a State warning point so that a State may activate related protective action plans; and

(B) submit a report of the findings under subparagraph (A), including of the costs and timeline for taking action to implement an alert designation described in subparagraph (A), to—

(i) the Subcommittee on Homeland Security of the Committee on Appropriations of the Senate;

(ii) the Committee on Homeland Security and Governmental Affairs of the Senate;

(iii) the Subcommittee on Homeland Security of the Committee on Appropriations of the House of Representatives;

(iv) the Committee on Transportation and Infrastructure of the House of Representatives; and

(v) the Committee on Homeland Security of the House of Representatives.

(g) USE OF INTEGRATED PUBLIC ALERT AND WARNING SYSTEM LAB.—Not later than 1 year after December 20, 2019, the Administrator shall—

(1) develop a program to increase the utilization of the public alert and warning system lab of the Agency by State, Tribal, and local governments to test incident management and warning tools and train emergency management professionals on alert origination protocols and procedures; and

(2) submit to the appropriate congressional committees a report describing—

(A) the impact on utilization of the public alert and warning system lab by State, Tribal, and local governments, with particular

attention given to the impact on utilization in rural areas, resulting from the program developed under paragraph (1); and

(B) any further recommendations that the Administrator would make for additional statutory or appropriations authority necessary to increase the utilization of the public alert and warning system lab by State, Tribal, and local governments.

(h) REVIEW OF AWARENESS OF ALERTS AND WARNINGS.—Not later than 1 year after December 20, 2019, the Administrator shall—

(1) conduct a review of the National Watch Center and each Regional Watch Center of the Agency; and

(2) submit to the appropriate congressional committees a report on the review conducted under paragraph (1), which shall include—

(A) an assessment of the technical capability of the National and Regional Watch Centers described in paragraph (1) to be notified of alerts and warnings issued by a State through the public alert and warning system;

(B) a determination of which State alerts and warnings the National and Regional Watch Centers described in paragraph (1) should be aware of; and

(C) recommendations for improving the ability of the National and Regional Watch Centers described in paragraph (1) to receive State alerts and warnings that the Administrator determines are appropriate.

(i) REPORTING FALSE ALERTS.—Not later than 15 days after the date on which a State, Tribal, or local government official transmits a false alert under the public alert and warning system, the Administrator shall report to the appropriate congressional committees on—

(1) the circumstances surrounding the false alert;

(2) the content, cause, and population impacted by the false alert; and

(3) any efforts to mitigate any negative impacts of the false alert.

(j) REPORTING PARTICIPATION RATES.—The Administrator shall, on an annual basis, report to the appropriate congressional committees on—

(1) participation rates in the public alert and warning system; and

(2) efforts to expand alert, warning, and interoperable communications to rural and underserved areas.

(k) TIMELINE FOR COMPLIANCE.—Each State shall be given a reasonable amount of time to comply with new rules, regulations, or requirements imposed under this section.

§ 11324. National planning and education

The Secretary shall, to the extent practicable—

(1) include in national planning frameworks the threat of an EMP or GMD event; and

(2) conduct outreach to educate owners and operators of critical infrastructure, emergency planners, and emergency response providers at all levels of government regarding threats of EMP and GMD.

§ 11325. Coordination of Department efforts related to food, agriculture, and veterinary defense against terrorism

(a) PROGRAM.—The Secretary, acting through the Assistant Secretary for the Countering Weapons of Mass Destruction Office, shall carry out a program to coordinate the Department's efforts related to defending the food, agriculture, and veterinary systems of the United States against terrorism and other high-consequence events that pose a high risk to homeland security.

(b) PROGRAM ELEMENTS.—The coordination program required by subsection (a) shall include, at a minimum, the following:

(1) Providing oversight and management of the Department's responsibilities pursuant to Homeland Security Presidential Directive–9—Defense of United States Agriculture and Food.

(2) Providing oversight and integration of the Department's activities related to veterinary public health, food defense, and agricultural security.

(3) Leading the Department's policy initiatives relating to food, animal, and agricultural incidents, and the impact of the incidents on animal and public health.

(4) Leading the Department's policy initiatives relating to overall domestic preparedness for and collective response to agricultural terrorism.

(5) Coordinating with other Department components, including U.S. Customs and Border Protection, as appropriate, on activities related to food and agriculture security and screening procedures for domestic and imported products.

(6) Coordinating with appropriate Federal departments and agencies.

(7) Engaging in other activities as determined necessary by the Secretary.

(c) AUTHORITY NOT ALTERED OR SUPERSEDED.—Nothing in this section may be construed as altering or superseding the authority of the Secretary of Agriculture or the Secretary of Health and Human Services.

§ 11326. Transfer of equipment during a public health emergency

(a) AUTHORIZATION OF TRANSFER OF EQUIPMENT.—During a public health emergency declared by the Secretary of Health and Human Services under section 319(a) of the Public Health Service Act (42 U.S.C. 247d(a)), the Secretary, at the request of the Secretary of Health and Human Services, may transfer to the Department of Health and Human Services, on a reimbursable basis, excess personal protection equipment or medically necessary equipment in the possession of the Department.

(b) DETERMINATION BY SECRETARIES.—

(1) IN GENERAL.—In carrying out this section—

(A) before requesting a transfer under subsection (a), the Secretary of Health and Human Services shall determine whether the personal protective equipment or medically necessary equipment is otherwise available; and

(B) before initiating a transfer under subsection (a), the Secretary, in consultation with the heads of each component in the Department, shall—

(i) determine whether the personal protective equipment or medically necessary equipment requested to be transferred under subsection (a) is excess equipment; and

(ii) certify that the transfer of the personal protective equipment or medically necessary equipment will not adversely impact the health or safety of officers, employees, or contractors of the Department.

(2) NOTIFICATION.—The Secretary of Health and Human Services and the Secretary shall each submit to Congress a notification explaining the determination made under subparagraphs (A) and (B), respectively, of paragraph (1).

(3) REQUIRED INVENTORY.—

(A) IN GENERAL.—The Secretary shall—

(i) acting through the Chief Medical Officer, maintain an inventory of all personal protective equipment and medically necessary equipment in the possession of the Department; and

(ii) make the inventory required under clause (i) available, on a continual basis, to—

(I) the Secretary of Health and Human Services; and

(II) the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Appropriations and

the Committee on Homeland Security of the House of Representatives.

(B) FORM.—Each inventory required to be made available under subparagraph (A) shall be submitted in unclassified form but may include a classified annex.

§ 11327. Continuity of the economy plan

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency'' has the meaning given that term in section 551 of title 5.

(2) ECONOMIC SECTOR.—The term ''economic sector'' means a sector of the economy of the United States.

(3) RELEVANT ACTOR.—The term ''relevant actor'' means—

(A) the Federal Government;

(B) a State, local, or Tribal government; or

(C) the private sector.

(4) SIGNIFICANT EVENT.—The term ''significant event'' means an event that causes sever degradation to economic activity in the United States due to—

(A) a cyber attack; or

(B) another significant event that is natural or human-caused.

(5) STATE.—The term ''State'' means a State, the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, the Northern Mariana Islands, and a possession of the United States.

(b) REQUIREMENT.—

(1) IN GENERAL.—The President shall develop and maintain a plan to maintain and restore the economy of the United States in response to a significant event.

(2) PRINCIPLES.—The plan under paragraph (1) shall—

(A) be consistent with—

(i) a free market economy; and

(ii) the rule of law; and

(B) respect private property rights.

(3) CONTENTS.—The plan required under paragraph (1) shall—

(A) examine the distribution of goods and services across the United States necessary for the reliable functioning of the United States during a significant event;

(B) identify the economic functions of relevant actors, the disruption, corruption, or dysfunction of which would have a debilitating effect in the United States on—

(i) security;

(ii) economic security;

(iii) defense readiness; or

(iv) public health or safety;

(C) identify the critical distribution mechanisms for each economic sector that should be prioritized for operation during a significant event, including—

(i) bulk power and electric transmission systems;

(ii) national and international financial systems, including wholesale payments, stocks, and currency exchanges;

(iii) national and international communications networks, data-hosting services, and cloud services;

(iv) interstate oil and natural gas pipelines; and

(v) mechanisms for the interstate and international trade and distribution of materials, food, and medical supplies, including road, rail, air, and maritime shipping;

(D) identify economic functions of relevant actors, the disruption, corruption, or dysfunction of which would cause—

(i) catastrophic economic loss;

(ii) the loss of public confidence; or

(iii) the widespread imperilment of human life;

(E) identify the economic functions of relevant actors that are so vital to the economy of the United States that the disruption, corruption, or dysfunction of those economic functions would undermine response, recovery, or mobilization efforts during a significant event;

(F) incorporate, to the greatest extent practicable, the principles and practices contained in Federal plans for the continuity of Government and continuity of operations;

(G) identify—

(i) industrial control networks for which a loss of internet connectivity, a loss of network integrity or availability, an exploitation of a system connected to the network, or another failure, disruption, corruption, or dysfunction would have a debilitating effect in the United States on—

(I) security;

(II) economic security;

(III) defense readiness; or

(IV) public health or safety; and

(ii) for each industrial control network identified under clause (i), risk mitigation measures, including—

(I) the installation of parallel services;

(II) the use of stand-alone analog services; or

(III) the significant hardening of the industrial control network against failure, disruption, corruption, or dysfunction;

(H) identify critical economic sectors for which the preservation of data in a protected, verified, and uncorrupted status would be required for the quick recovery of the economy of the United States in the face of a significant disruption following a significant event;

(I) include a list of raw materials, industrial goods, and other items, the absence of which would significantly undermine the ability of the United States to sustain the functions described in subparagraphs (B), (D), and (E);

(J) provide an analysis of supply chain diversification for the items described in subparagraph (I) in the event of a disruption caused by a significant event;

(K) include—

(i) a recommendation as to whether the United States should maintain a strategic reserve of 1 or more of the items described in subparagraph (I); and

(ii) for each item described in subparagraph (I) for which the President recommends maintaining a strategic reserve under clause (i), an identification of mechanisms for tracking inventory and availability of the item in the strategic reserve;

(L) identify mechanisms in existence on January 1, 2021, and mechanisms that can be developed to ensure that the swift transport and delivery of the items described in subparagraph (I) are feasible in the event of a distribution network disturbance or degradation, including a distribution network disturbance or degradation caused by a significant event;

(M) include guidance for determining the prioritization for the distribution of the items described in subparagraph (I), including distribution to States and Indian Tribes;

(N) consider the advisability and feasibility of mechanisms for extending the credit of the United States or providing other financial support authorized by law to key participants in the economy of the United States if the extension or provision of other financial support—

(i) is necessary to avoid severe economic degradation; or

(ii) allows for the recovery from a significant event;

(O) include guidance for determining categories of employees that should be prioritized to continue to work to sustain the func-

tions described in subparagraphs (B), (D), and (E) in the event that there are limitations on the ability of individuals to travel to workplaces or to work remotely, including considerations for defense readiness;

(P) identify critical economic sectors necessary to provide material and operational support to the defense of the United States;

(Q) determine whether the Secretary, the National Guard, and the Secretary of Defense have adequate authority to assist the United States in a recovery from a severe economic degradation caused by a significant event;

(R) review and assess the authority and capability of heads of other agencies that the President determines necessary to assist the United States in a recovery from a severe economic degradation caused by a significant event; and

(S) consider any other matter that would aid in protecting and increasing the resilience of the economy of the United States from a significant event.

(c) COORDINATION.—In developing the plan required under subsection (b)(1), the President shall—

(1) receive advice from—

(A) the Secretary;

(B) the Secretary of Defense;

(C) the Secretary of the Treasury;

(D) the Secretary of Health and Human Services;

(E) the Secretary of Commerce;

(F) the Secretary of Transportation;

(G) the Secretary of Energy;

(H) the Administrator of the Small Business Administration; and

(I) the head of any other agency that the President determines necessary to complete the plan;

(2) consult with economic sectors relating to critical infrastructure through sector-coordinated councils, as appropriate;

(3) consult with relevant State, Tribal, and local governments and organizations that represent those governments; and

(4) consult with any other non-Federal entity that the President determines necessary to complete the plan.

(d) SUBMISSION TO CONGRESS.—

(1) IN GENERAL.—Not later than 2 years after January 1, 2021, and not less frequently than every 3 years thereafter, the President

shall submit the plan required under subsection (b)(1) and the information described in paragraph (2) to—

(A) the majority and minority leaders of the Senate;

(B) the Speaker and the minority leader of the House of Representatives;

(C) the Committee on Armed Services of the Senate;

(D) the Committee on Armed Services of the House of Representatives;

(E) the Committee on Homeland Security and Governmental Affairs of the Senate;

(F) the Committee on Homeland Security of the House of Representatives;

(G) the Committee on Health, Education, Labor, and Pensions of the Senate;

(H) the Committee on Commerce, Science, and Transportation of the Senate;

(I) the Committee on Energy and Commerce of the House of Representatives;

(J) the Committee on Banking, Housing, and Urban Affairs of the Senate;

(K) the Committee on Finance of the Senate;

(L) the Committee on Financial Services of the House of Representatives;

(M) the Committee on Small Business and Entrepreneurship of the Senate;

(N) the Committee on Small Business of the House of Representatives;

(O) the Committee on Energy and Natural Resources of the Senate;

(P) the Committee on Environment and Public Works of the Senate;

(Q) the Committee on Indian Affairs of the Senate;

(R) the Committee on Oversight and Reform of the House of Representatives;

(S) the Committee on the Budget of the House of Representatives; and

(T) any other committee of the Senate or the House of Representatives that has jurisdiction over the subject of the plan.

(2) ADDITIONAL INFORMATION.—The information described in this paragraph is—

(A) any change to Federal law that would be necessary to carry out the plan required under subsection (b)(1); and

(B) any proposed change to the funding levels provided in appropriation Acts for the most recent fiscal year that can be implemented in future appropriation Acts or additional resources necessary to—

(i) implement the plan required under subsection (b)(1); or

(ii) maintain any program offices and personnel necessary to—

(I) maintain the plan required under subsection (b)(1) and the plans described in subsection (b)(3)(F); and

(II) conduct exercises, assessments, and updates to the plans described in subclause (I) over time.

(3) INCLUSION IN BUDGET OF THE PRESIDENT.—The President may include the information described in paragraph (2)(B) in the budget the President is required to submit under section 1105(a) of title 31.

§ 11328. Guidance on how to prevent exposure to and release of PFAS

(a) IN GENERAL.—Not later than December 20, 2023, the Secretary, in consultation with the Administrator of the United States Fire Administration, the Administrator of the Environmental Protection Agency, the Director of the National Institute for Occupational Safety and Health, and the heads of any other relevant agencies, shall—

(1) develop and publish guidance for firefighters and other emergency response personnel on training, education programs, and best practices;

(2) make available a curriculum designed to—

(A) reduce and eliminate exposure to per- and polyfluoroalkyl substances (in this section referred to as ''PFAS'') from firefighting foam and personal protective equipment;

(B) prevent the release of PFAS from firefighting foam into the environment; and

(C) educate firefighters and other emergency response personnel on foams and non-foam alternatives, personal protective equipment, and other firefighting tools and equipment that do not contain PFAS; and

(3) create an online public repository, which shall be updated on a regular basis, on tools and best practices for firefighters and other emergency response personnel to reduce, limit, and prevent the release of and exposure to PFAS.

(b) CURRICULUM.—

(1) IN GENERAL.—For the purpose of developing the curriculum required under subsection (a)(2), the Administrator of the United States Fire Administration shall make recommendations to the Secretary as to the content of the curriculum.

(2) CONSULTATION.—For the purpose of making recommendations under paragraph (1), the Administrator of the United States Fire Administration shall consult with interested entities, as appropriate, including—

(A) firefighters and other emergency response personnel, including national fire service and emergency response organizations;

(B) impacted communities dealing with PFAS contamination;

(C) scientists, including public and occupational health and safety experts, who are studying PFAS and PFAS alternatives in firefighting foam;

(D) voluntary-standards organizations engaged in developing standards for firefighter and firefighting equipment;

(E) State fire training academies;

(F) State fire marshals;

(G) manufacturers of firefighting tools and equipment; and

(H) any other relevant entities, as determined by the Secretary and the Administrator of the United States Fire Administration.

(c) REVIEW.—Not later than 3 years after the date on which the guidance and curriculum required under subsection (a) is issued, and not less frequently than once every 3 years thereafter, the Secretary, in consultation with the Administrator of the United States Fire Administration, the Administrator of the Environmental Protection Agency, and the Director of the National Institute for Occupational Safety and Health, shall review the guidance and curriculum and, as appropriate, issue updates to the guidance and curriculum.

(d) INAPPLICABILITY OF CHAPTER 5 OF TITLE 10.—Chapter 5 of title 10 shall not apply to this section.

(e) RULE OF CONSTRUCTION.—Nothing in this chapter shall be construed to require the Secretary to promulgate or enforce regulations under subchapter II ofchapter 5 of title 5.

Subchapter II—Fire Prevention and Control

§ 11351. Declaration of purpose

It is declared to be the purpose of Congress in this subchapter to—

(1) reduce the Nation's losses caused by fire through better fire prevention and control;

(2) supplement existing programs of research, training, and education, and to encourage new and improved programs and activities by State and local governments;

(3) establish the United States Fire Administration and the Fire Research Center in the Federal Emergency Management Agency; and

(4) establish an intensified program of research into the treatment of burn and smoke injuries and the rehabilitation of victims of fires in the National Institutes of Health.

§ 11352. Definitions

As used in this subchapter:

(1) ACADEMY.—The term ''Academy'' means the National Academy for Fire Prevention and Control.

(2) ADMINISTRATION.—The term ''Administration'' means the United States Fire Administration established pursuant to section 11353 of this title.

(3) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Administration, in the Federal Emergency Management Agency.

(4) ADMINISTRATOR OF FEMA.—The term ''Administrator of FEMA'' means the Administrator of the Federal Emergency Management Agency;

(5) FIRE SERVICE.—

(A) IN GENERAL.—The term ''fire service'' means any organization in a State consisting of personnel, apparatus, and equipment that has as its purpose protecting property and maintaining the safety and welfare of the public from the dangers of fire, including a private firefighting brigade.

(B) PERSONNEL, LOCATION, AND RESPONSIBILITY.—The personnel of the organization may be paid employees or unpaid volunteers or any combination. The location of the organization and its responsibility for extinguishment and suppression of fires may include a Federal installation, State, city, town, borough, parish, county, Indian tribe, fire district, fire protection district, rural fire district, or other special district.

(C) FIRE PREVENTION, FIREFIGHTING, FIRE CONTROL.—The terms ''fire prevention'', ''firefighting'', and ''fire control'' relate to activities conducted by a fire service.

(6) INDIAN TRIBE.—

(A) IN GENERAL.—The term ''Indian tribe'' has the meaning given the term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304).

(B) TRIBAL.—The term ''tribal'' means of or pertaining to an Indian tribe.

(7) LOCAL.—The term ''local'' means of or pertaining to a city, town, county, special purpose district, unincorporated territory, or other political subdivision of a State.

(8) PLACE OF PUBLIC ACCOMMODATION AFFECTING COMMERCE.—The term ''place of public accommodation affecting commerce''—

(A) means an inn, hotel, or other establishment not owned by the Federal Government that provides lodging to transient guests; but

(B) does not include an establishment—

(i) treated as an apartment building for purposes of a State or local law or regulation; or

(ii) located in a building that contains not more than 5 rooms for rent or hire and that is actually occupied as a residence by the proprietor of the establishment.

(9) WILDLIFE-URBAN INTERFACE.—The term ''wildland-urban interface'' has the meaning given the term in section 101 of the Healthy Forests Restoration Act of 2003 (16 U.S.C. 6511).

§ 11353. United States Fire Administration

(a) ESTABLISHMENT.—There is in the Federal Emergency Management Agency the United States Fire Administration.

(b) ADMINISTRATOR.—There shall be at the head of the Administration the Administrator of the Administration. The Administrator shall be appointed by the President and shall be compensated at the rate provided for level IV of the Executive Schedule pay rates (5 U.S.C. 5315). The Administrator shall report and be responsible to the Administrator of FEMA.

(c) DEPUTY ADMINISTRATOR.—The Administrator may appoint a Deputy Administrator, who shall—

(1) perform such functions as the Administrator shall assign or delegate; and

(2) act as Administrator during the absence or disability of the Administrator or in the event of a vacancy in the office of Administrator.

§ 11354. Public education

The Administrator may take such steps as the Administrator considers appropriate to educate the public and overcome public indifference as to fire, fire prevention, and individual preparedness. The steps may include publications, audiovisual presentations, and demonstrations. The public education efforts shall include programs to provide specialized information for those groups of individuals who are particularly vulnerable to fire hazards, such as the young and the elderly. The Administrator shall sponsor and en-

courage research, testing, and experimentation to determine the most effective means of the public education.

§ 11355. National Academy for Fire Prevention and Control

(a) ESTABLISHMENT AND PURPOSE.—The Administrator of FEMA shall establish a National Academy for Fire Prevention and Control. The purpose of the Academy shall be to advance the professional development of fire service personnel and of other individuals engaged in fire prevention and control activities.

(b) SUPERINTENDENT.—The Academy shall be headed by a Superintendent, who shall be appointed by the Administrator of FEMA. In exercising the powers and authority contained in this section the Superintendent shall be subject to the direction of the Administrator.

(c) POWERS OF SUPERINTENDENT.—The Superintendent may—

(1) develop and revise curricula, standards for admission and performance, and criteria for the awarding of degrees and certifications;

(2) consult with other Federal, State, and local agency officials in developing curricula for classes offered by the Academy;

(3) appoint such teaching staff and other personnel as the Superintendent determines to be necessary or appropriate;

(4) conduct courses and programs of training and education, as defined in subsection (d);

(5) appoint faculty members and consultants without regard to title 5, governing appointments in the competitive service, and, with respect to temporary and intermittent services, make appointments to the same extent as is authorized by section 3109 of title 5;

(6) establish, modify, or waive fees and other charges for attendance at, and subscription to, courses and programs offered by the Academy;

(7) conduct short courses, seminars, workshops, conferences, and similar education and training activities in all parts and localities of the United States, including on-site training;

(8) enter into such contracts and take such other actions as may be necessary in carrying out the purposes of the Academy; and

(9) consult with officials of the fire services and other interested persons in the exercise of the foregoing powers.

(d) PROGRAM OF THE ACADEMY.—The Superintendent may—

(1) train fire service personnel in such skills and knowledge as may be useful to advance their ability to prevent and control fires, including—

(A) techniques of fire prevention, fire inspection, firefighting, and fire and arson investigation;

(B) tactics and command of firefighting for present and future fire chiefs and commanders;

(C) administration and management of fire services;

(D) tactical training in the specialized field of aircraft fire control and crash rescue;

(E) tactical training in the specialized field of fire control and rescue aboard waterborne vessels;

(F) strategies for building collapse rescue;

(G) the use of technology in response to fires, including terrorist incidents and other national emergencies;

(H) tactics and strategies for dealing with natural disasters, acts of terrorism, and other man-made disasters;

(I) tactics and strategies for fighting large-scale fires or multiple fires in a general area that crosses jurisdictional boundaries;

(J) tactics and strategies for fighting fires occurring at the wildland-urban interface;

(K) tactics and strategies for fighting fires involving hazardous materials;

(L) advanced emergency medical services training;

(M) use of and familiarity with the Federal Response Plan;

(N) leadership and strategic skills, including integrated management systems operations and integrated response;

(O) applying new technology and developing strategies and tactics for fighting wildland fires;

(P) integrating the activities of terrorism response agencies into national terrorism incident response systems;

(Q) tactics and strategies for fighting fires at United States ports, including fires on the water and aboard vessels; and

(R) the training of present and future instructors in the aforementioned subjects;

(2) develop model curricula, training programs and other educational materials suitable for use at other educational institutions, and make the materials available without charge;

(3) develop and administer a program of correspondence courses to advance the knowledge and skills of fire service personnel;

(4) develop and distribute to appropriate officials model questions suitable for use in conducting entrance and promotional examinations for fire service personnel; and

(5) encourage the inclusion of fire prevention and detection technology and practices in the education and professional practice of ar-

chitects, builders, city planners, and others engaged in design and planning affected by fire safety problems.

(e) COORDINATION OF TRAINING.—The Administrator shall coordinate training provided under subsection (d)(1) with the Attorney General, the Secretary of Health and Human Services, and the heads of other Federal agencies—

(1) to ensure that the training does not duplicate existing courses available to fire service personnel; and

(2) to establish a mechanism for eliminating duplicative training programs.

(f) TECHNICAL ASSISTANCE.—The Administrator may, to the extent that the Administrator determines it necessary to meet the needs of the Nation, encourage new programs and strengthen existing programs of education and training by local fire services, units, and departments, State and local governments, and private institutions, by providing technical assistance and advice to—

(1) vocational training programs in techniques of fire prevention, fire inspection, firefighting, and fire and arson investigation;

(2) fire training courses and programs at junior colleges; and

(3) 4-year degree programs in fire engineering at colleges and universities.

(g) ASSISTANCE TO STATE AND LOCAL FIRE SERVICE TRAINING PROGRAMS.—The Administrator may provide assistance to State and local fire service training programs through grants, contracts, or otherwise. The assistance shall not exceed 7.5 percent of the amount authorized to be appropriated in each fiscal year pursuant to section 11388 of this title.

(h) CONSTRUCTION COSTS..—Of the sums authorized to be appropriated for the purpose of implementing the programs of the Administration, not more than $9,000,000 shall be available for the construction of facilities of the Academy. Sums for the construction shall remain available until expended.

(i) EDUCATIONAL AND PROFESSIONAL ASSISTANCE.—

(1) IN GENERAL.—The Administrator may—

(A) provide stipends to students attending Academy courses and programs, in amounts up to 75 percent of the expense of attendance, as established by the Superintendent;

(B) provide stipends to students attending courses and nondegree training programs approved by the Superintendent at universities, colleges, and junior colleges, in amounts up to 50 percent of the cost of tuition;

(C) make or enter into contracts to make payments to institutions of higher education for loans, not to exceed $2,500 per academic year for an individual who is enrolled on a full-time basis in an undergraduate or graduate program of fire research or engineering that is certified by the Superintendent; and

(D) establish and maintain a placement and promotion opportunities center in cooperation with the fire services, for firefighters who wish to learn and take advantage of different or better career opportunities.

(2) TERMS AND CONDITIONS OF LOANS.—Loans under paragraph (1)(C) shall be made on such terms and subject to such conditions as the Superintendent and each institution involved may jointly determine.

(3) CAREER ASSISTANCE NOT LIMITED TO ACADEMY STUDENTS AND GRADUATES.—The placement and promotion opportunities center shall not limit assistance under paragraph (1)(D) to students and graduates of the Academy but shall undertake to assist all fire service personnel.

(j) BOARD OF VISITORS.—The Administrator of FEMA shall establish a procedure for the selection of professionals in the field of fire safety, fire prevention, fire control, research and development in fire protection, treatment and rehabilitation of fire victims, or local government services management to serve as members of a Board of Visitors for the Academy. Pursuant to the procedure, the Administrator of FEMA shall select 8 individuals to serve as members of the Board of Visitors to serve such terms as the Administrator of FEMA may prescribe. The function of the Board of Visitors shall be to review annually the program of the Academy and to make comments and recommendations to the Administrator of FEMA regarding the operation of the Academy and any improvements in the Academy that the Board of Visitors considers appropriate. Each member of the Board of Visitors shall be reimbursed for expenses actually incurred by the member in the performance of the member's duties as a member of the Board of Visitors.

(k) ADMISSION.—The Superintendent may admit to the courses and programs of the Academy individuals who are members of the firefighting, rescue, and civil defense forces of the Nation and such other individuals, including candidates for membership in these forces, as the Superintendent determines can benefit from attendance. Students shall be admitted from any State, with due regard to adequate representation in the student body of all geographic regions of the Nation. In selecting students, the Superintendent may seek nominations and advice from the fire services and other organizations that wish to send students to the Academy. The Superintendent shall offer, at the Academy and at other sites, courses and train-

ing assistance as necessary to accommodate all geographic regions and needs of career and volunteer firefighters.

(l) ON-SITE TRAINING.—

(1) IN GENERAL.—Except as provided in paragraph (2), the Administrator may enter into a contract with nationally recognized organizations that have established on-site training programs that comply with national voluntary consensus standards for fire service personnel to facilitate the delivery of the education and training programs outlined in subsection (d)(1) directly to fire service personnel.

(2) LIMITATION.—

(A) IN GENERAL.—The Administrator may not enter into a contract with an organization described in paragraph (1) unless the organization provides training that—

(i) leads to certification by a fire service training program that is accredited by a nationally recognized accreditation organization; or

(ii) the Administrator determines is of equivalent quality to a fire service training program described in clause (i).

(B) APPROVAL OF UNACCREDITED FIRE SERVICE TRAINING PROGRAMS.—The Administrator may consider the fact that an organization has provided a satisfactory fire service training program pursuant to a cooperative agreement with a Federal agency as evidence that the program is of equivalent quality to a fire service training program described in subparagraph (A)(i).

(3) RESTRICTION ON USE OF FUNDS.—The amounts expended by the Administrator to carry out this subsection in a fiscal year shall not exceed 7.5 percent of the amount authorized to be appropriated in that fiscal year pursuant to section 11388 of this title.

(m) TRIENNIAL REPORT.—In the 1st annual report filed pursuant to section 11387 of this title for which the deadline for filing is after the expiration of the 18-month period that begins on October 8, 2008, and in every 3d annual report thereafter, the Administrator shall include information about changes made to the National Fire Academy curriculum, including—

(1) the basis for the changes, including a review of the incorporation of lessons learned by emergency response personnel after significant emergency events and emergency preparedness exercises performed under the National Exercise Program; and

(2) the desired training outcome of all the changes.

§ 11356. Fire technology

(a) DEVELOPMENT.—The Administrator shall conduct a continuing program of development, testing, and evaluation of equipment for use by the

Nation's fire, rescue, and civil defense services, with the aim of making available improved suppression, protective, auxiliary, and warning devices incorporating the latest technology. Attention shall be given to the standardization, compatibility, and interchangeability of the equipment. The development, testing, and evaluation activities shall include—

(1) safer, less cumbersome articles of protective clothing, including helmets, boots, and coats;

(2) breathing apparatus with the necessary duration of service, reliability, low weight, and ease of operation for practical use;

(3) safe and reliable auxiliary equipment for use in fire prevention, detection, and control, such as fire location detectors, visual and audio communications equipment, and mobile equipment;

(4) special clothing and equipment needed for forest fires, brush fires, oil and gasoline fires, aircraft fires and crash rescue, fires occurring aboard waterborne vessels, and in other special firefighting situations;

(5) fire detectors and related equipment for residential use with high sensitivity and reliability, and that are sufficiently inexpensive to purchase, install, and maintain to ensure wide acceptance and use;

(6) in-place fire prevention systems of low cost and of increased reliability and effectiveness;

(7) methods of testing fire alarms and fire protection devices and systems on a non-interference basis;

(8) the development of purchase specifications, standards, and acceptance and validation test procedures for the equipment and devices; and

(9) operation tests, demonstration projects, and fire investigations in support of the activities set forth in this section.

(b) LIMITATION ON MANUFACTURE AND SALE OF EQUIPMENT.—The Administration shall not engage in the manufacture or sale of any equipment or device developed pursuant to this section, except to the extent that it considers it necessary to adequately develop, test, or evaluate the equipment or device.

(c) MANAGEMENT STUDIES.—

(1) IN GENERAL.—The Administrator may conduct, directly or through contracts or grants, studies of the operations and management aspects of fire services, utilizing quantitative techniques, such as operations research, management economics, cost effectiveness studies, and such other techniques and methods as may be applicable and useful. The studies shall include the allocation of resources, the optimum location of fire stations, the optimum geographical area for an integrated

fire service, the manner of responding to alarms, the operation of city-wide and regional fire dispatch centers, firefighting under conditions of civil disturbance, and the effectiveness, frequency, and methods of building inspections.

(2) EMERGENCY MEDICAL SERVICES.—The Administrator may conduct, directly or through contracts or grants, studies of the operations and management aspects of fire service-based emergency medical services and coordination between emergency medical services and fire services. The studies may include the optimum protocols for on-scene care, the allocation of resources, and the training requirements for fire service-based emergency medical services.

(3) PRODUCTIVITY AND EFFICIENCY, JOB CATEGORIES AND SKILLS, REDUCTION OF INJURIES, EFFECTIVE PROGRAMS AND ACTIVITIES, AND TECHNIQUES.—The Administrator may conduct, directly or through contracts or grants, research concerning the productivity and efficiency of fire service personnel, the job categories and skills required by fire services under varying conditions, the reduction of injuries to fire service personnel, the most effective fire prevention programs and activities, and techniques for accurately measuring and analyzing the foregoing.

(4) NEW TECHNOLOGY, STANDARDS, OPERATING METHODS, COMMAND TECHNIQUES, AND MANAGEMENT SYSTEMS.—The Administrator may conduct, directly or through contracts, grants, or other forms of assistance, development, testing and demonstration projects to the extent considered necessary to introduce and to encourage the acceptance of new technology, standards, operating methods, command techniques, and management systems for utilization by the fire services.

(5) ASSIST FIRE SERVICES.—The Administrator may assist the Nation's fire services, directly or through contracts, grants, or other forms of assistance, to measure and evaluate, on a cost-benefit basis, the effectiveness of the programs and activities of each fire service and the predictable consequences on the applicable local fire services of coordination or combination, in whole or in part, in a regional, metropolitan, or statewide fire service.

(d) RURAL AND REMOTE AREAS AND WILDLAND-URBAN INTERFACE ASSISTANCE.—The Administrator may, in coordination with the Secretary of Agriculture, the Secretary of the Interior, and the Wildland Fire Leadership Council, assist the fire services of the United States, directly or through contracts, grants, or other forms of assistance, in sponsoring and encouraging research into approaches, techniques, systems, equipment, and land-use policies to improve fire prevention and control in—

(1) the rural and remote areas of the United States; and

(2) the wildland-urban interface.

(e) ASSISTANCE TO OTHER FEDERAL AGENCIES.—At the request of other Federal agencies, including the Department of Agriculture and the Department of the Interior, the Administrator may provide assistance in fire prevention and control technologies, including methods of containing insect-infested forest fires and limiting dispersal of resultant fire particle smoke, and methods of measuring and tracking the dispersal of fine-particle smoke resulting from fires of insect-infested fuel.

(f) TECHNOLOGY EVALUATION AND STANDARDS DEVELOPMENT.—

(1) IN GENERAL.—In addition to, or as part of, the program conducted under subsection (a), the Administrator, in consultation with the National Institute of Standards and Technology, the Inter-Agency Board for Equipment Standardization and Inter-Operability, the National Institute for Occupational Safety and Health, the Science and Technology Directorate of the Department, national voluntary consensus standards development organizations, interested Federal, State, and local agencies, and other interested parties, shall—

(A) develop new, and utilize existing, measurement techniques and testing methodologies for evaluating new firefighting technologies, including—

(i) personal protection equipment;

(ii) devices for advance warning of extreme hazard;

(iii) equipment for enhanced vision;

(iv) devices to locate victims, firefighters, and other rescue personnel in above-ground and below-ground structures;

(v) equipment and methods to provide information for incident command, including the monitoring and reporting of individual personnel welfare;

(vi) equipment and methods for training, especially for virtual reality training; and

(vii) robotics and other remote-controlled devices;

(B) evaluate the compatibility of new equipment and technology with existing firefighting technology; and

(C) support the development of new voluntary consensus standards through national voluntary consensus standards organizations for new firefighting technologies based on techniques and methodologies described in subparagraph (A).

(2) STANDARDS FOR NEW EQUIPMENT OR SYSTEMS.—

(A) REQUIREMENT THAT STANDARDS BE MET FOR NEW EQUIPMENT OR SYSTEMS PURCHASED THROUGH ASSISTANCE PROGRAM.—The Administrator shall, by regulation, require that new

equipment or systems purchased through the assistance program established by section 11377 of this title meet or exceed applicable voluntary consensus standards for the equipment or systems for which applicable voluntary consensus standards have been established.

(B) EXPLANATION WHY NEW EQUIPMENT OR SYSTEMS THAT DON'T MEET OR EXCEED STANDARDS WILL BETTER SERVE NEEDS OF APPLICANT.—

(i) IN GENERAL.—If an applicant for a grant under section 11377 of this title proposes to purchase, with assistance provided under the grant, new equipment or systems that do not meet or exceed applicable voluntary consensus standards, the applicant shall include in the application an explanation of why the equipment or systems will serve the needs of the applicant better than equipment or systems that do meet or exceed the standards.

(ii) SECOND GRANT REQUEST IN APPLICATION.—Applicants that apply for a grant under the terms of clause (i) may include a 2d grant request in the application to be considered by the Administrator in the event that the Administrator does not approve the primary grant request on the grounds of the equipment not meeting applicable voluntary consensus standards.

(C) WAIVER.—The Administrator may waive the requirement under subparagraph (A) with respect to specific standards. In making a determination whether or not to waive the requirement with respect to a specific standard, the Administrator shall, to the greatest extent practicable—

(i) consult with grant applicants and other members of the fire services regarding the impact on fire departments of the requirement to meet or exceed the specific standard;

(ii) take into consideration the explanation provided by the applicant under subparagraph (B); and

(iii) seek to minimize the impact of the requirement to meet or exceed the specific standard on the applicant, particularly if meeting the standard would impose additional costs.

(g) COORDINATION.—In establishing and conducting programs under this section, the Administrator shall take full advantage of applicable technological developments made by other departments and agencies of the Fed-

eral Government, by State and local governments, and by business, industry, and nonprofit associations.

(h) PUBLICATION OF RESEARCH RESULTS.—

(1) IN GENERAL.—For each fire-related research program funded by the Administration, the Administrator shall make available to the public on the website of the Administration the following:

(A) A description of the research program, including the scope, methodology, and goals of the research program.

(B) Information that identifies the individuals or institutions conducting the research program.

(C) The amount of funding provided by the Administration for the research program.

(D) The results or findings of the research program.

(2) DEADLINES.—The information required by paragraph (1) shall be published with respect to a research program as follows:

(A) The information described in subparagraphs (A), (B), and (C) of paragraph (1) with respect to the research program shall be made available under paragraph (1) not later than 30 days after the Administrator has awarded the funding for the research program.

(B) The information described in subparagraph (D) of paragraph (1) with respect to a research program shall be made available under paragraph (1) not later than 60 days after the date the research program has been completed.

§ 11357. National Fire Data Center

(a) FUNCTIONS.—

(1) IN GENERAL.—The Administrator shall operate, directly or through contracts or grants, an integrated, comprehensive National Fire Data Center for the selection, analysis, publication, and dissemination of information related to the prevention, occurrence, control, and results of fires of all types. The program of the National Fire Data Center shall be designed to—

(A) provide an accurate nationwide analysis of the fire problem;

(B) identify major problem areas;

(C) assist in setting priorities;

(D) determine possible solutions to problems; and

(E) monitor the progress of programs to reduce fire losses.

(2) GATHERING AND ANALYZING INFORMATION.—To carry out the functions described in paragraph (1), the National Fire Data Center shall gather and analyze—

(A) information on the frequency, causes, spread, and extinguishment of fires;

(B) information on the number of injuries and deaths resulting from fires, including the maximum available information on the specific causes and nature of the injuries and deaths, categorized by the type of fire, and information on property losses;

(C) information on the occupational hazards faced by firefighters, including the causes of deaths and injuries arising, directly and indirectly, from firefighting activities, including—

(i) all injuries sustained by a firefighter and treated by a doctor, categorized by the type of firefighter;

(ii) all deaths sustained while undergoing a pack test or preparing for a work capacity;

(iii) all injuries or deaths resulting from vehicle accidents; and

(iv) all injuries or deaths resulting from aircraft crashes;

(D) information on all types of firefighting activities, including inspection practices;

(E) technical information related to building construction, fire properties of materials, and similar information;

(F) information on fire prevention and control laws, systems, methods, techniques, and administrative structures used in foreign nations;

(G) information on the causes, behavior, and best method of control of other types of fire, including forest fires, brush fires, fire underground, oil blow-out fires, and water-borne fires; and

(H) such other information and data as is considered useful and applicable.

(b) METHODS.—In carrying out the program of the National Fire Data Center, the Administrator may—

(1) develop standardized data reporting methods;

(2) encourage and assist Federal, State, local, and other agencies, public and private, in developing and reporting information; and

(3) make full use of existing data gathering and analysis organizations, both public and private, including the Center for Firefighter Injury Research and Safety Trends.

(c) DISSEMINATION OF FIRE DATA.—The Administrator shall ensure dissemination to the maximum extent possible of fire data collected and developed by the National Fire Data Center, and shall make the data, information, and analysis available in appropriate form to Federal agencies, State

and local governments, private organizations, industry, business, and other interested persons.

(d) NATIONAL FIRE INCIDENT REPORTING SYSTEM UPDATE.—The Administrator shall update the National Fire Incident Reporting System to ensure that the information in the system is available, and can be updated, through the Internet and in real time.

(e) MEDICAL PRIVACY OF FIREFIGHTERS.—The collection, storage, and transfer of medical data collected under this section shall be conducted in accordance with—

(1) the privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191, 42 U.S.C. 1320d–2 note); and

(2) other applicable regulations, including parts 160, 162, and 164 of title 45, Code of Federal Regulations (as in effect on March 12, 2019).

§ 11358. Master plans

(a) DEFINITION OF MASTER PLAN.—For the purposes of this section, the term ''master plan'' means a plan that will result in the planning and implementation in the area involved of a general program of action for fire prevention and control. The master plan is reasonably expected to include—

(1) a survey of the resources and personnel of existing fire services and an analysis of the effectiveness of the fire and building codes in the area;

(2) an analysis of short- and long-term fire prevention and control needs in the area;

(3) a plan to meet the fire prevention and control needs in the area; and

(4) an estimate of cost and realistic plans for financing the implementation of the plan and operation on a continuing basis and a summary of problems that are anticipated in implementing the master plan.

(b) ENCOURAGEMENT BY ADMINISTRATOR.—The establishment of master plans for fire prevention and control is the responsibility of the States and the political subdivisions of the States. The Administrator may encourage and assist the States and political subdivisions in the planning activities, consistent with the Administrator's powers and duties under this subchapter.

(c) MUTUAL AID SYSTEMS.—

(1) IN GENERAL.—The Administrator shall provide technical assistance and training to State and local fire service officials to establish

nationwide and State mutual aid systems for dealing with national emergencies that—

(A) include threat assessment and equipment deployment strategies;

(B) include means of collecting asset and resource information to provide accurate and timely data for regional deployment; and

(C) are consistent with the Federal Response Plan.

(2) MODEL MUTUAL AID PLANS.—The Administrator shall develop and make available to State and local fire service officials model mutual aid plans for both intrastate and interstate assistance.

§ 11359. Reimbursement for costs of firefighting on Federal property

(a) FILING OF CLAIMS.—Each fire service that engages in the fighting of a fire on property that is under the jurisdiction of the United States may file a claim with the Administrator for the amount of direct expenses and direct losses incurred by the fire service as a result of fighting the fire. The claim shall include such supporting information as the Administrator may prescribe.

(b) DETERMINATION.—On receipt of a claim filed under subsection (a), the Administrator shall determine—

(1) what payments, if any, to the fire service or its parent jurisdiction, including taxes or payments in lieu of taxes, the United States has made for the support of fire services on the property in question;

(2) the extent to which the fire service incurred additional firefighting costs, over and above its normal operating costs, in connection with the fire that is the subject of the claim; and

(3) the amount, if any, of the additional costs referred to in paragraph (2) that were not adequately covered by the payments referred to in paragraph (1).

(c) PAYMENT.—The Administrator of FEMA shall forward the claim and a copy of the Administrator's determination under subsection (b)(3) to the Secretary of the Treasury. The Secretary of the Treasury shall, on receipt of the claim and determination, pay the fire service or its parent jurisdiction, from any money in the Treasury not otherwise appropriated but subject to reimbursement (from any appropriations that may be available or that may be made available for the purpose) by the Federal department or agency under whose jurisdiction the fire occurred, an amount no greater than the amount determined with respect to the claim under subsection (b)(3).

(d) ADJUDICATION.—In the case of a dispute arising in connection with a claim under this section, the United States Court of Federal Claims has jurisdiction to adjudicate the claim and enter judgment accordingly.

§ 11360. Review of fire prevention codes

The Administrator may review, evaluate, and suggest improvements in State and local fire prevention codes, building codes, and relevant Federal or private codes and regulations. In evaluating a code, the Administrator shall consider the human impact of all code requirements, standards, or provisions in terms of comfort and habitability for residents or employees, as well as the fire prevention and control value or potential of each requirement, standard, or provision.

§ 11361. Fire safety effectiveness statements

The Administrator may encourage owners and managers of residential multiple-unit, commercial, industrial, and transportation structures to prepare fire safety effectiveness statements, pursuant to standards, forms, rules, and regulations to be developed and issued by the Administrator.

§ 11362. Annual conference

The Administrator may organize, or participate in organizing, an annual conference on fire prevention and control. The Administrator may pay, in whole or in part, the cost of the conference and the expenses of some or all of the participants. All of the Nation's fire services are eligible to send representatives to each conference to discuss, exchange ideas on, and participate in educational programs on new techniques in fire prevention and control. The conferences shall be open to the public.

§ 11363. Public safety awards

(a) DEFINITION OF PUBLIC SAFETY OFFICER.—As used in this section, the term ''public safety officer'' means an individual serving a public agency, with or without compensation, as—

(1) a firefighter;

(2) a law enforcement officer, including a corrections or court officer; or

(3) a civil defense officer.

(b) ESTABLISHMENT.—There is an honorary award for the recognition of outstanding and distinguished service by public safety officers known as the Administrator's Award For Distinguished Public Safety Service (in this section referred to as the ''Administrator's Award'').

(c) DESCRIPTION.—The Administrator's Award shall be presented by the Administrator of FEMA or by the Attorney General to public safety officers for distinguished service in the field of public safety.

(d) AWARD.—Each Administrator's Award shall consist of an appropriate citation.

(e) REGULATIONS.—The Administrator of FEMA and the Attorney General shall issue jointly such regulations as may be necessary to carry out this section.

§ 11364. Public access to information

(a) IN GENERAL.—Copies of any document, report, statement, or information received or sent by the Administrator of FEMA or the Administrator shall be made available to the public pursuant to section 552 of title 5.

(b) TRADE SECRET.—Notwithstanding section 552(b) of title 5 and section 1905 of title 18, the Administrator of FEMA may disclose information that concerns or relates to a trade secret—

(1) on request, to other Federal Government departments and agencies for official use;

(2) on request, to a committee of Congress having jurisdiction over the subject matter to which the information relates;

(3) in a judicial proceeding under a court order formulated to preserve the confidentiality of the information without impairing the proceedings; and

(4) to the public when the Administrator of FEMA determines the disclosure to be necessary to protect health and safety after notice and opportunity for comment in writing or for discussion in closed session within 15 days by the party to which the information pertains (if the delay resulting from the notice and opportunity for comment would not be detrimental to health and safety).

§ 11365. Assistance to Consumer Product Safety Commission

On request, the Administrator shall assist the Consumer Product Safety Commission in the development of fire safety standards or codes for consumer products, as defined in the Consumer Product Safety Act (15 U.S.C. 2051 et seq.).

§ 11366. Arson prevention, detection, and control

The Administrator shall—

(1) develop arson detection techniques to assist Federal agencies and States and local jurisdictions in improving arson prevention, detection, and control;

(2) provide training and instructional materials in the skills and knowledge necessary to assist Federal, State, and local fire service and law enforcement personnel in arson prevention, detection, and control, with particular emphasis on the needs of volunteer firefighters for improved and more widely available arson training courses;

(3) formulate methods for collection of arson data that would be compatible with methods of collection used for the uniform crime statistics of the Federal Bureau of Investigation;

(4) develop and implement programs for improved collection of nationwide arson statistics in the National Fire Incident Reporting System at the National Fire Data Center;

(5) develop programs for public education on the extent, causes, and prevention of arson; and

(6) develop handbooks to assist Federal, State, and local fire service and law enforcement personnel in arson prevention and detection.

§ 11367. Arson prevention grants

(a) DEFINITIONS.—As used in this section:

(1) ARSON.—The term ''arson'' includes all incendiary and suspicious fires.

(2) OFFICE.—The term ''Office'' means the Office of Fire Prevention and Arson Control of the Administration.

(b) GRANTS.—The Administrator, acting through the Office, shall carry out a demonstration program under which not more than 10 grant awards shall be made to States, or consortia of States, for programs relating to arson research, prevention, and control.

(c) GOALS.—In carrying out this section, the Administrator shall award 2-year grants on a competitive, merit basis to States, or consortia of States, for projects that promote 1 or more of the following goals:

(1) To improve the training by States leading to professional certification of arson investigators, in accordance with nationally recognized certification standards.

(2) To provide resources for the formation of arson task forces or interagency organizational arrangements involving police and fire departments and other relevant local agencies, such as a State arson bureau and the office of a fire marshal of a State.

(3) To combat fraud as a cause of arson and to advance research at the State and local levels on the significance and prevention of fraud as a motive for setting fires.

(4) To provide for the management of arson squads, including—

(A) training courses for fire departments in arson case management, including standardization of investigative techniques and reporting methodology;

(B) the preparation of arson unit management guides; and

(C) the development and dissemination of new public education materials relating to the arson problem.

(5) To combat civil unrest as a cause of arson and to advance research at the State and local levels on the prevention and control of arson linked to urban disorders.

(6) To combat juvenile arson, such as juvenile fire-setter counseling programs and similar intervention programs, and to advance research at the State and local levels on the prevention of juvenile arson.

(7) To combat drug-related arson and to advance research at the State and local levels on the causes and prevention of drug-related arson.

(8) To combat domestic violence as a cause of arson and to advance research at the State and local levels on the prevention of arson arising from domestic violence.

(9) To combat arson in rural areas and to improve the capability of firefighters to identify and prevent arson-initiated fires in rural areas and public forests.

(10) To improve the capability of firefighters to identify and combat arson through expanded training programs, including—

(A) training courses at the State fire academies; and

(B) innovative courses developed with the Academy and made available to volunteer firefighters through regional delivery methods, including teleconferencing and satellite delivered television programs.

(d) ASSISTANCE IN STRUCTURING OF APPLICATIONS.—The Administrator shall assist grant applicants in structuring their applications so as to ensure that at least 1 grant is awarded for each goal described in subsection (c).

(e) STATE QUALIFICATION CRITERIA.—To qualify for a grant under this section, a State, or consortium of States, shall provide assurances adequate to the Administrator that the State or consortium—

(1) will obtain at least 25 percent of the cost of programs funded by the grant, in cash or in kind, from non-Federal sources;

(2) will not as a result of receiving the grant decrease the prior level of spending of funds of the State or consortium from non-Federal sources for arson research, prevention, and control programs;

(3) will use no more than 10 percent of funds provided under the grant for administrative costs of the programs; and

(4) is making efforts to ensure that all local jurisdictions will provide arson data to the National Fire Incident Reporting System or the Uniform Crime Reporting program.

(f) EXTENSION.—A grant awarded under this section may be extended for 1 or more additional periods, at the discretion of the Administrator, subject to the availability of appropriations.

(g) TECHNICAL ASSISTANCE.—The Administrator shall provide technical assistance to States in carrying out programs funded by grants under this section.

(h) CONSULTATION AND COOPERATION.—In carrying out this section, the Administrator shall consult and cooperate with other Federal agencies to enhance program effectiveness and avoid duplication of effort, including the conduct of regular meetings initiated by the Administrator with representatives of other Federal agencies concerned with arson and concerned with efforts to develop a more comprehensive profile of the magnitude of the national arson problem.

(i) REGULATIONS.—The Administrator shall issue regulations to implement this section, including procedures for grant applications.

(j) ADMINISTRATION.—The Administrator shall directly administer the grant program required by this section, and shall not enter into a contract under which the grant program or a portion of the program will be administered by another party.

(k) PURCHASE OF AMERICAN MADE EQUIPMENT AND PRODUCTS.—

(1) SENSE OF CONGRESS.—It is the sense of Congress that a recipient of a grant under this section should purchase, when available and cost-effective, American made equipment and products when expending grant monies.

(2) NOTICE TO RECIPIENTS OF ASSISTANCE.—In allocating grants under this section, the Administrator shall provide to each recipient a notice describing the statement made in paragraph (1) by Congress.

§ 11368. Review of existing response information

(a) DEFINITION OF EMERGENCY RESPONSE PERSONNEL.—As used in this section, the term ''emergency response personnel'' means personnel responsible for mitigation activities in a medical emergency, fire emergency, hazardous material emergency, or natural disaster.

(b) IN GENERAL.—The Administrator shall conduct a review of existing response information used by emergency response personnel at the State and local levels to evaluate its accuracy and consistency, and to determine whether it is properly expressed. The information should clearly communicate to emergency response personnel the probable hazards that they must contend with in an emergency situation involving hazardous materials, and the appropriate response to those hazards.

§ 11369. Working group

(a) ESTABLISHMENT.—For the purpose of carrying out section 11368 of this title, there is a working group established by the Administrator that, at a minimum, consists of—

(1) program officials from each of—

(A) the Environmental Protection Agency;

(B) the National Oceanic and Atmospheric Administration;

(C) the Department of Transportation;

(D) the Occupational Safety and Health Administration; and

(E) the Bureau of Alcohol, Tobacco, Firearms, and Explosives, Department of Justice;

(2) State and local operational officials with emergency response or relevant regulatory responsibilities; and

(3) representatives of companies engaged in the manufacture and processing of chemicals.

(b) DUTIES.—The working group shall develop and disseminate hazardous materials identification and response data and collect, collate, analyze, and disseminate hazardous materials incident data.

§ 11370. Annual revision of recommendations

The working group established under section 11369 of this title shall meet as needed, but at least once every 12 months, to review and recommend changes and additions to the report cited in section 4 of the Firefighters' Safety Study Act (Public Law 101–446, 104 Stat. 1045) that are necessary and appropriate for operational personnel at the local level.

§ 11371. Listings of places of public accommodation that meet guidelines

(a) PERIODIC UPDATE OF LIST BY STATES.—The Administrator of FEMA shall formulate procedures under which each State (acting through its Governor (or if none exists, chief executive officer) or the Governor's or chief executive officer's designee) shall periodically update the list of those places of public accommodation affecting commerce located in each State that meet the requirements of the guidelines described in section 11372 of this title that the State submitted pursuant to section 28(a)(1) of the Federal Fire Prevention and Control Act of 1974 (Public Law 93–498, as added by section 3(a) of the Hotel and Motel Fire Safety Act of 1990 (Public Law 101–391, 104 Stat. 747)).

(b) COMPILATION AND DISTRIBUTION OF MASTER LIST BY ADMINISTRATOR OF FEMA.—

(1) DEFINITION OF AGENCY.—For purposes of this subsection, the term ''agency'' has the same meaning given the term in section 5701 of title 5.

(2) IN GENERAL.—The Administrator of FEMA shall periodically update the national master list of all of the places of public accommodation affecting commerce located in each State that meet the requirements of the guidelines described in section 11372 of this title compiled and published in the Federal Register pursuant to section 28(b)(1) of the Federal Fire Prevention and Control Act of 1974 (Public Law 93–498, as added by section 3(a) of the Hotel and Motel Fire Safety Act of 1990 (Public Law 101–391, 104 Stat. 748)) to reflect changes in the State lists submitted to the Administrator of FEMA pursuant to subsection (a), and shall periodically redistribute the updated master list to each agency of the Federal Government.

§ 11372. Dissemination of fire prevention and control information

The Administrator of FEMA, acting through the Administrator, may take steps to encourage the States to promote the use of automatic sprinkler systems and automatic smoke detection systems and disseminate to the maximum extent possible information on the life safety value and use of those systems. The steps may include providing copies of the guidelines described in section 11373 of this title and of the master list compiled under section 28(b)(1) of the Federal Fire Prevention and Control Act of 1974 (Public Law 93–498, as added by section 3(a) of the Hotel and Motel Fire Safety Act of 1990 (Public Law 101–391, 104 Stat. 748)) to Federal agencies, State and local governments, and fire services throughout the United States, and making copies of the master list available on request to interested private organizations and individuals.

§ 11373. Fire prevention and control guidelines for places of public accommodation

(a) DEFINITIONS.–For purposes of this section, the following definitions apply:

(1) AUTOMATIC SPRINKLER SYSTEM.—The term ''automatic sprinkler system'' means an electronically supervised, integrated system of piping to which sprinklers are attached in a systematic pattern, and that, when activated by heat from a fire, will protect human lives by discharging water over the fire area, and by providing appropriate warning signals (to the extent the signals are required by Federal, State, or local laws or regulations) through the building's fire alarm system.

(2) GOVERNMENTAL AUTHORITY HAVING JURISDICTION.—The term ''governmental authority having jurisdiction'' means the Federal, State, local, or other governmental entity with statutory or regulatory author-

ity for the approval of fire safety systems, equipment, installations, or procedures in a specified locality.

(3) SMOKE DETECTOR.—The term ''smoke detector'' means an alarm that is designed to respond to the presence of visible or invisible particles of combustion.

(b) CONTENTS.—The guidelines referred to in sections 11371 and 11372 of this title consist of—

(1) a requirement that hard-wired, single-station smoke detectors be installed in accordance with National Fire Protection Association Standard 74 or any successor standard to that standard in each guest room in each place of public accommodation affecting commerce; and

(2) a requirement that an automatic sprinkler system be installed in accordance with National Fire Protection Association Standard 13 or 13–R, or any successor standard to that standard, whichever is appropriate, in each place of public accommodation affecting commerce except those places that are 3 stories or lower.

(c) EXCEPTIONS.—

(1) AUTOMATIC SPRINKLER SYSTEM ALREADY INSTALLED.—The requirement described in subsection (b)(2) shall not apply to a place of public accommodation affecting commerce with an automatic sprinkler system installed before October 25, 1992, if the automatic sprinkler system is installed in compliance with an applicable standard (adopted by the governmental authority having jurisdiction, and in effect, at the time of installation) that required the placement of a sprinkler head in the sleeping area of each guest room.

(2) STANDARD PREVENTS COMPLIANCE WITH AUTOMATIC SPRINKLER SYSTEM STANDARD.—The requirement described in subsection (a)(2) shall not apply to a place of public accommodation affecting commerce to the extent that the place of public accommodation affecting commerce is subject to a standard that includes a requirement or prohibition that prevents compliance with a provision of National Fire Protection Association Standard 13 or 13–R, or any successor standard to that standard. In that, the place of public accommodation affecting commerce is exempt only from that specific provision.

(d) EFFECT ON STATE AND LOCAL LAW.—This section shall not be construed to limit the power of a State or political subdivision of a State to implement or enforce any law, rule, regulation, or standard concerning fire prevention and control.

§ 11374. Prohibiting Federal funding of conferences held at non-certified places of public accommodation

(a) IN GENERAL.—No Federal funds may be used to sponsor or fund in whole or in part a meeting, convention, conference, or training seminar that is conducted in, or that otherwise uses the rooms, facilities, or services of, a place of public accommodation that does not meet the requirements of the fire prevention and control guidelines described in section 11373 of this title.

(b) WAIVER.—

(1) IN GENERAL.—The head of an agency of the Federal Government sponsoring or funding a particular meeting, convention, conference, or training seminar may waive the prohibition described in subsection (a) if the head of the agency determines that a waiver of the prohibition is necessary in the public interest in the case of the particular event.

(2) DELEGATION OF AUTHORITY.—The head of an agency of the Federal Government may delegate the authority provided under paragraph (1) to waive the prohibition described in subsection (a) and to determine whether the waiver is necessary in the public interest to an officer or employee of the agency if the officer or employee is given the authority with respect to all meetings, conventions, conferences, and training seminars sponsored or funded by the agency.

(c) NOTICE REQUIREMENTS.—

(1) ADVERTISEMENTS AND APPLICATIONS.—

(A) IN GENERAL.—An advertisement for, or application for attendance at, a meeting, convention, conference, or training seminar sponsored or funded in whole or in part by the Federal Government shall include a notice regarding the prohibition described in subsection (a).

(B) NONAPPLICATION.—The requirement described in subparagraph (A) shall not apply in the case of an event for which a head of an agency of the Federal Government, pursuant to subsection (b), waives the prohibition described in subsection (a).

(2) PROVIDING NOTICE TO RECIPIENTS OF FUNDS.—

(A) DEFINITIONS.—In subparagraph (B), the terms ''Executive department'', ''Government corporation'', and ''independent establishment'' have the meanings given those terms in chapter 1 of title 5.

(B) IN GENERAL.—Each Executive department, Government corporation, and independent establishment providing Federal

funds to non-Federal entities shall notify recipients of the funds of the prohibition described in subsection (a).

§ 11375. Fire safety systems in federally assisted buildings

(a) DEFINITIONS.—For purposes of this section, the following definitions apply:

(1) AFFORDABLE COST.—The term ''affordable cost'' means the cost to a Federal agency of leasing office space in a building that is protected by an automatic sprinkler system or equivalent level of safety, which cost is no more than 10 percent greater than the cost of leasing available comparable office space in a building that is not so protected.

(2) AUTOMATIC SPRINKLER SYSTEM.—The term ''automatic sprinkler system'' means an electronically supervised, integrated system of piping to which sprinklers are attached in a systematic pattern, and that, when activated by heat from a fire—

(A) will protect human lives by discharging water over the fire area, in accordance with the National Fire Protection Association Standard 13, 13D, or 13R, whichever is appropriate for the type of building and occupancy being protected, or any successor standard to that standard; and

(B) includes an alarm signaling system with appropriate warning signals (to the extent the alarm systems and warning signals are required by Federal, State, or local laws or regulations) installed in accordance with the National Fire Protection Association Standard 72, or any successor standard to that standard.

(3) EQUIVALENT LEVEL OF SAFETY.—The term ''equivalent level of safety'' means an alternative design or system (that may include automatic sprinkler systems), based on fire protection engineering analysis, that achieves a level of safety equal to or greater than that provided by automatic sprinkler systems.

(4) FEDERAL EMPLOYEE OFFICE BUILDING.—The term ''Federal employee office building'' means an office building in the United States, whether owned or leased by the Federal Government, that is regularly occupied by more than 25 full-time Federal employees in the course of their employment.

(5) HOUSING ASSISTANCE.—The term ''housing assistance''—

(A) means assistance provided by the Federal Government to be used in connection with the provision of housing that is provided in the form of a grant, contract, loan, loan guarantee, cooperative agreement, interest subsidy, insurance, or direct appropriation; but

(B) does not include assistance provided by—

(i) the Secretary of Veterans Affairs;

(ii) the Federal Emergency Management Agency;

(iii) the Secretary of Housing and Urban Development under the single family mortgage insurance programs under the National Housing Act (12 U.S.C. 1701 et seq.) or the homeownership assistance program under section 235 of the National Housing Act (12 U.S.C. 1715z);

(iv) the National Homeownership Trust; or

(v) the Federal Deposit Insurance Corporation under the affordable housing program under section 40 of the Federal Deposit Insurance Act (12 U.S.C. 1831q).

(6) HAZARDOUS AREAS.—The term ''hazardous areas'' means those areas in a building referred to as hazardous areas in National Fire Protection Association Standard 101, known as the Life Safety Code, or any successor standard to that standard.

(7) MULTIFAMILY PROPERTY.—The term ''multifamily property'' means—

(A) in the case of housing for Federal employees or their dependents, a residential building consisting of more than 2 residential units that are under 1 roof; and

(B) in any other case, a residential building consisting of more than 4 residential units that are under 1 roof.

(8) PREFIRE PLAN.—The term ''prefire plan'' means specific plans for firefighting activities at a property or location.

(9) REBUILDING.—The term ''rebuilding'' means the repairing or reconstructing of portions of a multifamily property where the cost of the alterations is 70 percent or more of the replacement cost of the completed multifamily property, not including the value of the land on which the multifamily property is located.

(10) RENOVATED.—The term ''renovated'' means the repairing or reconstructing of 50 percent or more of the current value of a Federal employee office building, not including the value of the land on which the Federal employee office building is located.

(11) SMOKE DETECTORS.—The term ''smoke detectors'' means single or multiple station, self-contained alarm devices designed to respond to the presence of visible or invisible particles of combustion, installed in accordance with the National Fire Protection Association Standard 74 or any successor standard to that standard.

(b) FEDERAL EMPLOYEE OFFICE BUILDINGS.—

(1) RESTRICTION ON USE OF FEDERAL FUNDS.—

(A) CONSTRUCTION OR PURCHASE.—No Federal funds may be used for the construction or purchase of—

(i) a Federal employee office building of 6 or more stories unless during the period of occupancy by Federal employees the building is protected by an automatic sprinkler system or equivalent level of safety; or

(ii) any other Federal employee office building unless during the period of occupancy by Federal employees the hazardous areas of the building are protected by automatic sprinkler systems or an equivalent level of safety.

(B) LEASE.—

(i) IN GENERAL.—No Federal funds may be used for the lease of—

(I) a Federal employee office building of 6 or more stories, where at least some portion of the federally leased space is on the 6th floor or above and at least 35,000 square feet of space is federally occupied, unless during the period of occupancy by Federal employees the entire Federal employee office building is protected by an automatic sprinkler system or equivalent level of safety; or

(II) any other Federal employee office building unless during the period of occupancy by Federal employees the hazardous areas of the entire Federal employee office building are protected by automatic sprinkler systems or an equivalent level of safety.

(ii) EXCEPTION.—Clause (i)(I) shall not apply to the lease of a building the construction of which is completed before October 26, 1992, if the leasing agency certifies that no suitable building with automatic sprinkler systems or an equivalent level of safety is available at an affordable cost.

(C) RENOVATION.—No Federal funds may be used for the renovation of—

(i) a Federal employee office building of 6 or more stories that is owned by the Federal Government unless after that renovation the Federal employee office building is protected by an automatic sprinkler system or equivalent level of safety; or

(ii) any other Federal employee office building that is owned by the Federal Government unless after that renovation the hazardous areas of the Federal employee office building are protected by automatic sprinkler systems or an equivalent level of safety.

(D) ENTERING INTO OR RENEWING A LEASE OF A FEDERAL EMPLOYEE OFFICE BUILDING RENOVATED AFTER OCTOBER 26, 1992.—No Federal funds may be used for entering into or renewing a lease of—

(i) a Federal employee office building of 6 or more stories that is renovated after October 26, 1992, where at least some portion of the federally leased space is on the 6th floor or above and at least 35,000 square feet of space is federally occupied, unless after that renovation the Federal employee office building is protected by an automatic sprinkler system or equivalent level of safety; or

(ii) any other Federal employee office building that is renovated after October 26, 1992, unless after that renovation the hazardous areas of the Federal employee office building are protected by automatic sprinkler systems or an equivalent level of safety.

(2) EXCEPTIONS.—

(A) ACTIONS BEFORE OCTOBER 26, 1992, OR TEMPORARY LEASE.—Subparagraphs (A) and (B) of paragraph (1) shall not apply to—

(i) a Federal employee office building that was owned by the Federal Government before October 26, 1992;

(ii) space leased in a Federal employee office building if the space was leased by the Federal Government before October 26, 1992;

(iii) space leased on a temporary basis for not longer than 6 months; or

(iv) a Federal employee office building that becomes a Federal employee office building pursuant to a commitment to move Federal employees into the building that is made prior to October 26, 1992.

(B) INSTALLATION OF AUTOMATIC SPRINKLER SYSTEM OR EQUIVALENT LEVEL OF SAFETY NOT REQUIRED.—Nothing in this subsection shall require the installation of an automatic sprinkler system or equivalent level of safety by reason of the leasing, after October 26, 1992, of space below the 6th floor in a Federal employee office building.

(c) HOUSING.—

(1) FOR FEDERAL EMPLOYEES AND THEIR DEPENDENTS.—

(A) IN GENERAL.—No Federal funds may be used for the construction, purchase, lease, or operation by the Federal Government

of housing in the United States for Federal employees or their dependents unless—

(i) in the case of a multifamily property acquired or rebuilt by the Federal Government after October 26, 1992, the housing is protected, before occupancy by Federal employees or their dependents, by an automatic sprinkler system (or equivalent level of safety) and hard-wired smoke detectors; and

(ii) in the case of any other housing, the housing is protected by hard-wired smoke detectors.

(B) HIGHER LEVEL OF FIRE SAFETY PROTECTION NOT SUPERSEDED.—Nothing in this paragraph shall be construed to supersede any guidelines or requirements applicable to housing for Federal employees that call for a higher level of fire safety protection than is required under this paragraph.

(C) ADEQUATE AND RELIABLE ELECTRICAL SYSTEM NOT AVAILABLE.—Housing covered by this paragraph that does not have an adequate and reliable electrical system shall not be subject to the requirement under subparagraph (A) for protection by hard-wired smoke detectors but shall be protected by battery operated smoke detectors.

(D) HOUSING SCHEDULED FOR DEMOLITION.—If funding has been programmed or designated for the demolition of housing covered by this paragraph, the housing shall not be subject to the fire protection requirements of subparagraph (A) but shall be protected by battery operated smoke detectors.

(2) HOUSING ASSISTANCE.—

(A) NEWLY CONSTRUCTED MULTIFAMILY PROPERTY.—

(i) DEFINITION OF NEWLY CONSTRUCTED MULTIFAMILY PROPERTY.—For purposes of clause (ii), the term ''newly constructed multifamily property'' means a multifamily property of 4 or more stories above ground level—

(I) that is newly constructed after October 26, 1992; and

(II) for which—

(aa) housing assistance is used for the new construction; or

(bb) a binding commitment is made, before commencement of the construction, to provide housing assistance for the newly constructed property.

(ii) RESTRICTION ON USE OF HOUSING ASSISTANCE.—Housing assistance may not be used in connection with newly

constructed multifamily property, unless after the new construction the multifamily property is protected by an automatic sprinkler system and hard-wired smoke detectors.

(iii) EXCEPTION.—Clause (ii) shall not apply to multifamily property for which, before October 26, 1992, a binding commitment was made to provide housing assistance for the new construction of the property or for the newly constructed property.

(B) REBUILT MULTIFAMILY PROPERTY.—

(i) DEFINITION OF REBUILT MULTIFAMILY PROPERTY.—For purposes of this subparagraph, the term ''rebuilt multifamily property'' means a multifamily property of 4 or more stories above ground level—

(I) that is rebuilt after the last day of the second fiscal year that ends after October 26, 1992; and

(II) for which—

(aa) housing assistance is used for the rebuilding; or

(bb) a binding commitment is made, before commencement of the rebuilding, to provide housing assistance for the rebuilt property.

(ii) RESTRICTION ON USE OF HOUSING ASSISTANCE.—Except as provided in clause (iii), housing assistance may not be used in connection with rebuilt multifamily property, unless after the rebuilding the multifamily property complies with the chapter on existing apartment buildings of National Fire Protection Association Standard 101 (known as the Life Safety Code) or any successor standard to that standard, as in effect at the earlier of—

(I) the time of any approval by the Department of Housing and Urban Development of the specific plan or budget for rebuilding; or

(II) the time that a binding commitment is made to provide housing assistance for the rebuilt property.

(iii) EXCEPTION.—If a rebuilt multifamily property is subject to, and in compliance with, a provision of a State or local fire safety standard or code that prevents compliance with a specific provision of National Fire Protection Association Standard 101 or any successor standard to that standard, the requirement under clause (ii) shall not apply with respect to the specific provision.

(C) OTHER DWELLING UNIT.—Housing assistance may not be used in connection with any other dwelling unit, unless the unit is protected by a hard-wired or battery-operated smoke detector. For purposes of this subparagraph, housing assistance shall be considered to be used in connection with a particular dwelling unit only if the assistance is provided—

(i) for the particular unit, in the case of assistance provided on a unit-by-unit basis; or

(ii) for the multifamily property in which the unit is located, in the case of assistance provided on a structure-by-structure basis.

(d) REGULATIONS.—The Administrator of General Services, in cooperation with the Administration, the National Institute of Standards and Technology, and the Department of Defense shall promulgate regulations to further define the term ''equivalent level of safety'', and shall, to the extent practicable, base those regulations on nationally recognized codes.

(e) STATE AND LOCAL AUTHORITY NOT LIMITED.—Nothing in this section shall be construed—

(1) to limit the power of a State or political subdivision of a State to implement or enforce a law, rule, regulation, or standard that establishes requirements concerning fire prevention and control; or

(2) to reduce fire resistance requirements that otherwise would have been required.

(f) PREFIRE PLAN.—The head of a Federal agency that owns, leases, or operates a building or housing unit with Federal funds shall invite the local agency or voluntary organization having responsibility for fire protection in the jurisdiction where the building or housing unit is located to prepare, and biennially review, a prefire plan for the building or housing unit.

(g) REPORTS TO CONGRESS.—Within 3 years after October 26, 1992, and every 3 years thereafter, the Administrator of General Services shall transmit to Congress a report on the level of fire safety in Federal employee office buildings subject to fire safety requirements under this section. The report shall contain a description of the buildings for each Federal agency.

(h) RELATION TO OTHER REQUIREMENTS.—In the implementation of this section, the process for meeting space needs in urban areas shall continue to give first consideration to a centralized community business area and adjacent areas of similar character to the extent of any Federal requirement for meeting those needs.

§ 11376. CPR training

No funds shall be made available to a State or local government under section 11367 of this title unless the government has a policy to actively promote the training of its firefighters in cardiopulmonary resuscitation.

§ 11377. Firefighter assistance

(a) DEFINITIONS.—In this section:

(1) ADMINISTRATOR OF FEMA.—The term ''Administrator of FEMA'' means the Administrator of FEMA, acting through the Administrator.

(2) AVAILABLE GRANT FUNDS.—The term ''available grant funds'', with respect to a fiscal year, means those funds appropriated pursuant to the authorization of appropriations in subsection (q)(1) for the fiscal year less funds used for administrative costs pursuant to subsection (q)(2) in that fiscal year.

(3) CAREER FIRE DEPARTMENT.—The term ''career fire department'' means a fire department that has an all-paid force of firefighting personnel other than paid-on-call firefighters.

(4) COMBINATION FIRE DEPARTMENT.—The term ''combination fire department'' means a fire department that has—

(A) paid firefighting personnel; and

(B) volunteer firefighting personnel.

(5) FIREFIGHTING PERSONNEL.—The term ''firefighting personnel'' means individuals, including volunteers, who are firefighters, officers of fire departments, or emergency medical service personnel of fire departments.

(6) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given the term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

(7) NONAFFILIATED EMS ORGANIZATION.—The term ''nonaffiliated EMS organization'' means a public or private nonprofit emergency medical services organization that is not affiliated with a hospital and does not serve a geographic area in which the Administrator of FEMA finds that emergency medical services are adequately provided by a fire department.

(8) PAID-ON-CALL.—The term ''paid-on-call'' with respect to firefighting personnel means firefighting personnel who are paid a stipend for each event to which they respond.

(9) VOLUNTEER FIRE DEPARTMENT.—The term ''volunteer fire department'' means a fire department that has an all-volunteer force of firefighting personnel.

(b) ASSISTANCE PROGRAM.—

(1) AUTHORITY TO AWARD ASSISTANCE.—In accordance with this section, the Administrator of FEMA may award—

(A) assistance to firefighters grants under subsection (c); and

(B) fire prevention and safety grants and other assistance under subsection (d).

(2) DUTIES OF ADMINISTRATOR OF FEMA.—The Administrator of FEMA shall—

(A) establish specific criteria for the selection of grant recipients under this section; and

(B) provide assistance with application preparation to applicants for the grants.

(c) ASSISTANCE TO FIREFIGHTERS GRANTS.—

(1) IN GENERAL.—The Administrator of FEMA may, in consultation with the chief executives of the States in which the recipients are located, award grants on a competitive basis directly to—

(A) fire departments for the purpose of protecting the health and safety of the public and firefighting personnel throughout the United States against fire, fire-related, and other hazards;

(B) nonaffiliated EMS organizations to support the provision of emergency medical services; and

(C) State fire training academies for the purposes described in subparagraphs (G), (H), and (I) of paragraph (3).

(2) MAXIMUM GRANT AMOUNTS.—

(A) POPULATION.—The Administrator of FEMA may not award a grant under this subsection in excess of amounts as follows:

(i) In the case of a recipient that serves a jurisdiction with 100,000 people or fewer, the amount of the grant awarded to the recipient shall not exceed $1,000,000 in a fiscal year.

(ii) In the case of a recipient that serves a jurisdiction with more than 100,000 people but not more than 500,000 people, the amount of the grant awarded to the recipient shall not exceed $2,000,000 in a fiscal year.

(iii) In the case of a recipient that serves a jurisdiction with more than 500,000 but not more than 1,000,000 people, the amount of the grant awarded to the recipient shall not exceed $3,000,000 in a fiscal year.

(iv) In the case of a recipient that serves a jurisdiction with more than 1,000,000 people but not more than 2,500,000 people, the amount of the grant awarded to the recipient shall not exceed $6,000,000 for a fiscal year.

(v) In the case of a recipient that serves a jurisdiction with more than 2,500,000 people, the amount of the grant awarded to the recipient shall not exceed $9,000,000 in a fiscal year.

(B) AGGREGATE.—

(i) IN GENERAL.—Notwithstanding subparagraph (A) and except as provided under clause (ii), the Administrator of FEMA may not award a grant under this subsection in a fiscal year that exceeds 1 percent of the available grant funds in that fiscal year.

(ii) EXCEPTION.—The Administrator of FEMA may waive the limitation in clause (i) with respect to a grant recipient if the Administrator of FEMA determines that the recipient has an extraordinary need for a grant in an amount that exceeds the limit under clause (i).

(3) USE OF GRANT FUNDS.—Each entity receiving a grant under this subsection shall use the grant for 1 or more of the following purposes:

(A) To train firefighting personnel in—

(i) firefighting;

(ii) emergency medical services and other emergency response (including response to natural disasters, acts of terrorism, and other man-made disasters);

(iii) arson prevention and detection;

(iv) maritime firefighting; or

(v) the handling of hazardous materials.

(B) To train firefighting personnel to provide any of the training described under subparagraph (A).

(C) To fund the creation of rapid intervention teams to protect firefighting personnel at the scenes of fires and other emergencies.

(D) To certify—

(i) fire inspectors; and

(ii) building inspectors—

(I) whose responsibilities include fire safety inspections; and

(II) who are employed by or serving as volunteers with a fire department.

(E) To establish wellness and fitness programs for firefighting personnel to ensure that the firefighting personnel are able to carry out their duties as firefighters, including programs dedicated

to raising awareness of, and preventing, job-related mental health issues.

(F) To fund emergency medical services provided by fire departments and nonaffiliated EMS organizations.

(G) To acquire additional firefighting vehicles, including fire trucks and other apparatus.

(H) To acquire additional firefighting equipment, including equipment for—

(i) fighting fires with foam in remote areas without access to water; and

(ii) communications, monitoring, and responding to a natural disaster or act of terrorism or other man-made disaster, including the use of a weapon of mass destruction.

(I) To acquire personal protective equipment, including personal protective equipment—

(i) prescribed for firefighting personnel by the Occupational Safety and Health Administration of the Department of Labor; or

(ii) for responding to a natural disaster or act of terrorism or other man-made disaster, including the use of a weapon of mass destruction.

(J) To modify fire stations, fire training facilities, and other facilities to protect the health and safety of firefighting personnel.

(K) To educate the public about arson prevention and detection.

(L) To provide incentives for the recruitment and retention of volunteer firefighting personnel for volunteer firefighting departments and other firefighting departments that utilize volunteers.

(M) To provide specialized training to firefighters, paramedics, emergency medical service workers, and other first responders to recognize individuals who have mental illness and how to properly intervene with individuals with mental illness, including strategies for verbal de-escalation of crisis.

(N) To support such other activities, consistent with the purposes of this subsection, as the Administrator of FEMA determines appropriate.

(d) FIRE PREVENTION AND SAFETY GRANTS

(1) IN GENERAL.—For the purpose of assisting fire prevention programs and supporting firefighter health and safety research and development, the Administrator of FEMA may, on a competitive basis—

(A) award grants to fire departments;

(B) award grants to, or enter into contracts or cooperative agreements with, national, State, local, tribal, or nonprofit organizations that are not fire departments and that are recognized for their experience and expertise with respect to fire prevention or fire safety programs and activities and firefighter research and development programs, for the purpose of carrying out—

(i) fire prevention programs; and

(ii) research to improve firefighter health and life safety; and

(C) award grants to institutions of higher education, national fire service organizations, or national fire safety organizations to establish and operate fire safety research centers.

(2) MAXIMUM GRANT AMOUNT.—A grant awarded under this subsection may not exceed $1,500,000 for a fiscal year.

(3) USE OF GRANT FUNDS.—Each entity receiving a grant under this subsection shall use the grant for 1 or more of the following purposes:

(A) To enforce fire codes and promote compliance with fire safety standards.

(B) To fund fire prevention programs, including programs that educate the public about arson prevention and detection.

(C) To fund wildland fire prevention programs, including education, awareness, and mitigation programs that protect lives, property, and natural resources from fire in the wildland-urban interface.

(D) In the case of a grant awarded under paragraph (1)(C), to fund the establishment or operation of a fire safety research center for the purpose of significantly reducing the number of fire-related deaths and injuries among firefighters and the general public through research, development, and technology transfer activities.

(E) To support such other activities, consistent with the purposes of this subsection, as the Administrator of FEMA determines appropriate.

(4) LIMITATION.—None of the funds made available under this subsection may be provided to the Association of Community Organizations for Reform Now (ACORN) or any of its affiliates, subsidiaries, or allied organizations.

(e) APPLICATIONS FOR GRANTS.—

(1) IN GENERAL.—An entity seeking a grant under this section shall submit to the Administrator of FEMA an application in such form and in such manner as the Administrator of FEMA determines appropriate.

(2) ELEMENTS.—Each application submitted under paragraph (1) shall include the following:

(A) A description of the financial need of the applicant for the grant.

(B) An analysis of the costs and benefits, with respect to public safety, of the use for which a grant is requested.

(C) An agreement to provide information to the national fire incident reporting system for the period covered by the grant.

(D) A list of other sources of funding received by the applicant—

(i) for the same purpose for which the application for a grant under this section was submitted; or

(ii) from the Federal Government for other fire-related purposes.

(E) Such other information as the Administrator of FEMA determines appropriate.

(3) JOINT OR REGIONAL APPLICATIONS.—

(A) IN GENERAL.—Two or more entities may submit an application under paragraph (1) for a grant under this section to fund a joint program or initiative, including acquisition of shared equipment or vehicles.

(B) NONEXCLUSIVITY.—Applications under this paragraph may be submitted instead of or in addition to any other application submitted under paragraph (1).

(C) GUIDANCE.—The Administrator of FEMA shall—

(i) publish guidance on applying for and administering grants awarded for joint programs and initiatives described in subparagraph (A); and

(ii) encourage applicants to apply for grants for joint programs and initiatives described in subparagraph (A) as the Administrator of FEMA determines appropriate to achieve greater cost effectiveness and regional efficiency.

(f) PEER REVIEW OF GRANT APPLICATIONS.—

(1) IN GENERAL.—The Administrator of FEMA shall, after consultation with national fire service and emergency medical services organizations, appoint fire service personnel to conduct peer reviews of applications received under subsection (e)(1).

(2) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of title 5 shall not apply to activities carried out pursuant to this subsection.

(g) CONSIDERATIONS FOR GRANT AWARDS.—In awarding grants under this section, the Administrator of FEMA shall consider the following:

(1) The findings and recommendations of the peer reviews carried out under subsection (f).

(2) The degree to which an award will reduce deaths, injuries, and property damage by reducing the risks associated with fire-related and other hazards.

(3) The extent of the need of an applicant for a grant under this section and the need to protect the United States as a whole.

(4) The number of calls requesting or requiring a firefighting or emergency medical response received by an applicant.

(h) ALLOCATION OF GRANT AWARDS.—In awarding grants under this section, the Administrator of FEMA shall ensure that of the available grant funds in each fiscal year—

(1) not less than 25 percent is awarded under subsection (c) to career fire departments;

(2) not less than 25 percent is awarded under subsection (c) to volunteer fire departments;

(3) not less than 25 percent is awarded under subsection (c) to combination fire departments and fire departments using paid-on-call firefighting personnel;

(4) not less than 10 percent is available for open competition among career fire departments, volunteer fire departments, combination fire departments, and fire departments using paid-on-call firefighting personnel for grants awarded under subsection (c);

(5) not less than 10 percent is awarded under subsection (d); and

(6) not more than 2 percent is awarded under this section to non-affiliated EMS organizations described in subsection (c)(1)(B).

(i) ADDITIONAL REQUIREMENTS AND LIMITATIONS.—

(1) FUNDING FOR EMERGENCY MEDICAL SERVICES.—Not less than 3.5 percent of the available grant funds for a fiscal year shall be awarded under this section for purposes described in subsection (c)(3)(F).

(2) STATE FIRE TRAINING ACADEMIES.—

(A) MAXIMUM SHARE.—Not more than 3 percent of the available grant funds for a fiscal year may be awarded under subsection (c)(1)(C).

(B) MAXIMUM GRANT AMOUNT.—The Administrator of FEMA may not award a grant under subsection (c)(1)(C) to a State fire training academy in an amount that exceeds $1,000,000 in a fiscal year.

(3) AMOUNTS FOR PURCHASING FIREFIGHTING VEHICLES.—Not more than 25 percent of the available grant funds for a fiscal year may be used to assist grant recipients to purchase vehicles pursuant to subsection (c)(3)(G).

(j) FURTHER CONSIDERATIONS.—

(1) ASSISTANCE TO FIREFIGHTERS GRANTS TO FIRE DEPARTMENTS.—In considering applications for grants under subsection (c)(1)(A), the Administrator of FEMA shall consider—

(A) the extent to which the grant would enhance the daily operations of the applicant and the impact of the grant on the protection of lives and property; and

(B) a broad range of factors important to the applicant's ability to respond to fires and related hazards, such as the following:

(i) Population served.

(ii) Geographic response area.

(iii) Hazards vulnerability.

(iv) Call volume.

(v) Financial situation, including unemployment rate of the area being served.

(vi) Need for training or equipment.

(2) APPLICATIONS FROM NONAFFILIATED EMS ORGANIZATIONS.—In the case of an application submitted under subsection (e)(1) by a nonaffiliated EMS organization, the Administrator of FEMA shall consider the extent to which other sources of Federal funding are available to the applicant to provide the assistance requested in the application.

(3) FIRE PREVENTION AND SAFETY GRANTS TO CERTAIN ORGANIZATIONS THAT ARE NOT FIRE DEPARTMENTS.—In the case of applicants for grants under this section that are described in subsection (d)(1)(B), the Administrator of FEMA shall give priority to applicants that focus on

(A) prevention of injuries to high risk groups from fire; and

(B) research programs that demonstrate a potential to improve firefighter safety.

(4) GRANTS FOR FIRE SAFETY RESEARCH CENTERS.—

(A) CONSIDERATIONS.—In awarding grants under subsection (d)(1)(C), the Administrator of FEMA shall—

(i) select each grant recipient on—

(I) the demonstrated research and extension resources available to the recipient to carry out the research, development, and technology transfer activities;

(II) the capability of the recipient to provide leadership in making national contributions to fire safety;

(III) the recipient's ability to disseminate the results of fire safety research; and

(IV) the strategic plan the recipient proposes to carry out under the grant;

(ii) give special consideration in selecting recipients under clause (i) to an applicant for a grant that consists of a partnership between—

(I) a national fire service organization or a national fire safety organization; and

(II) an institution of higher education, including a minority-serving institution (as described in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)); and

(iii) consider the research needs identified and prioritized through the workshop required by subparagraph (B)(i).

(B) RESEARCH NEEDS.—

(i) WORKSHOP TO IDENTIFY NEEDS.—The Administrator of FEMA shall convene a workshop of the fire safety research community, fire service organizations, and other appropriate stakeholders to identify and prioritize fire safety research needs.

(ii) PUBLICATION OF RESULTS.—The Administrator of FEMA shall ensure that the results of the workshop are made available to the public.

(C) LIMITATIONS ON GRANTS FOR FIRE SAFETY RESEARCH CENTERS.—

(i) IN GENERAL.—The Administrator of FEMA may award grants under subsection (d) to establish not more than 3 fire safety research centers.

(ii) RECIPIENTS.—An institution of higher education, a national fire service organization, and a national fire safety organization may not directly receive a grant under subsection (d) for a fiscal year for more than 1 fire safety research center.

(5) AVOIDING DUPLICATION.—The Administrator of FEMA shall review lists submitted by applicants pursuant to subsection (e)(2)(D) and take such actions as the Administrator of FEMA considers necessary to prevent unnecessary duplication of grant awards.

(k) MATCHING AND MAINTENANCE OF EXPENDITURE REQUIREMENTS.—

(1) MATCHING REQUIREMENT FOR ASSISTANCE TO FIREFIGHTERS GRANTS.—

(A) IN GENERAL.—Except as provided in subparagraph (B), an applicant seeking a grant to carry out an activity under subsection (c) shall agree to make available non-Federal funds to carry out the activity in an amount equal to not less than 15 percent of the grant awarded to the applicant under subsection (c).

(B) EXCEPTION FOR ENTITIES SERVING SMALL COMMUNITIES.—In the case that an applicant seeking a grant to carry out an activity under subsection (c) serves a jurisdiction of—

(i) more than 20,000 residents but not more than 1,000,000 residents, the applicant shall agree to make available non-Federal funds in an amount equal to not less than 10 percent of the grant awarded to the applicant under subsection (c); and

(ii) 20,000 residents or fewer, the applicant shall agree to make available non-Federal funds in an amount equal to not less than 5 percent of the grant awarded to the applicant under subsection (c).

(2) MATCHING REQUIREMENT FOR FIRE PREVENTION AND SAFETY GRANTS.—

(A) IN GENERAL.—An applicant seeking a grant to carry out an activity under subsection (d) shall agree to make available non-Federal funds to carry out the activity in an amount equal to not less than 5 percent of the grant awarded to the applicant under subsection (d).

(B) MEANS OF MATCHING.—An applicant for a grant under subsection (d) may meet the matching requirement under subparagraph (A) through direct funding, funding of complementary activities, or the provision of staff, facilities, services, material, or equipment.

(3) MAINTENANCE OF EXPENDITURES.—An applicant seeking a grant under subsection (c) or (d) shall agree to maintain during the term of the grant the applicant's aggregate expenditures relating to the uses described in subsections (c)(3) and (d)(3) at not less than 80 percent of the average amount of the expenditures in the 2 fiscal years preceding the fiscal year in which the grant amounts are received.

(4) WAIVER OR REDUCTION OF REQUIREMENTS.—

(A) IN GENERAL.—Except as provided in subparagraph (C)(ii), the Administrator of FEMA may waive or reduce the requirements

of paragraphs (1), (2), and (3) in cases of demonstrated economic hardship.

(B) GUIDELINES.—

(i) IN GENERAL.—The Administrator of FEMA shall establish and publish guidelines for determining what constitutes economic hardship for purposes of this paragraph.

(ii) CONSULTATION.—In developing guidelines under clause (i), the Administrator of FEMA shall consult with individuals who are—

(I) recognized for expertise in firefighting, emergency medical services provided by fire services, or the economic affairs of State and local governments; and

(II) members of national fire service organizations or national organizations representing the interests of State and local governments.

(iii) CONSIDERATIONS.—In developing guidelines under clause (i), the Administrator of FEMA shall consider, with respect to relevant communities, the following:

(I) Changes in rates of unemployment from previous years.

(II) Whether the rates of unemployment of the relevant communities are currently exceeding and have consistently exceeded the annual national average rates of unemployment.

(III) Changes in percentages of individuals eligible to receive food stamps from previous years.

(IV) Such other factors as the Administrator of FEMA considers appropriate.

(C) CERTAIN APPLICANTS FOR FIRE PREVENTION AND SAFETY GRANTS NOT ELIGIBLE FOR WAIVER OR REDUCTION.—The authority under subparagraph (A) shall not apply with respect to a nonprofit organization that—

(i) is described in subsection (d)(1)(B); and

(ii) is not a fire department or emergency medical services organization.

(l) GRANT GUIDELINES.—

(1) ANNUAL PUBLICATION IN FEDERAL REGISTER.—For each fiscal year, prior to awarding grants under this section, the Administrator of FEMA shall publish in the Federal Register—

(A) guidelines that describe—

(i) the process for applying for grants under this section; and

(ii) the criteria that will be used for selecting grant recipients; and

(B) an explanation of any differences between the guidelines and the recommendations obtained under paragraph (2).

(2) ANNUAL MEETING TO OBTAIN RECOMMENDATIONS.—

(A) QUALIFIED MEMBERS.—For purposes of this paragraph, a qualified member of an organization is a member who—

(i) is recognized for expertise in firefighting or emergency medical services;

(ii) is not an employee of the Federal Government; and

(iii) in the case of a member of an emergency medical service organization, is a member of an organization that represents—

(I) providers of emergency medical services that are affiliated with fire departments; or

(II) nonaffiliated EMS providers.

(B) IN GENERAL.—For each fiscal year, the Administrator of FEMA shall convene a meeting of qualified members of national fire service organizations and, at the discretion of the Administrator of FEMA, qualified members of emergency medical service organizations to obtain recommendations regarding the following:

(i) Criteria for the awarding of grants under this section.

(ii) Administrative changes to the assistance program established under subsection (b).

(3) INAPPLICABILITY OF CHAPTER 5 OF TITLE 10.—Chapter 5 of title 10 shall not apply to activities carried out under this subsection.

(m) ACCOUNTING DETERMINATION.—Notwithstanding another law, for purposes of this section, equipment costs shall include all costs attributable to any design, purchase of components, assembly, manufacture, and transportation of equipment not otherwise commercially available.

(n) ELIGIBLE GRANTEE ON BEHALF OF ALASKA NATIVE VILLAGES.—The Alaska Village Initiatives, a non-profit organization incorporated in Alaska, shall be eligible to apply for and receive a grant or other assistance under this section on behalf of Alaska Native villages.

(o) TRAINING STANDARDS.—If an applicant for a grant under this section is applying for the grant to purchase training that does not meet or exceed any applicable national voluntary consensus standards, including those developed under section 20507 of this title, the applicant shall submit to the Administrator of FEMA an explanation of the reasons that the train-

ing proposed to be purchased will serve the needs of the applicant better than training that meets or exceeds the standards.

(p) ENSURING EFFECTIVE USE OF GRANTS.—

(1) AUDITS.—The Administrator of FEMA may audit a recipient of a grant awarded under this section to ensure that–

(A) the grant amounts are expended for the intended purposes; and

(B) the grant recipient complies with the requirements of subsection (k).

(2) PERFORMANCE ASSESSMENT.—

(A) IN GENERAL.—The Administrator of FEMA shall develop and implement a performance assessment system, including quantifiable performance metrics, to evaluate the extent to which grants awarded under this section are furthering the purposes of this section, including protecting the health and safety of the public and firefighting personnel against fire and fire-related hazards.

(B) CONSULTATION.—The Administrator of FEMA shall consult with fire service representatives and with the Comptroller General in developing the assessment system required by subparagraph (A).

(3) ANNUAL REPORTS TO ADMINISTRATOR OF FEMA.—Not less frequently than once each year during the term of a grant awarded under this section, the recipient of the grant shall submit to the Administrator of FEMA an annual report describing how the recipient used the grant amounts.

(q) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There is authorized to be appropriated to carry out this section for fiscal year 2023 an amount equal to the amount authorized for the previous fiscal year increased by the percentage by which—

(A) the Consumer Price Index (all items, United States city average) for the previous fiscal year; exceeds

(B) the Consumer Price Index for the fiscal year preceding the fiscal year described in subparagraph (A).

(2) ADMINISTRATIVE EXPENSES.—Of the amounts appropriated pursuant to paragraph (1) for a fiscal year, the Administrator of FEMA may use not more than 5 percent of the amounts for salaries and expenses and other administrative costs incurred by the Administrator of FEMA in the course of awarding grants and providing assistance under this section.

(3) CONGRESSIONALLY DIRECTED SPENDING NOT ALLOWED.—Consistent with the requirements in subsections (c)(1) and (d)(1) that grants under those subsections be awarded on a competitive basis, none of the funds appropriated pursuant to this subsection may be used for a congressionally directed spending item (as defined under the rules of the Senate and the House of Representatives).

(r) SUNSET OF AUTHORITIES.—The authority to award assistance and grants under this section shall expire on September 30, 2024.

§ 11378. Staffing for adequate fire and emergency response

(a) DEFINITION OF FIREFIGHTER.—In this section, the term ''firefighter'' has the meaning given the term ''employee in fire protection activities'' under section 3 of the Fair Labor Standards Act of 1938 (29 U.S.C. 203).

(b) EXPANDED AUTHORITY TO MAKE GRANTS.—

(1) HIRING GRANTS.—

(A) PURPOSE.—The Administrator of FEMA shall make grants directly to career fire departments, combination fire departments, and volunteer fire departments, in consultation with the chief executive of the State in which the applicant is located, for the purpose of increasing the number of firefighters to help communities meet industry minimum standards and attain 24-hour staffing to provide adequate protection from fire and fire-related hazards, and to fulfill traditional missions of fire departments that antedate the creation of the Department.

(B) TERM AND USE.—Grants made under this paragraph shall be for 3 years and be used for programs to hire new, additional firefighters or to change the status of part-time or paid-on-call (as defined in section 11377 of this title) firefighters to full-time firefighters.

(C) PREFERENTIAL CONSIDERATION.—In awarding grants under this subsection, the Administrator of FEMA may give preferential consideration to applications that involve a non-Federal contribution exceeding the minimums under subparagraph (E).

(D) TECHNICAL ASSISTANCE.—The Administrator of FEMA may provide technical assistance to States, units of local government, Indian tribal governments, and other public entities in furtherance of the purposes of this section.

(E) MAXIMUM GRANT AMOUNT.—The portion of the costs of hiring firefighters provided by a grant under this paragraph may not exceed—

(i) 75 percent in the 1st year of the grant;

(ii) 75 percent in the 2d year of the grant; and

(iii) 35 percent in the 3d year of the grant.

(F) VOLUNTEER ACTIVITIES ALLOWED.—Notwithstanding another law, a firefighter hired with funds provided under this subsection shall not be discriminated against for, or be prohibited from, engaging in volunteer activities in another jurisdiction during off-duty hours.

(G) AWARD ON COMPETITIVE BASIS.—All grants made pursuant to this subsection shall be awarded on a competitive basis through a neutral peer review process.

(H) SET ASIDE FOR DEPARTMENT WITH A MAJORITY OF VOLUNTEER OR ALL-VOLUNTEER PERSONNEL.—At the beginning of the fiscal year, the Administrator of FEMA shall set aside 10 percent of the funds appropriated for carrying out this paragraph for departments with majority volunteer or all-volunteer personnel. After awards have been made, if less than 10 percent of the funds appropriated for carrying out this paragraph are not awarded to departments with a majority of volunteer or all-volunteer personnel, the Administrator of FEMA shall transfer from funds appropriated for carrying out this paragraph to funds available for carrying out paragraph (2) an amount equal to the difference between the amount that is provided to the fire departments and 10 percent.

(2) RECRUITMENT AND RETENTION GRANTS.—In addition to amounts transferred under paragraph (1)(H), the Administrator of FEMA shall direct at least 10 percent of the total amount of funds appropriated pursuant to this section annually to a competitive grant program for the recruitment and retention of volunteer firefighters who are involved with or trained in the operations of firefighting and emergency response. Eligible entities shall include volunteer or combination fire departments, and national, State, local, or tribal organizations that represent the interests of volunteer firefighters.

(c) APPLICATIONS.—

(1) APPROVED APPLICATION REQUIRED.—No grant may be made under this section unless an application has been submitted to, and approved by, the Administrator of FEMA.

(2) REQUIRED FORM AND INFORMATION.—An application for a grant under this section shall be submitted in such form, and contain such information, as the Administrator of FEMA may prescribe.

(3) CONTENTS.—At a minimum, each application for a grant under this section shall—

(A) explain the applicant's inability to address the need without Federal assistance;

(B) in the case of a grant under subsection (b)(1), explain how the applicant plans to meet the requirements of subsection (b)(1)(F);

(C) specify long-term plans for retaining firefighters following the conclusion of Federal support provided under this section; and

(D) provide assurances that the applicant will, to the extent practicable, seek, recruit, and hire members of racial and ethnic minority groups and women in order to increase their ranks within firefighting.

(d) REQUIREMENTS AND ALLOWANCES FOR USE OF FUNDS.—

(1) FUNDS DO NOT SUPPLANT OTHER FUNDS.—Funds made available under this section to fire departments for salaries and benefits to hire new, additional firefighters shall not be used to supplant State or local funds, or, in the case of Indian tribal governments, funds supplied by the Bureau of Indian Affairs, but shall be used to increase the amount of funds that would, in the absence of Federal funds received under this section, be made available from State or local sources, or in the case of Indian tribal governments, from funds supplied by the Bureau of Indian Affairs.

(2) MINIMUM REQUIRED BUDGET OF RECIPIENT FOR FIRE-RELATED PROGRAMS AND EMERGENCY RESPONSE.—No grant shall be awarded pursuant to this section to a municipality or other recipient whose annual budget at the time of the application for fire-related programs and emergency response has been reduced below 80 percent of the average funding level in the 3 years prior to the date of the application for the grant.

(3) USE FOR NON-FEDERAL SHARE OF COST OF PROGRAMS OR PROJECTS.—Funds appropriated by Congress for the activities of an agency of an Indian tribal government or the Bureau of Indian Affairs performing firefighting functions on Indian lands may be used to provide the non-Federal share of the cost of programs or projects funded under this section.

(4) MAXIMUM PROVIDED FOR HIRING FIREFIGHTERS.—The amount of funding provided under this section to a recipient fire department for hiring a firefighter in a fiscal year may not exceed—

(A) in the 1st year of the grant, 75 percent of the usual annual cost of a 1st-year firefighter in that department at the time the grant application was submitted;

(B) in the 2d year of the grant, 75 percent of the usual annual cost of a 1st-year firefighter in that department at the time the grant application was submitted; and

(C) in the 3d year of the grant, 35 percent of the usual annual cost of a 1st-year firefighter in that department at the time the grant application was submitted.

(e) WAIVERS.—

(1) IN GENERAL.—In a case of demonstrated economic hardship, the Administrator of FEMA may—

(A) waive the requirements of subsection (d)(1); or

(B) waive or reduce the requirements in subsection (b)(1)(E) or paragraph (2) or (4) of subsection (d).

(2) GUIDELINES.—

(A) DEVELOPMENT AND PUBLICATION.—The Administrator of FEMA shall develop and publish guidelines for determining what constitutes economic hardship for purposes of paragraph (1).

(B) CONSULTATION.—In developing guidelines under subparagraph (A), the Administrator of FEMA shall consult with individuals who are—

(i) recognized for expertise in firefighting, emergency medical services provided by fire services, or the economic affairs of State and local governments; and

(ii) members of national fire service organizations or national organizations representing the interests of State and local governments.

(C) CONSIDERATIONS.—In developing guidelines under subparagraph (A), the Administrator of FEMA shall consider, with respect to relevant communities, the following:

(i) Changes in rates of unemployment from previous years.

(ii) Whether the rates of unemployment of the relevant communities are currently exceeding, and have consistently exceeded, the annual national average rates of unemployment.

(iii) Changes in percentages of individuals eligible to receive food stamps from previous years.

(iv) Such other factors as the Administrator of FEMA considers appropriate.

(f) PERFORMANCE EVALUATION.—

(1) ESTABLISHMENT.—The Administrator of FEMA shall establish a performance assessment system, including quantifiable performance metrics, to evaluate the extent to which grants awarded under this section are furthering the purposes of this section.

(2) SUBMITTAL OF INFORMATION.—The Administrator of FEMA may require a grant recipient to submit any information the Administrator of FEMA considers reasonably necessary to evaluate the program.

(g) REVOCATION OR SUSPENSION OF FUNDING.—If the Administrator of FEMA determines that a grant recipient under this section is not in substantial compliance with the terms and requirements of an approved grant application submitted under this section, the Administrator of FEMA may revoke or suspend funding of that grant, in whole or in part.

(h) ACCESS TO DOCUMENTS.—

(1) ADMINISTRATOR OF FEMA.—The Administrator of FEMA shall have access for the purpose of audit and examination to any pertinent books, documents, papers, or records of a grant recipient under this section and to the pertinent books, documents, papers, or records of State and local governments, persons, businesses, and other entities that are involved in programs, projects, or activities for which assistance is provided under this section.

(2) COMPTROLLER GENERAL.—Paragraph (1) shall apply with respect to audits and examinations conducted by the Comptroller General or by an authorized representative of the Comptroller General.

(i) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There is authorized to be appropriated for the purposes of carrying out this section for fiscal year 2023 an amount equal to the amount authorized for the previous fiscal year increased by the percentage by which—

(A) the Consumer Price Index (all items, United States city average) for the previous fiscal year, exceeds

(B) the Consumer Price Index for the fiscal year preceding the fiscal year described in subparagraph (A).

(2) ADMINISTRATIVE EXPENSES.—Of the amounts appropriated pursuant to paragraph (1) for a fiscal year, the Administrator of FEMA may use not more than 5 percent of the amounts for salaries and expenses and other administrative costs incurred by the Administrator of FEMA to make grants and provide assistance under this section.

(3) CONGRESSIONALLY DIRECTED SPENDING NOT ALLOWED.—Consistent with the requirement in subsection (a) that grants under this section be awarded on a competitive basis, none of the funds appropriated pursuant to this subsection may be used for a congressionally direct spending item (as defined under the rules of the Senate and the House of Representatives).

(j) SUNSET OF AUTHORITIES.—The authority to award assistance and grants under this section shall expire on September 30, 2024.

§ 11379. Training for administration, and oversight and monitoring, of grants programs

(a) TRAINING ON ADMINISTRATION OF FIRE GRANT PROGRAMS.—

(1) DEVELOPMENT OF TRAINING COURSE.—The Administrator of FEMA, acting through the Administrator, may develop and make widely available an electronic, online training course for members of the fire and emergency response community on matters relating to the administration of grants under sections 11377 and 11378 of this title.

(2) REQUIREMENTS.—The Administrator of FEMA shall ensure that training developed and made available under paragraph (1) is—

(A) tailored to the financial and time constraints of members of the fire and emergency response community; and

(B) accessible to all individuals in the career, combination, paid-on-call, and volunteer fire and emergency response community.

(b) GRANT MONITORING AND OVERSIGHT FRAMEWORK.—

(1) FRAMEWORK.—The Administrator of FEMA shall develop and implement a grant monitoring and oversight framework to mitigate and minimize risks of fraud, waste, abuse, and mismanagement relating to the grants programs under sections 11377 and 11378 of this title.

(2) ELEMENTS.—The framework required under paragraph (1) shall include the following:

(A) Developing standardized guidance and training for all participants in the grant programs described in paragraph (1).

(B) Conducting regular risk assessments.

(C) Conducting desk reviews and site visits.

(D) Enforcement actions to recoup potential questionable costs of grant recipients.

(E) Such other oversight and monitoring tools as the Administrator of FEMA considers necessary to mitigate and minimize fraud, waste, abuse, and mismanagement relating to the grant programs described in paragraph (1).

§ 11380. Surplus and excess Federal equipment

The Administrator shall make publicly available, including through the Internet, information on procedures for acquiring surplus and excess equipment or property that may be useful to State and local fire, emergency, and hazardous material handling service providers.

§ 11381. Cooperative agreements with Federal facilities

The Administrator shall make publicly available, including through the Internet, information on procedures for establishing cooperative agreements

between State and local fire and emergency services and Federal facilities in their region relating to the provision of fire and emergency services.

§ 11382. Burn research

(a) OFFICE.—The Administrator of FEMA shall establish an office in the Federal Emergency Management Agency to establish specific criteria of grant recipients and to administer grants under this section.

(b) SAFETY ORGANIZATION GRANTS.—The Administrator of FEMA may make grants, on a competitive basis, to safety organizations that have experience in conducting burn safety programs for the purpose of assisting those organizations in conducting burn prevention programs or augmenting existing burn prevention programs.

(c) HOSPITAL GRANTS.—The Administrator of FEMA may make grants, on a competitive basis, to hospitals that serve as regional burn centers to conduct acute burn care research.

(d) OTHER GRANTS.—The Administrator of FEMA may make grants, on a competitive basis, to governmental and nongovernmental entities to provide after-burn treatment and counseling to individuals that are burn victims.

§ 11383. Removal of civil liability barriers that discourage the donation of fire equipment to volunteer fire companies

(a) DEFINITIONS.—In this section:

(1) AUTHORIZED TECHNICIAN.—The term ''authorized technician'' means a technician who has been certified by the manufacturer of fire control or fire rescue equipment to inspect the equipment. The authorized technician need not be employed by the State or local agency administering the distribution of the fire control or fire rescue equipment.

(2) FIRE CONTROL OR RESCUE EQUIPMENT.—The term ''fire control or fire rescue equipment'' includes any fire vehicle, firefighting tool, communications equipment, protective gear, fire hose, or breathing apparatus.

(3) PERSON.—The term ''person'' includes a governmental or other entity.

(4) QUALIFIED FIRE CONTROL OR RESCUE EQUIPMENT.—The term ''qualified fire control or rescue equipment'' means fire control or fire rescue equipment that has been recertified by an authorized technician as meeting the manufacturer's specifications.

(5) STATE.—The term ''State'' includes the States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the Virgin Islands, any other territory (including a pos-

session) of the United States, and a political subdivision of a State or territory.

(6) VOLUNTEER FIRE COMPANY.—The term ''volunteer fire company'' means an association of individuals who provide fire protection and other emergency services, where at least 30 percent of the individuals receive little or no compensation compared with an entry level full-time paid individual in that association or in the nearest association with an entry level full-time paid individual.

(b) LIABILITY PROTECTION.—A person that donates qualified fire control or rescue equipment to a volunteer fire company shall not be liable for civil damages under any State or Federal law for personal injuries, property damage or loss, or death caused by the equipment after the donation.

(c) EXCEPTIONS.—Subsection (b) does not apply to a person if—

(1) the person's act or omission causing the injury, damage, loss, or death constitutes gross negligence or intentional misconduct;

(2) the person is the manufacturer of the qualified fire control or rescue equipment; or

(3) the person or agency modified or altered the equipment after it had been recertified by an authorized technician as meeting the manufacturer's specifications.

(d) PREEMPTION.—This section—

(1) preempts the laws of a State to the extent that the laws are inconsistent with this section; except that

(2) notwithstanding subsection (c) shall not preempt a State law that provides additional protection from liability for a person that donates fire control or fire rescue equipment to a volunteer fire company.

§ 11384. Encouraging adoption of standards for firefighter health and safety

The Administrator shall promote adoption by fire services of national voluntary consensus standards for firefighter health and safety, including standards for firefighter operations, training, staffing, and fitness, by—

(1) educating fire services about the standards;

(2) encouraging the adoption of the standards at all levels of government; and

(3) making recommendations on other ways in which the Federal Government can promote the adoption of the standards by fire services.

§ 11385. Investigation authorities

(a) DEFINITION OF MAJOR FIRE.—For purposes of this section, the term ''major fire'' has the meaning given the term under regulations to be issued by the Administrator.

(b) FIRE SAFETY INVESTIGATION OF MAJOR FIRE.—In the case of a major fire, the Administrator may send incident investigators, which may include safety specialists, fire protection engineers, codes and standards experts, researchers, and fire training specialists, to the site of the fire to conduct a fire safety investigation as described in subsection (c).

(c) REQUIREMENTS OF INVESTIGATION.—A fire safety investigation conducted under this section—

(1) shall be conducted in coordination and cooperation with appropriate Federal, State, local, Tribal, and territorial authorities, including Federal agencies that are authorized to investigate any fire; and

(2) shall examine the previously determined cause and origin of the fire and assess broader systematic matters to include use of codes and standards, demographics, structural characteristics, smoke and fire dynamics (movement) during the event, and costs of associated injuries and deaths.

(d) REPORT.—

(1) IN GENERAL.—Subject to paragraph (2), on concluding a fire safety investigation under this section, the Administrator shall—

(A) issue a public report to the appropriate Federal, State, local, Tribal, and territorial authorities on the findings of the investigation; or

(B) collaborate with another investigating Federal, State, local, Tribal, or territorial agency on the report of that agency.

(2) CONTENTS.—Each public report issued under paragraph (1) shall include recommendations on—

(A) any other buildings with similar characteristics that may bear similar fire risks;

(B) improving tactical response to similar fires;

(C) improving civilian safety practices;

(D) assessing the costs and benefits to the community of adding fire safety features; and

(E) how to mitigate the causes of the fire.

(3) EXCEPTION.—If the Administrator, in consultation with appropriate Federal, State, local, Tribal, and territorial authorities, determines that issuing a report under paragraph (1) would have a negative impact on a potential or ongoing criminal investigation, the Administrator is not required to issue the report.

(e) ADDITIONAL FIRE SAFETY INVESTIGATION.—In addition to a fire safety investigation conducted pursuant to subsection (b), provided doing so would not have a negative impact on a potential or ongoing criminal investigation, the Administrator may send fire investigators to conduct a fire

safety investigation at the site of any fire with unusual or remarkable context that results in losses less severe than those occurring as a result of a major fire, in coordination and cooperation with the appropriate Federal, State, local, Tribal, and territorial authorities, including Federal agencies that are authorized to investigate the fire.

(f) CONSTRUCTION.—Nothing in this section shall be construed to—

(1) affect or otherwise diminish the authorities or the mandates vested in other Federal agencies;

(2) grant the Administrator authority to investigate a major fire for the purpose of an enforcement action or criminal prosecution; or

(3) require the Administrator to send investigators or issue a report for a major fire when the Administrator, in coordination and cooperation with the appropriate Federal, State, local, Tribal, and territorial authorities, determines that it may compromise a potential or ongoing criminal investigation.

§ 11386. Administrative provisions

(a) ASSISTANCE TO ADMINISTRATOR.—Each department, agency, and instrumentality of the executive branch of the Federal Government and each independent regulatory agency of the United States shall furnish to the Administrator, on request, on a reimbursable basis or otherwise, such assistance as the Administrator considers necessary to carry out the Administrator's functions and duties pursuant to this subchapter, including transfer of personnel with their consent and without prejudice to their position and ratings.

(b) POWERS OF ADMINISTRATOR.—With respect to this subchapter, the Administrator may—

(1) enter into, without regard to section 6101 of title 41, such contracts, grants, leases, cooperative agreements, or other transactions as may be necessary to carry out this subchapter;

(2) accept gifts and voluntary and uncompensated services, notwithstanding section 1342 of title 31;

(3) purchase, lease, or otherwise acquire, own, hold, improve, use, or deal in and with any property (real, personal, or mixed, tangible or intangible), or interest in property, wherever situated, and sell, convey, mortgage, pledge, lease, exchange, or otherwise dispose of property and assets;

(4) procure temporary and intermittent services to the same extent as is authorized under section 3109 of title 5, but at rates not to exceed the daily equivalent of the maximum annual rate of basic pay then in effect for grade GS–15 of the General Schedule (5 U.S.C. 5332(a)) for qualified experts; and

(5) establish such rules, regulations, and procedures as are necessary to carry out this subchapter.

(c) AUDIT.—The Administrator of FEMA and the Comptroller Genera, or any of their duly authorized representatives, shall have access to any books, documents, papers, and records of the recipients of contracts, grants, or other forms of assistance that are pertinent to its activities under this subchapter for the purpose of audit or to determine if a proposed activity is in the public interest.

(d) INVENTIONS AND DISCOVERIES.—All property rights with respect to inventions and discoveries, which are made in the course of or under contract with a government agency pursuant to this subchapter, shall be subject to the basic policies set forth in the President's Statement of Government Patent Policy issued August 23, 1971, or such revisions of that statement of the policy as may subsequently be promulgated and published in the Federal Register.

(e) COORDINATION.—

(1) USE OF EXISTING RESOURCES.—To the extent practicable, the Administrator shall use existing programs, data, information, and facilities already available in other Federal Government departments and agencies and, where appropriate, existing research organizations, centers, and universities.

(2) COORDINATION OF FIRE PREVENTION AND CONTROL PROGRAMS.—The Administrator shall provide liaison at an appropriate organizational level to ensure coordination of the activities of the Administrator with Federal, State, and local government agencies and departments and nongovernmental organizations concerned with any matter relating to programs of fire prevention and control.

(3) COORDINATION OF EMERGENCY MEDICAL SERVICES PROGRAMS.—The Administrator shall provide liaison at an appropriate organizational level to ensure coordination of the activities of the Administrator relating to emergency medical services provided by fire service-based systems with Federal, State, and local government agencies and departments and nongovernmental organizations so concerned, as well as those entities concerned with emergency medical services generally.

(f) ENHANCEMENT OF SCIENCE AND MATHEMATICS PROGRAMS.—

(1) DEFINITIONS.—In this section:

(A) EDUCATIONALLY USEFUL FEDERAL EQUIPMENT.—The term ''educationally useful Federal equipment'' means computers and related peripheral tools and research equipment that is appropriate for use in schools.

(B) SCHOOL.—The term ''school'' means a public or private educational institution that serves any of the grades of kindergarten through grade 12.

(2) REPORTS.—Not later than 1 year after November 20, 1997, and annually thereafter, the Administrator shall prepare and submit to the President a report that describes donations of educationally useful Federal equipment to schools to enhance the science and mathematics programs of those schools made during the period covered by the report. The President shall submit the report to Congress at the same time as the President submits a budget request to Congress under section 1105(a) of title 31.

§ 11387. Reports to Congress and the President

The Administrator of FEMA shall report to Congress and the President not later than 90 calendar days following the year ending September 30, 1980, and similarly each year thereafter on all activities relating to fire prevention and control, and all measures taken to implement and carry out this subchapter during the preceding calendar year. The report shall include—

(1) a thorough appraisal, including statistical analysis, estimates, and long-term projections of the human and economic losses due to fire;

(2) a survey and summary, in such detail as is considered advisable, of the research and technology program undertaken or sponsored pursuant to this subchapter;

(3) a summary of the activities of the Academy for the preceding 12 months, including—

(A) an explanation of the curriculum of study;

(B) a description of the standards of admission and performance;

(C) the criteria for the awarding of degrees and certificates; and

(D) a statistical compilation of the number of students attending the Academy and receiving degrees or certificates;

(4) a summary of the activities undertaken to assist the Nation's fire services;

(5) a summary of the public education programs undertaken;

(6) an analysis of the extent of participation in preparing and submitting Fire Safety Effectiveness Statements;

(7) a summary of outstanding problems confronting the administration of this subchapter, in order of priority;

(8) such recommendations for additional legislation as are considered necessary or appropriate; and

(9) a summary of reviews, evaluations, and suggested improvements in State and local fire prevention and building codes, fire services, and relevant Federal or private codes, regulations, and fire services.

§ 11388. Authorization of appropriations

(a) IN GENERAL.—Except as otherwise specifically provided with respect to the payment of claims under section 11360 of this title, there is authorized to be appropriated to carry out the purposes of this subchapter $76,490,890 for fiscal year 2023, of which $2,753,672 shall be used to carry out section 11357(f) of this title.

(b) NATIONAL EMERGENCY TRAINING CENTER SITE ADMINISTRATION.—Of the amounts referred to in subsection (a), not more than $4,150,000 is authorized to be appropriated for each fiscal year for National Emergency Training Center site administration.

Subchapter III—Global catastrophic risk management

§ 11401. Definitions.—

In this subchapter:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Federal Emergency Management Agency.

(2) BASIC NEED.—The term ''basic need''—

(A) means any good, service, or activity necessary to protect the health, safety, and general welfare of the civilian population of the United States; and

(B) includes—

(i) food;

(ii) water;

(iii) shelter;

(iv) basic communication services;

(v) basic sanitation and health services; and

(vi) public safety.

(3) CATASTROPHIC INCIDENT.—The term ''catastrophic incident''—

(A) means any natural or man-made disaster that results in extraordinary levels of casualties or damage, mass evacuations, or disruption severely affecting the population, infrastructure, environment, economy, national morale, or government functions in an area; and

(B) may include an incident—

(i) with a sustained national impact over a prolonged period of time;

(ii) that may rapidly exceed resources available to State and local government and private sector authorities in the impacted area; or

(iii) that may significantly interrupt governmental operations and emergency services to such an extent that national security could be threatened.

(4) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given such term insection 1016(e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c(e)).

(5) EXISTENTIAL RISK.—The term ''existential risk'' means the potential for an outcome that would result in human extinction.

(6) GLOBAL CATASTROPHIC RISK.—The term ''global catastrophic risk'' means the risk of events or incidents consequential enough to significantly harm or set back human civilization at the global scale.

(7) GLOBAL CATASTROPHIC AND EXISTENTIAL THREATS.—The term ''global catastrophic and existential threats'' means threats that with varying likelihood may produce consequences severe enough to result in systemic failure or destruction of critical infrastructure or significant harm to human civilization. Examples of global catastrophic and existential threats include severe global pandemics, nuclear war, asteroid and comet impacts, supervolcanoes, sudden and severe changes to the climate, and intentional or accidental threats arising from the use and development of emerging technologies.

(8) INDIAN TRIBAL GOVERNMENT.—The term ''Indian Tribal government'' has the meaning given the term ''Indian tribal government'' insection 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(9) LOCAL GOVERNMENT.—The term ''local government'' has the meaning given the term in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(10) NATIONAL EXERCISE PROGRAM.—The term ''national exercise program'' means activities carried out to test and evaluate the national preparedness goal and related plans and strategies as described insection 20508(b) of this title.

(11) STATE.—The term ''State'' has the meaning given the term in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122)

§ 11402. Assessment of global catastrophic risk

(a) IN GENERAL.—The Secretary and the Administrator shall coordinate an assessment of global catastrophic risk.

(b) COORDINATION.—When coordinating the assessment under subsection (a), the Secretary and the Administrator shall coordinate with senior designees of—

(1) the Assistant to the President for National Security Affairs;

(2) the Director of the Office of Science and Technology Policy;

(3) the Secretary of State and the Under Secretary of State for Arms Control and International Security;

(4) the Attorney General and the Director of the Federal Bureau of Investigation;

(5) the Secretary of Energy, the Under Secretary of Energy for Nuclear Security, and the Director of Science;

(6) the Secretary of Health and Human Services, the Assistant Secretary for Preparedness and Response, and the Assistant Secretary of Global Affairs;

(7) the Secretary of Commerce, the Under Secretary of Commerce for Oceans and Atmosphere, and the Under Secretary of Commerce for Standards and Technology;

(8) the Secretary of the Interior and the Director of the United States Geological Survey;

(9) the Administrator of the Environmental Protection Agency and the Assistant Administrator for Water;

(10) the Administrator of the National Aeronautics and Space Administration;

(11) the Director of the National Science Foundation;

(12) the Secretary of the Treasury;

(13) the Secretary of Defense, the Assistant Secretary of the Army for Civil Works, and the Chief of Engineers and Commanding General of the Army Corps of Engineers;

(14) the Chairman of the Joint Chiefs of Staff;

(15) the Administrator of the United States Agency for International Development;

(16) the Secretary of Transportation; and

(17) other stakeholders the Secretary and the Administrator determine appropriate.

§ 11403. Report

(a) IN GENERAL.—Not later than December 23, 2023, and every 10 years thereafter, the Secretary, in coordination with the Administrator, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services of the Senate and the Committee on Transportation and Infrastructure and the Committee on Armed Services of the House of Representatives a report containing a detailed assessment,

based on the input and coordination required undersection 10742 of this title, of global catastrophic and existential risk.

(b) MATTERS COVERED.—Each report required under subsection (a) shall include—

(1) expert estimates of cumulative global catastrophic and existential risk in the next 30 years, including separate estimates for the likelihood of occurrence and potential consequences;

(2) expert-informed analyses of the risk of the most concerning specific global catastrophic and existential threats, including separate estimates, where reasonably feasible and credible, of each threat for its likelihood of occurrence and its potential consequences, as well as associated uncertainties;

(3) a comprehensive list of potential catastrophic or existential threats, including even those that may have very low likelihood;

(4) technical assessments and lay explanations of the analyzed global catastrophic and existential risks, including their qualitative character and key factors affecting their likelihood of occurrence and potential consequences;

(5) an explanation of any factors that limit the ability of the Secretary to assess the risk both cumulatively and for particular threats, and how those limitations may be overcome through future research or with additional resources, programs, or authorities;

(6) a forecast of if and why global catastrophic and existential risk is likely to increase or decrease significantly in the next 10 years, both qualitatively and quantitatively, as well as a description of associated uncertainties;

(7) proposals for how the Federal Government may more adequately assess global catastrophic and existential risk on an ongoing basis in future years;

(8) recommendations for legislative actions, as appropriate, to support the evaluation and assessment of global catastrophic and existential risk; and

(9) other matters considered appropriate by the Secretary, in coordination with the Administrator, and based on the input and coordination required undersection 11402 of this title.

(c) CONSULTATION REQUIREMENT.—In producing the report required under subsection (a), the Secretary shall—

(1) regularly consult with experts on severe global pandemics, nuclear war, asteroid and comet impacts, supervolcanoes, sudden and severe changes to the climate, and intentional or accidental threats arising from the use and development of emerging technologies; and

(2) share information gained through the consultation required under paragraph (1) with relevant Federal partners listed insection 11402(b) of this title.

11404. Enhanced catastrophic incident annex

(a) IN GENERAL.—The Secretary, in coordination with the Administrator and the Federal partners listed insection 11402(b) of this title, shall supplement each Federal Interagency Operational Plan to include an annex containing a strategy to ensure the health, safety, and general welfare of the civilian population affected by catastrophic incidents by—

(1) providing for the basic needs of the civilian population of the United States that is impacted by catastrophic incidents in the United States;

(2) coordinating response efforts with State, local, and Indian Tribal governments, the private sector, and nonprofit relief organizations;

(3) promoting personal and local readiness and non-reliance on government relief during periods of heightened tension or after catastrophic incidents; and

(4) developing international partnerships with allied nations for the provision of relief services and goods.

(b) ELEMENTS OF STRATEGY.—The strategy required under subsection (a) shall include a description of—

(1) actions the Federal Government should take to ensure the basic needs of the civilian population of the United States in a catastrophic incident are met;

(2) how the Federal Government should coordinate with non-Federal entities to multiply resources and enhance relief capabilities, including—

(A) State and local governments;

(B) Indian Tribal governments;

(C) State disaster relief agencies;

(D) State and local disaster relief managers;

(E) State National Guards;

(F) law enforcement and first response entities; and

(G) nonprofit relief services;

(3) actions the Federal Government should take to enhance individual resiliency to the effects of a catastrophic incident, which actions shall include—

(A) readiness alerts to the public during periods of elevated threat;

(B) efforts to enhance domestic supply and availability of critical goods and basic necessities; and

(C) information campaigns to ensure the public is aware of response plans and services that will be activated when necessary;

(4) efforts the Federal Government should undertake and agreements the Federal Government should seek with international allies to enhance the readiness of the United States to provide for the general welfare;

(5) how the strategy will be implemented should multiple levels of critical infrastructure be destroyed or taken offline entirely for an extended period of time; and

(6) the authorities the Federal Government should implicate in responding to a catastrophic incident.

(c) ASSUMPTIONS.—In designing the strategy under subsection (a), the Secretary, in coordination with the Administrator and the Federal partners listed insection 11402(b) of this title, shall account for certain factors to make the strategy operationally viable, including the assumption that—

(1) multiple levels of critical infrastructure have been taken offline or destroyed by catastrophic incidents or the effects of catastrophic incidents;

(2) impacted sectors may include—

(A) the transportation sector;

(B) the communication sector;

(C) the energy sector;

(D) the healthcare and public health sector; and

(E) the water and wastewater sector;

(3) State, local, Indian Tribal, and territorial governments have been equally affected or made largely inoperable by catastrophic incidents or the effects of catastrophic incidents;

(4) the emergency has exceeded the response capabilities of State, local, and Indian Tribal governments under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) and other relevant disaster response laws; and

(5) the United States military is sufficiently engaged in armed or cyber conflict with State or non-State adversaries, or is otherwise unable to augment domestic response capabilities in a significant manner due to a catastrophic incident.(.)

§ 11405. Rules of construction

(a) ADMINISTRATOR.—Nothing in this subchapter shall be construed to supersede the civilian emergency management authority of the Administrator under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) or subtitle II (except section 20525) of this title.

(b) SECRETARY.—Nothing in this subchapter shall be construed as providing new authority to the Secretary, except to coordinate and facilitate the development of the assessments and reports required pursuant to this subchapter.

Chapter 115—Transportation Security Administration

Subchapter I—General

§ 11501. Functions

(a) FUNCTIONS.—The Administrator of the Transportation Security Administration (in this chapter referred to as the ''Administrator''), is responsible for security in all modes of transportation, including—

(1) carrying out chapter 409 of this title and related research and development activities; and

(2) assuming security responsibilities over other modes of transportation that are exercised by the Department.

(b) SCREENING OPERATIONS.—The Administrator shall—

(1) be responsible for day-to-day Federal security screening operations for passenger air transportation and intrastate air transportation under sections 40911 and 40955 of this title;

(2) develop standards for the hiring and retention of security screening personnel;

(3) train and test security screening personnel; and

(4) be responsible for hiring and training personnel to provide security screening at all airports in the United States where screening is required under section 40911 of this title, in consultation with the Secretary of Transportation and the heads of other appropriate Federal agencies and departments.

(c) ADDITIONAL DUTIES AND POWERS.—In addition to carrying out the functions specified in subsections (a) and (b), the Administrator shall—

(1) receive, assess, and distribute intelligence information related to transportation security;

(2) assess threats to transportation;

(3) develop policies, strategies, and plans for dealing with threats to transportation security;

(4) make other plans related to transportation security, including coordinating countermeasures with appropriate departments, agencies, and instrumentalities of the United States Government;

(5) serve as the primary liaison for transportation security to the intelligence and law enforcement communities;

(6) on a day-to-day basis, manage and provide operational guidance to the field security resources of the Administration, including Federal Security Directors as provided by section 40953 of this title;

(7) enforce security-related regulations and requirements;

(8) identify and undertake research and development activities necessary to enhance transportation security;

(9) inspect, maintain, and test security facilities, equipment, and systems;

(10) ensure the adequacy of security measures for the transportation of cargo;

(11) oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities;

(12) require background checks for airport security screening personnel, individuals with access to secure areas of airports, and other transportation security personnel;

(13) work in conjunction with the Administrator of the Federal Aviation Administration with respect to actions or activities that may affect aviation safety or air carrier operations;

(14) maintain a National Deployment Office as required under section 10310(f) of this title;

(15) work with the International Civil Aviation Organization and appropriate aeronautic authorities of foreign governments under section 40917 of this title, to address security concerns on passenger flights by foreign air carriers in foreign air transportation; and

(16) carry out other duties, and exercise other powers, relating to transportation security the Administrator considers appropriate, to the extent authorized by law.

§ 11502. National emergency responsibilities

(a) IN GENERAL.—Subject to the direction and control of the Secretary, the Administrator, during a national emergency, has the following responsibilities:

(1) To coordinate domestic transportation, including aviation, rail, and other surface transportation, and maritime transportation (including port security).

(2) To coordinate and oversee the transportation-related responsibilities of other departments and agencies of the Federal Government other than the Department of Defense and the military departments.

(3) To coordinate and provide notice to other departments and agencies of the Federal Government, and appropriate agencies of State and local governments, including departments and agencies for transportation, law enforcement, and border control, about threats to transportation.

(4) To carry out other duties, and exercise other powers, relating to transportation during a national emergency, that the Secretary shall prescribe.

(b) AUTHORITY OF OTHER DEPARTMENTS AND AGENCIES.—The authority of the Administrator under this section shall not supersede the authority of another department or agency of the Federal Government under law with respect to transportation or transportation-related matters, whether or not during a national emergency.

(c) CIRCUMSTANCES.—The Secretary shall prescribe the circumstances constituting a national emergency for purposes of this section.

§ 11503. Management of security information

In consultation with the Transportation Security Oversight Board, the Administrator shall—

(1) enter into memoranda of understanding with Federal agencies or other entities to share or otherwise cross-check, as necessary, data on individuals identified on Federal agency databases who may pose a risk to transportation or national security;

(2) establish procedures for notifying the Administrator of the Federal Aviation Administration, appropriate State and local law enforcement officials, and airport or airline security officers of the identity of individuals known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety;

(3) in consultation with other appropriate Federal agencies and air carriers, establish policies and procedures requiring air carriers—

(A) to use information from government agencies to identify individuals on passenger lists who may be a threat to civil aviation or national security; and

(B) if such an individual is identified, to notify appropriate law enforcement agencies, prevent the individual from boarding an aircraft, or take other appropriate action with respect to that individual; and

(4) consider requiring passenger air carriers to share passenger lists with appropriate Federal agencies for the purpose of identifying individuals who may pose a threat to aviation safety or national security.

§ 11504. View of National Transportation Safety Board

In taking an action under this section that could affect safety, the Administrator shall give great weight to the timely views of the National Transportation Safety Board.

§ 11505. Acquisitions

(a) IN GENERAL.—The Administrator may—

(1) acquire (by purchase, lease, condemnation, or otherwise) real property, or an interest in the property, in and outside the continental United States, that the Administrator considers necessary;

(2) acquire (by purchase, lease, condemnation, or otherwise) and to construct, repair, operate, and maintain personal property (including office space and patents), or an interest in the property, in and outside the continental United States, that the Administrator considers necessary;

(3) lease to others the real and personal property and to provide by contract or otherwise for necessary facilities for the welfare of Transportation Security Administration employees and to acquire, maintain, and operate equipment for these facilities;

(4) acquire services, including personal services the Secretary determines necessary, and acquire (by purchase, lease, condemnation, or

otherwise) and construct, repair, operate, and maintain research and testing sites and facilities; and

(5) in cooperation with the Administrator of the Federal Aviation Administration, utilize the research and development facilities of the Federal Aviation Administration.

(b) TITLE.—Title to property or an interest in property acquired under this section shall be held by the Government of the United States.

(c) CHARGE FOR LEASE OF REAL AND PERSONAL PROPERTY.—Notwithstanding section 3302 of title 31, the Administrator may impose a reasonable charge for the lease of real and personal property to Transportation Security Administration employees and for use by Transportation Security Administration employees and may credit amounts received to the appropriation or fund initially charged for operating and maintaining the property. The amounts are available, without fiscal year limitation, for expenditure for property management, operation, protection, construction, repair, alteration, and related activities.

§ 11506. Transfers of funds

The Administrator may accept transfers of unobligated balances and unexpended balances of funds appropriated to other Federal agencies (as the term ''agency'' is defined in section 551 of title 5) to carry out functions assigned by law to the Administrator.

§ 11507. Regulations

(a) IN GENERAL.—The Administrator may issue, rescind, and revise regulations as necessary to carry out the functions of the Transportation Security Administration.

(b) EMERGENCY PROCEDURES.—

(1) IN GENERAL.—Notwithstanding another law or Executive order (including an Executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary.

(2) REVIEW BY TRANSPORTATION SECURITY OVERSIGHT BOARD.—A regulation or security directive issued under this subsection shall be subject to review by the Transportation Security Oversight Board established under section 10319 of this title. A regulation or security directive issued under this subsection shall remain effective for a period not to exceed 90 days unless ratified or disapproved by the Board or rescinded by the Secretary.

(c) FACTORS TO CONSIDER.—In determining whether to issue, rescind, or revise a regulation under this chapter, the Administrator shall consider, as a factor in the final determination, whether the costs of the regulation are excessive in relation to the enhancement of security the regulation will provide. The Administrator may waive requirements for an analysis that estimates the number of lives that will be saved by the regulation and the monetary value of lives if the Administrator determines that it is not feasible to make an estimate.

(d) AIRWORTHINESS OBJECTIONS BY FEDERAL AVIATION ADMINISTRATION.—

(1) IN GENERAL.—The Administrator shall not take an aviation security action under this title if the Administrator of the Federal Aviation Administration notifies the Administrator that the action could adversely affect the airworthiness of an aircraft.

(2) REVIEW BY ADMINISTRATOR.—Notwithstanding paragraph (1), the Administrator may take an aviation security action, after receiving a notification concerning the action from the Administrator of the Federal Aviation Administration under paragraph (1), if the Secretary of Transportation subsequently approves the action.

§ 11508. Personnel and services

(a) AUTHORITY OF ADMINISTRATOR.—In carrying out the functions of the Transportation Security Administration, the Administrator has the same authority as is provided to the Administrator of the Federal Aviation Administration under subsections (l) and (m) of section 106 of title 49.

(b) AUTHORITY OF AGENCY HEADS.—The head of a Federal agency shall have the same authority to provide services, supplies, equipment, personnel, and facilities to the Secretary as the head has to provide services, supplies, equipment, personnel, and facilities to the Administrator of the Federal Aviation Administration under section 106(m) of title 49.

(c) COORDINATION TO PREPARE FOR, PROTECT AGAINST, AND RESPOND TO PUBLIC HEALTH THREATS TO THE TRANSPORTATION SECURITY SYSTEM.—

(1) IN GENERAL.—Pursuant tosection 106(m) of title 49, the Administrator may provide Transportation Security Administration personnel, who are not engaged in front line transportation security efforts, to other components of the Department and other Federal agencies to improve coordination with the components and agencies to prepare for, protect against, and respond to public health threats to the transportation security system of the United States.

(2)BRIEFING.—Not later than 180 days after December 27, 2021, the Administrator shall brief the appropriate congressional committees

regarding efforts to improve coordination with other components of the Department and other Federal agencies to prepare for, protect against, and respond to public health threats to the transportation security system of the United States

§ 11509. Personnel management system

(a) IN GENERAL.—The personnel management system established by the Administrator of the Federal Aviation Administration under section 40122 of title 49 applies to employees of the Transportation Security Administration.

(b) MODIFICATIONS.—Subject to the requirements of section 40122 of title 49, the Administrator may make modifications to the personnel management system with respect to those employees as the Administrator considers appropriate, such as adopting aspects of other personnel systems of the Department.

(c) MERITORIOUS EXECUTIVE OR DISTINGUISHED EXECUTIVE RANK AWARDS.—

(1) DEFINITION OF APPLICABLE SECTIONS OF TITLE 5.—In this subsection, the term ''applicable sections of title 5'' means—

(A) section 4507(b) through (d) of title 5; and

(B) section 4507a(b) and (c) of title 5.

(2) IN GENERAL.—Notwithstanding section 40122(g)(2) of title 49, the applicable sections of title 5 shall apply to the Transportation Security Administration personnel management system, except that—

(A) for purposes of applying the applicable sections of title 5 to the personnel management system—

(i) the term ''agency'' means the Department;

(ii) the term ''career appointee'' means a Transportation Security Administration employee serving on a career Transportation Security Administration Executive appointment;

(iii) the term ''senior career employee'' means a Transportation Security Administration employee covered by the Transportation Security Administration Core Compensation System at the L or M pay band; and

(iv) the term ''senior executive'' means a Transportation Security Administration executive serving on a Transportation Security Administration Executive appointment;

(B) receipt by a career appointee or a senior career employee of the rank of Meritorious Executive or Meritorious Senior Professional entitles the individual to a lump-sum payment of an amount equal to 20 percent of annual basic pay, which shall be in addition

to the basic pay paid under the applicable Transportation Security Administration pay system; and

(C) receipt by a career appointee or a senior career employee of the rank of Distinguished Executive or Distinguished Senior Professional entitles the individual to a lump-sum payment of an amount equal to 35 percent of annual basic pay, which shall be in addition to the basic pay paid under the applicable Transportation Security Administration pay system.

§ 11510. Authority of Inspector General

The Transportation Security Administration is subject to chapter 4 of title 5 and other laws relating to the authority of the Inspector General of the Department.

§ 11511. Law enforcement powers

(a) IN GENERAL.—The Administrator may designate an employee of the Transportation Security Administration or other Federal agency to serve as a law enforcement officer.

(b) POWERS.—While engaged in official duties of the Transportation Security Administration as required to fulfill the responsibilities under this section, a law enforcement officer designated under paragraph (1) may—

(1) carry a firearm;

(2) make an arrest without a warrant for any offense against the United States committed in the presence of the officer, or for any felony cognizable under the laws of the United States if the officer has probable cause to believe that the person to be arrested has committed or is committing the felony; and

(3) seek and execute warrants for arrest or seizure of evidence issued under the authority of the United States upon probable cause that a violation has been committed.

(c) GUIDELINES ON EXERCISE OF AUTHORITY.—The authority provided by this section shall be exercised in accordance with guidelines prescribed by the Administrator, in consultation with the Attorney General, and shall include adherence to the Attorney General's policy on use of deadly force.

(d) REVOCATION OR SUSPENSION OF AUTHORITY.—The powers authorized by this section may be rescinded or suspended should the Attorney General determine that the Administrator has not complied with the guidelines prescribed in subsection (c) and convey the determination in writing to the Secretary and the Administrator.

§ 11512. Authority to exempt

The Administrator may grant an exemption from a regulation prescribed in carrying out this chapter if the Administrator determines that the exemption is in the public interest.

§ 11513. Nondisclosure of security activities

(a) IN GENERAL.—Notwithstanding section 552 of title 5, the Administrator shall prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of chapter 409 of this title or the Aviation and Transportation Security Act (Public Law 107–71, 115 Stat. 597) if the Administrator decides that disclosing the information would—

(1) be an unwarranted invasion of personal privacy;

(2) reveal a trade secret or privileged or confidential commercial or financial information; or

(3) be detrimental to the security of transportation.

(b) AVAILABILITY OF INFORMATION TO CONGRESS.—Subsection (a) does not authorize information to be withheld from a committee of Congress authorized to have the information.

(c) LIMITATION ON TRANSFERABILITY OF DUTIES.—Except as otherwise provided by law, the Administrator may not transfer a duty or power under this section to another department, agency, or instrumentality of the United States.

(d) LIMITATIONS.—Nothing in this section, or any other provision of law, shall be construed to authorize the designation of information as sensitive security information (as defined in section 1520.5 of title 49, Code of Federal Regulations)—

(1) to conceal a violation of law, inefficiency, or administrative error;

(2) to prevent embarrassment to a person, organization, or agency;

(3) to restrain competition; or

(4) to prevent or delay the release of information that does not require protection in the interest of transportation security, including basic scientific research information not clearly related to transportation security.

§ 11514. Transportation security strategic planning

(a) IN GENERAL.—The Secretary shall develop, prepare, implement, and update, as needed—

(1) a National Strategy for Transportation Security; and

(2) transportation modal security plans addressing security risks, including threats, vulnerabilities, and consequences, for aviation, railroad, ferry, highway, maritime, pipeline, public transportation, over-the-road bus, and other transportation infrastructure assets.

(b) ROLE OF SECRETARY OF TRANSPORTATION.—The Secretary shall work jointly with the Secretary of Transportation in developing, revising, and updating the documents required by paragraph (1).

(c) CONTENTS OF NATIONAL STRATEGY FOR TRANSPORTATION SECURITY.—The National Strategy for Transportation Security shall include the following:

(1) An identification and evaluation of the transportation assets in the United States that, in the interests of national security and commerce, must be protected from attack or disruption by terrorist or other hostile forces, including modal security plans for aviation, bridge and tunnel, commuter rail and ferry, highway, maritime, pipeline, rail, mass transit, over-the-road bus, and other public transportation infrastructure assets that could be at risk of attack or disruption.

(2) The development of risk-based priorities, based on risk assessments conducted or received by the Secretary (including assessments conducted under the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 266)), across all transportation modes and realistic deadlines for addressing security needs associated with those assets referred to in paragraph (1).

(3) The most appropriate, practical, and cost-effective means of defending those assets against threats to their security.

(4) A forward-looking strategic plan that sets forth the agreed-on roles and missions of Federal, State, regional, local, and tribal authorities and establishes mechanisms for encouraging cooperation and participation by private-sector entities, including nonprofit employee labor organizations, in the implementation of the plan.

(5) A comprehensive delineation of prevention, response, and recovery responsibilities and issues regarding threatened and executed acts of terrorism within the United States and threatened and executed acts of terrorism outside the United States to the extent the acts affect United States transportation systems.

(6) A prioritization of research and development objectives that support transportation security needs, giving a higher priority to research and development directed toward protecting vital transportation assets. Transportation security research and development projects shall be based, to the extent practicable, on the prioritization. Nothing in the preceding sentence shall be construed to require the termination of a research or development project initiated by the Secretary or the Secretary of Transportation before August 3, 2007.

(7) A 3- and 10-year budget for Federal transportation security programs that will achieve the priorities of the National Strategy for Transportation Security.

(8) Methods for linking the individual transportation modal security plans and the programs contained therein, and a plan for addressing the security needs of intermodal transportation.

(9) Transportation modal security plans described in subsection (a)(2), including operational recovery plans to expedite, to the maximum extent practicable, the return to operation of an adversely affected transportation system following a major terrorist attack on that system or other incident. These plans shall be coordinated with the resumption of trade protocols required under section 30502 of this title and the National Maritime Transportation Security Plan required under section 70103(a) of title 46.

(d) SUBMISSIONS OF PLANS.—

(1) DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEES.—In this subsection, the term ''appropriate congressional committees'' means the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation, the Committee on Homeland Security and Governmental Affairs, and the Committee on Banking, Housing, and Urban Affairs of the Senate.

(2) BIENNIAL STRATEGY REPORT.—The Secretary shall submit the National Strategy for Transportation Security, including the transportation modal security plans and any revisions to the National Strategy for Transportation Security and the transportation modal security plans, to appropriate congressional committees not less frequently than April 1 of each even-numbered year.

(3) PERIODIC PROGRESS REPORT.—

(A) REQUIREMENT FOR REPORT.—Each year, in conjunction with the submission of the budget to Congress under section 1105(a) of title 31, the Secretary shall submit to the appropriate congressional committees an assessment of the progress made on implementing the National Strategy for Transportation Security, including the transportation modal security plans.

(B) CONTENT.—Each progress report submitted under this paragraph shall include, at a minimum, the following:

(i) Recommendations for improving and implementing the National Strategy for Transportation Security and the transportation modal and intermodal security plans that the Secretary of Homeland Security, in consultation with the Secretary of Transportation, considers appropriate.

(ii) An accounting of all grants for transportation security, including grants and contracts for research and development,

awarded by the Secretary in the most recent fiscal year and a description of how the grants accomplished the goals of the National Strategy for Transportation Security.

(iii) An accounting of all—

(I) funds requested in the President's budget submitted pursuant to section 1105 of title 31 for the most recent fiscal year for transportation security, by mode;

(II) personnel working on transportation security by mode, including the number of contractors; and

(III) information on the turnover in the previous year among senior staff of the Department, including component agencies, working on transportation security issues. The information shall include the number of employees who have permanently left the office, agency, or area in which they worked, and the amount of time that they worked for the Department.

(C) WRITTEN EXPLANATION OF TRANSPORTATION SECURITY ACTIVITIES NOT DELINEATED IN THE NATIONAL STRATEGY FOR TRANSPORTATION SECURITY.—At the end of each fiscal year, the Secretary shall submit to the appropriate congressional committees a written explanation of any Federal transportation security activity that is inconsistent with the National Strategy for Transportation Security, including the amount of funds to be expended for the activity and the number of personnel involved.

(4) CLASSIFIED MATERIAL.—Any part of the National Strategy for Transportation Security, or any part of the transportation modal security plans, that involves information that is properly classified under criteria established by Executive order shall be submitted to the appropriate congressional committees separately in a classified format.

(e) PRIORITY STATUS.—

(1) IN GENERAL.—The National Strategy for Transportation Security shall be the governing document for Federal transportation security efforts.

(2) OTHER PLANS AND REPORTS.—The National Strategy for Transportation Security shall include, as an integral part or as an appendix—

(A) the current National Maritime Transportation Security Plan under section 70103 of title 46;

(B) the report required by section 40958 of this title;

(C) transportation modal security plans required under this chapter;

(D) the transportation-sector-specific plan required under Homeland Security Presidential Directive–7; and

(E) any other transportation security plan or report that the Secretary determines appropriate for inclusion.

(f) COORDINATION.—In carrying out the responsibilities under this section, the Secretary, in coordination with the Secretary of Transportation, shall consult, as appropriate, with Federal, State, and local agencies, tribal governments, private-sector entities (including nonprofit employee labor organizations), institutions of higher learning, and other entities.

(g) PLAN DISTRIBUTION.—The Secretary shall make available and appropriately publicize an unclassified version of the National Strategy for Transportation Security, including its component transportation modal security plans, to Federal, State, regional, local and tribal authorities, transportation system owners or operators, private-sector stakeholders, including nonprofit employee labor organizations representing transportation employees, institutions of higher learning, and other appropriate entities.

§ 11515. Risk scenarios

(a) ANNUAL DEVELOPMENT OF RISK-BASED PRIORITIES.—The Administrator shall annually develop, consistent with the transportation modal security plans required under section 11514 of this title, risk-based priorities based on risk assessments conducted or received by the Secretary across all transportation modes that consider threats, vulnerabilities, and consequences.

(b) ANALYSIS OF SCENARIOS.—The Administrator shall ensure that the risk-based priorities identified under subsection (a) are informed by an analysis of terrorist attack scenarios for each transportation mode, including cyberattack scenarios and intelligence and open source information about current and evolving threats.

(c) REPORT.—Not later than 120 days after the date the annual risk-based priorities are developed under subsection (a), the Administrator shall submit to the Committees on Commerce, Science, and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives a report that includes the following:

(1) Copies of the risk assessments for each transportation mode.

(2) A summary that ranks the risks within and across modes.

(3) A description of the risk-based priorities for securing the transportation sector that identifies and prioritizes the greatest security needs of the transportation sector, both across and within modes, in the order in which the priorities should be addressed.

(4) Information on the underlying methodologies used to assess risks across and within each transportation mode and the basis for assumptions regarding threats, vulnerabilities, and consequences made in assessing and prioritizing risks within each mode and across modes.

(d) SUBMISSION OF INFORMATION.—Information provided under subsection (c) may be submitted in a classified format or unclassified format, as the Administrator considers appropriate.

§ 11516. Transportation Security Information Sharing Plan

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' has the meaning given the term in section 11514 of this title.

(2) PLAN.—The term ''Plan'' means the Transportation Security Information Sharing Plan established under subsection (b).

(3) PUBLIC AND PRIVATE STAKEHOLDERS.—The term ''public and private stakeholders'' means Federal, State, and local agencies, tribal governments, and appropriate private entities, including nonprofit employee labor organizations representing transportation employees.

(4) TRANSPORTATION SECURITY INFORMATION.—The term ''transportation security information'' means information relating to the risks to transportation modes, including aviation, public transportation, railroad, ferry, highway, maritime, pipeline, and over-the-road bus transportation, and may include specific and general intelligence products, as appropriate.

(b) ESTABLISHMENT OF PLAN.—The Secretary, in consultation with the program manager of the information sharing environment established under section 11908 of this title, the Secretary of Transportation, and public and private stakeholders, shall establish a Transportation Security Information Sharing Plan. In establishing the Plan, the Secretary shall gather input on the development of the Plan from private and public stakeholders and the program manager of the information sharing environment established under section 11908 of this title.

(c) PURPOSE OF PLAN.—The Plan shall promote the sharing of transportation security information between the Department of Homeland Security and public and private stakeholders.

(d) CONTENT OF PLAN.—The Plan shall include—

(1) a description of how intelligence analysts in the Department will coordinate their activities in the Department and with other Federal, State, and local agencies, and tribal governments, including coordination with existing modal information sharing centers and the center described in section 40509 of this title;

(2) the establishment of a point of contact, which may be a single point of contact in the Department, for each mode of transportation for the sharing of transportation security information with public and private stakeholders, including an explanation and justification to the appropriate congressional committees if the point of contact established under this paragraph differs from the agency in the Department that has the primary authority, or has been delegated the authority by the Secretary, to regulate the security of that transportation mode;

(3) a reasonable deadline by which the Plan will be implemented; and

(4) a description of resource needs for fulfilling the Plan.

(e) COORDINATION WITH INFORMATION SHARING.—The Plan shall be—

(1) implemented in coordination, as appropriate, with the program manager for the information sharing environment established under section 11908 of this title; and

(2) consistent with the establishment of the information sharing environment and policies, guidelines, procedures, instructions, or standards established by the President or the program manager for the implementation and management of the information sharing environment.

(f) REPORTS TO CONGRESS.—The Secretary shall annually submit to the appropriate congressional committees a report containing the Plan.

(g) SECURITY CLEARANCES.—The Secretary shall, to the greatest extent practicable, take steps to expedite the security clearances needed for designated public and private stakeholders to receive and obtain access to classified information distributed under this section, as appropriate.

(h) CLASSIFICATION OF MATERIAL.—The Secretary, to the greatest extent practicable, shall provide designated public and private stakeholders with transportation security information in an unclassified format.

(i) STAKEHOLDER SEMIANNUAL REPORT.—

(1) IN GENERAL.—Except as provided in paragraph (2), the Secretary shall provide a semiannual report to the appropriate congressional committees that includes—

(A) the number of public and private stakeholders who were provided with each report on the Plan;

(B) a description of the measures the Secretary has taken to ensure proper treatment and security for classified information to be shared with the public and private stakeholders under the Plan; and

(C) an explanation of the reason for the denial of transportation security information to a stakeholder who had previously received the information.

(2) WHEN REPORT NOT REQUIRED.—The Secretary is not required to provide a semiannual report under paragraph (1) if no stakeholders have been added to or removed from the group of persons with whom transportation security information is shared under the Plan since the end of the period covered by the last preceding semiannual report.

§ 11517. Public area security

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on Commerce, Science, and Transportation of the Senate;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Homeland Security of the House of Representatives.

(2) PUBLIC AND PRIVATE STAKEHOLDERS.—The term ''public and private stakeholders'' has the meaning given the term in section 11516 of this title.

(3) SURFACE TRANSPORTATION ASSET.—The term ''surface transportation asset'' includes—

(A) facilities, equipment, or systems used to provide transportation services by—

(i) a public transportation agency (as defined in section 40501 of this title);

(ii) a railroad carrier (as defined in section 20102 of title 49); or

(iii) an owner or operator of—

(I) an entity offering scheduled, fixed-route transportation services by over-the road bus (as defined in section 40701 of this title); or

(II) a bus terminal; or

(B) other transportation facilities, equipment, or systems, as determined by the Secretary.

(b) WORKING GROUP.—

(1) ESTABLISHMENT.—The Administrator, in coordination with the Cybersecurity and Infrastructure Security Agency, shall establish a working group to promote collaborative engagement between the Transportation Security Administration and public and private stakeholders to develop non-binding recommendations for enhancing security in public areas of transportation facilities (including facilities that are surface

transportation assets), including recommendations regarding the following:

(A) Information sharing and interoperable communication capabilities among the Transportation Security Administration and public and private stakeholders with respect to terrorist or other threats.

(B) Coordinated incident response procedures.

(C) The prevention of terrorist attacks and other incidents through strategic planning, security training, exercises and drills, law enforcement patrols, worker vetting, and suspicious activity reporting.

(D) Infrastructure protection through effective construction design barriers and installation of advanced surveillance and other security technologies.

(2) ANNUAL REPORT.—

(A) SUBMISSION.—Not later than 1 year after the date the working group is established under paragraph (1), the Administrator shall submit to the appropriate committees of Congress a report, covering the 12-month period preceding the date of the report, on—

(i) the organization of the working group;

(ii) the activities of the working group;

(iii) the participation of the Transportation Security Administration and public and private stakeholders in the activities of the working group;

(iv) the findings of the working group, including any recommendations.

(B) PUBLICATION.—The Administrator may publish a public version of the report that describes the activities of the working group and such related matters as would be informative to the public, consistent with section 552(b) of title 5.

(3) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of title 5 shall not apply to the working group established under paragraph (1) or any subcommittee of the working group.

(c) TECHNICAL ASSISTANCE.—The Secretary shall—

(1) inform owners and operators of surface transportation assets about the availability of technical assistance, including vulnerability assessment tools and cybersecurity guidelines, to help protect and enhance the resilience of public areas of the assets; and

(2) on request, and subject to the availability of appropriations, provide the technical assistance to owners and operators of surface transportation assets.

(d) BEST PRACTICES.—

(1) SECRETARY.—Not later than 1 year after October 5, 2018, and periodically thereafter, the Secretary shall publish on the Department website and widely disseminate, as appropriate, current best practices for protecting and enhancing the resilience of public areas of transportation facilities (including facilities that are surface transportation assets), including associated frameworks or templates for implementation.

(2) ADMINISTRATOR.—The Administrator shall, in accordance with law, periodically submit information, as received or developed, on best practices developed by the Transportation Security Administration or appropriate transportation stakeholders related to protecting the public spaces of transportation infrastructure from emerging threats, to the following:

(A) Federal Security Directors at airports.

(B) Appropriate security directors for other modes of transportation.

(C) Other appropriate transportation security stakeholders.

(e) INFORMATION SHARING.—The Administrator shall, in accordance with law—

(1) in coordination with the Office of the Director of National Intelligence and industry partners, implement improvements to the Air Domain Intelligence and Analysis Center to encourage increased participation from stakeholders and enhance government and industry security information sharing on transportation security threats, including on cybersecurity threat awareness;

(2) improve and expand the City and Airport Threat Assessment or similar program to public and private stakeholders to capture, quantify, communicate, and apply applicable intelligence to inform transportation infrastructure mitigation measures, such as—

(A) quantifying levels of risk by airport that can be used to determine risk-based security mitigation measures at each location; and

(B) determining random and surge employee inspection operations based on changing levels of risk;

(3) continue to disseminate Transportation Intelligence Notes, tearlines, and related intelligence products to appropriate transportation security stakeholders on a regular basis; and

(4) continue to regularly conduct routine and threat-specific classified briefings between the Transportation Security Administration and appropriate transportation sector stakeholders on an individual or group basis to provide greater information sharing between public and private sectors.

(f) MASS NOTIFICATION.—The Administrator shall encourage security stakeholders to utilize mass notification systems, including the Integrated Public Alert Warning System of the Federal Emergency Management Agency and social media platforms, to disseminate information to transportation community employees, travelers, and the general public, as appropriate.

(g) PUBLIC AWARENESS PROGRAMS.—The Secretary, in coordination with the Administrator, shall expand public programs of the Department and the Transportation Security Administration that increase security threat awareness, education, and training to include transportation network public area employees, including airport and transportation vendors, local hotels, cab and limousine companies, ridesharing companies, cleaning companies, gas station attendants, cargo operators, and general aviation members.

(h) REVIEW.—

(1) IN GENERAL.—Not later than 1 year after October 5, 2018, the Administrator shall—

(A) review regulations, directives, policies, and procedures issued by the Administrator regarding the transportation of a firearm and ammunition; and

(B) submit to the appropriate committees of Congress a report on the findings of the review under subparagraph (A), including, as appropriate, information on plans to modify a regulation, directive, policy, or procedure based on the review.

(2) CONSULTATION.—In preparing the report under paragraph (1), the Administrator shall consult with—

(A) the Aviation Security Advisory Committee;

(B) the Surface Transportation Security Advisory Committee under section 40722 of this title; and

(C) appropriate public and private stakeholders.

§ 11518. Best practices to secure against vehicle-based attacks

The Administrator shall disseminate best practices to public and private stakeholders regarding how to enhance transportation security against the threat of a vehicle-based terrorist attack.

§ 11519. Enforcement of certain regulations and orders of the Secretary

(a) DEFINITIONS.—In this section:

(1) PERSON.—The term ''person'' does not include—

(A) the United States Postal Service; or

(B) the Department of Defense.

(2) SMALL BUSINESS CONCERN.—The term ''small business concern'' has the meaning given the term in section 3 of the Small Business Act (15 U.S.C. 632).

(b) APPLICABILITY OF SECTION.—

(1) IN GENERAL.—This section applies to the enforcement of regulations prescribed, and orders issued, by the Secretary under a provision of chapter 701 of title 46 or under a provision of title 49 other than a provision of former chapter 449 (in this section referred to as an ''applicable provision of title 49'').

(2) VIOLATIONS OF FORMER CHAPTER 449 OF TITLE 49.—The penalties under part B of subchapter V of chapter 409 of this title apply to violations of regulations prescribed and orders issued by the Secretary or the Administrator under former chapter 449 of title 49.

(3) NON-APPLICABILITY TO CERTAIN VIOLATIONS.—

(A) IN GENERAL.—Subsections (c) through (f) do not apply to violations of regulations prescribed, and orders issued, by the Secretary under a provision of title 49—

(i) involving the transportation of personnel or shipments of materials by contractors where the Department of Defense has assumed control and responsibility;

(ii) by a member of the armed forces of the United States when performing official duties; or

(iii) by a civilian employee of the Department of Defense when performing official duties.

(B) ALTERNATIVE PENALTIES.—Violations described in clause (i), (ii), or (iii) of subparagraph (A) shall be subject to penalties as determined by the Secretary of Defense or the designee of the Secretary of Defense.

(c) CIVIL PENALTY.—

(1) IN GENERAL.—A person is liable to the United States Government for a civil penalty of not more than $10,000 for a violation of a regulation prescribed, or order issued, by the Secretary under an applicable provision of title 49.

(2) REPEAT VIOLATIONS.—A separate violation occurs under this subsection for each day the violation continues.

(d) ADMINISTRATIVE IMPOSITION OF CIVIL PENALTIES.—

(1) IN GENERAL.—The Secretary may impose a civil penalty for a violation of a regulation prescribed, or order issued, under an applicable provision of title 49. The Secretary shall give written notice of the finding of a violation and the penalty.

(2) SCOPE OF CIVIL ACTION.—In a civil action to collect a civil penalty imposed by the Secretary under this section, a court may not reexamine issues of liability or the amount of the penalty.

(3) JURISDICTION.—The district courts of the United States shall have exclusive jurisdiction of civil actions to collect a civil penalty imposed by the Secretary under this section if—

(A) the amount in controversy is more than—

(i) $400,000, if the violation was committed by a person other than an individual or small business concern; or

(ii) $50,000 if the violation was committed by an individual or small business concern;

(B) the action is in rem or another action in rem based on the same violation has been brought; or

(C) another action has been brought for an injunction based on the same violation.

(4) MAXIMUM PENALTY.—The maximum civil penalty the Secretary administratively may impose under this subsection is—

(A) $400,000, if the violation was committed by a person other than an individual or small business concern; or

(B) $50,000, if the violation was committed by an individual or small business concern.

(5) NOTICE AND OPPORTUNITY TO REQUEST HEARING.—Before imposing a penalty under this chapter, the Secretary shall provide to the person against whom the penalty is to be imposed—

(A) written notice of the proposed penalty; and

(B) the opportunity to request a hearing on the proposed penalty, if the Secretary receives the request not later than 30 days after the date on which the person receives notice.

(e) COMPROMISE AND SETOFF.—

(1) COMPROMISE.—The Secretary may compromise the amount of a civil penalty imposed under this section.

(2) SETOFF.—The United States Government may deduct the amount of a civil penalty imposed or compromised under this section from amounts it owes the person liable for the penalty.

(f) INVESTIGATIONS AND PROCEEDINGS.—Subchapter V of chapter 409 of this title applies to investigations and proceedings brought under this sec-

tion to the same extent that chapter 461 of title 49 applies to investigations and proceedings brought with respect to aviation security duties designated to be carried out by the Secretary.

(g) ENFORCEMENT TRANSPARENCY.—

(1) IN GENERAL.—The Secretary shall—

(A) provide an annual summary to the public of all enforcement actions taken by the Secretary under this section; and

(B) include in each summary the docket number of each enforcement action, the type of alleged violation, the penalty or penalties proposed, and the final assessment amount of each penalty.

(2) ELECTRONIC AVAILABILITY.—Each summary under this subsection shall be made available to the public by electronic means.

(3) RELATIONSHIP TO FREEDOM OF INFORMATION ACT AND PRIVACY ACT.—Nothing in this subsection shall be construed to require disclosure of information or records that are exempt from disclosure under section 552 or 552a of title 5.

§ 11520. Registered traveler fee

Notwithstanding section 553 of title 5, the Secretary shall impose a fee for a registered traveler program undertaken by the Department by notice in the Federal Register, and may modify the fee from time to time by notice in the Federal Register. Fees shall not exceed the aggregate costs associated with the program, shall be credited to the Transportation Security Administration registered traveler fee account, and are available until expended.

§ 11521. Enhanced security measures

(a) IN GENERAL.—The Administrator may take the following actions:

(1) Require effective 911 emergency call capability for telephones serving passenger aircraft and passenger trains.

(2) Establish a uniform system of identification for all State and local law enforcement personnel for use in obtaining permission to carry weapons in aircraft cabins and in obtaining access to a secured area of an airport, if otherwise authorized to carry the weapons.

(3) Establish requirements to implement trusted passenger programs and use available technologies to expedite the security screening of passengers who participate in the programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.

(4) In consultation with the Commissioner of the Food and Drug Administration, develop alternative security procedures under which a medical product to be transported on a flight of an air carrier would not be subject to an inspection that would irreversibly damage the product.

(5) Provide for the use of technologies, including wireless and wire line data technologies, to enable the private and secure communication of threats to aid in the screening of passengers and other individuals on airport property who are identified on any State or Federal security-related data base for the purpose of having an integrated response coordination of various authorized airport security forces.

(6) In consultation with the Administrator of the Federal Aviation Administration, consider whether to require all pilot licenses to incorporate a photograph of the license holder and appropriate biometric imprints.

(7) Provide for the use of voice stress analysis, biometric, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft of an air carrier or foreign air carrier in air transportation or intrastate air transportation.

(8) Provide for the use of technology that will permit enhanced instant communications and information between airborne passenger aircraft and appropriate individuals or facilities on the ground.

(9) Require that air carriers provide flight attendants with a discreet, hands-free, wireless method of communicating with the pilots.

(b) ANNUAL REPORT.—Until the Administrator has implemented or decided not to take each of the actions specified in subsection (a), the Administrator shall transmit to Congress by May 19 each year a report on the progress of the Administrator in evaluating and taking the actions, including legislative recommendations that the Secretary may have for enhancing transportation security.

§ 11522. Performance management system

(a) ESTABLISHING A FAIR AND EQUITABLE SYSTEM FOR MEASURING STAFF PERFORMANCE.—The Administrator shall establish a performance management system that strengthens the organization's effectiveness by providing for the establishment of goals and objectives for managers, employees, and organizational performance consistent with the performance plan.

(b) ESTABLISHING MANAGEMENT ACCOUNTABILITY FOR MEETING PERFORMANCE GOALS.—

(1) ADMINISTRATOR.—Each year, the Secretary and the Administrator shall enter into an annual performance agreement that shall set forth organizational and individual performance goals for the Administrator.

(2) SENIOR MANAGERS.—Each year, the Administrator and each senior manager who reports to the Administrator shall enter into an annual performance agreement that sets forth organization and indi-

vidual goals for those managers. All other employees hired under the authority of the Administrator shall enter into an annual performance agreement that sets forth organization and individual goals for those employees.

(c) PERFORMANCE-BASED SERVICE CONTRACTING.—To the extent contracts are used to implement the Aviation and Transportation Security Act (Public Law 107–71, 115 Stat. 597), the Administrator shall, to the extent practical, maximize the use of performance-based service contracts. These contracts should be consistent with guidelines published by the Office of Federal Procurement Policy.

§ 11523. Voluntary provision of emergency services

(a) PROGRAM FOR PROVISION OF VOLUNTARY SERVICES.—

(1) PROGRAM.—The Administrator shall carry out a program to permit qualified law enforcement officers, firefighters, and emergency medical technicians to provide emergency services on commercial air flights during emergencies.

(2) REQUIREMENTS.—The Administrator shall establish requirements for qualifications of providers of voluntary services under the program under paragraph (1), including training requirements, that the Administrator considers appropriate.

(3) CONFIDENTIALITY OF REGISTRY.—If as part of the program under paragraph (1), the Administrator requires or permits registration of law enforcement officers, firefighters, or emergency medical technicians who are willing to provide emergency services on commercial flights during emergencies, the Administrator shall take appropriate actions to ensure that the registry is available only to appropriate airline personnel and otherwise remains confidential.

(4) CONSULTATION.—The Administrator shall consult with the Administrator of the Federal Aviation Administration, appropriate representatives of the commercial airline industry, and organizations representing community-based law enforcement, firefighters, and emergency medical technicians, in carrying out the program under paragraph (1), including the actions taken under paragraph (3).

(b) EXEMPTION FROM LIABILITY.—An individual is not liable for damages in an action brought in a Federal or State court that arises from an act or omission of the individual in providing, or attempting to provide, assistance in the case of an in-flight emergency in an aircraft of an air carrier if the individual meets qualifications as the Administrator prescribes for purposes of this section.

(c) EXCEPTION.—The exemption under subsection (b) shall not apply in a case in which an individual provides, or attempts to provide, assistance

described in subsection (b) in a manner that constitutes gross negligence or willful misconduct.

§ 11524. Disposition of unclaimed money and clothing

(a) IN GENERAL.—

(1) DISPOSITION OF UNCLAIMED MONEY.—Notwithstanding section 3302 of title 31, unclaimed money recovered at an airport security checkpoint—

(A) shall be retained by the Transportation Security Administration; and

(B) shall remain available until expended for the purpose of providing civil aviation security as required in this chapter.

(2) DISPOSITION OF UNCLAIMED CLOTHING.—

(A) IN GENERAL.—In disposing of unclaimed clothing recovered at any airport security checkpoint, the Administrator shall make every reasonable effort, in consultation with the Secretary of Veterans Affairs, to transfer the clothing to the local airport authority or other local authorities for donation to charity, including local veterans organizations or other local charitable organizations for distribution to homeless or needy veterans and veteran families.

(B) AGREEMENTS.—In implementing subparagraph (A), the Administrator may enter into agreements with airport authorities.

(C) OTHER CHARITABLE ARRANGEMENTS.—Nothing in this subsection prevents an airport or the Transportation Security Administration from donating unclaimed clothing to a charitable organization of their choosing.

(D) LIMITATION.—Nothing in this subsection creates a cost to the Government.

(b) ANNUAL REPORT.—Not later than 180 days after October 18, 2004, and annually thereafter, the Administrator shall transmit annually to the Committee on Transportation and Infrastructure of the House of Representatives; the Committee on Appropriations of the House of Representatives; the Committee on Commerce, Science and Transportation of the Senate; and the Committee on Appropriations of the Senate, a report that contains a detailed description of the amount of unclaimed money recovered in total and at each individual airport, and specifies how the unclaimed money is being used to provide civil aviation security.

§ 11525. Transmittals to Congress

The Administrator shall transmit directly to the appropriate committee of Congress each report, legislative proposal, or other communication of the executive branch relating to the Transportation Security Administration and

required to be submitted to Congress or the appropriate committee of Congress.

§ 11526. Transportation security preparedness plan for communicable disease outbreak

(a) DEVELOPMENT.—Not later than December 27, 2023, the Secretary, acting through the Administrator, in coordination with the Chief Medical Officer of the Department, and in consultation with the partners identified under subparagraphs (A) through (D) of subsection (c)(1), shall develop a transportation security preparedness plan to address the event of a communicable disease outbreak. The Secretary, acting through the Administrator, shall ensure the plan aligns with relevant Federal plans and strategies for communicable disease outbreaks.

(b) CONSIDERATIONS.—In developing the plan required under subsection (a), the Secretary, acting through the Administrator, shall consider each of the following:

(1) The findings of the survey required under section 6411 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81, div. F, 135 Stat. 2409).

(2) The findings of the analysis required under section 6414 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81, div. F, 135 Stat. 2412).

(3) The plan required under section 6415 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81, div. F, 135 Stat. 2413).

(4) All relevant reports and recommendations regarding the Administration's response to the COVID19 pandemic, including any reports and recommendations issued by the Comptroller General and the Inspector General of the Department.

(5) Lessons learned from Federal interagency efforts during the COVID19 pandemic.

(c) CONTENTS.—The plan developed under subsection (a) shall include each of the following:

(1) Plans for communicating and collaborating in the event of a communicable disease outbreak with the following partners:

(A) Appropriate Federal departments and agencies, including the Department of Health and Human Services, the Centers for Disease Control and Prevention, the Department of Transportation, the Department of Labor, and appropriate interagency task forces.

(B) The workforce of the Transportation Security Administration, including through the labor organization certified as the ex-

clusive representative of full- and part-time non-supervisory Transportation Security Administration personnel carrying out screening functions undersection 40911 of this title.

(C) International partners, including the International Civil Aviation Organization and foreign governments, airports, and air carriers.

(D) Public and private stakeholders, as the term is defined under section 11516(a) of this title.

(E) The traveling public.

(2) Plans for protecting the safety of the Transportation Security Administration workforce, including—

(A) reducing the risk of communicable disease transmission at screening checkpoints and within the Transportation Security Administration's workforce related to the Administration's transportation security operations and mission;

(B) ensuring the safety and hygiene of screening checkpoints and other workstations;

(C) supporting equitable and appropriate access to relevant vaccines, prescriptions, and other medical care; and

(D) tracking rates of employee illness, recovery, and death.

(3) Criteria for determining the conditions that may warrant the integration of additional actions in the aviation screening system in response to the communicable disease outbreak and a range of potential roles and responsibilities that align with the conditions.

(4) Contingency plans for temporarily adjusting checkpoint operations to provide for passenger and employee safety while maintaining security during the communicable disease outbreak.

(5) Provisions setting forth criteria for establishing an interagency task force or other standing engagement platform with other appropriate Federal departments and agencies, including the Department of Health and Human Services and the Department of Transportation, to address the communicable disease outbreak.

(6) A description of scenarios in which the Administrator should consider exercising authorities provided under section 11502 of this title and for what purposes.

(7) Considerations for assessing the appropriateness of issuing security directives and emergency amendments to regulated parties in various modes of transportation, including surface transportation, and plans for ensuring compliance with the measures.

(8) A description of any potential obstacles, including funding constraints and limitations to authorities, that could restrict the ability of

the Administration to respond appropriately to a communicable disease outbreak.

(d) DISSEMINATION.—On development of the plan required under subsection (a), the Administrator shall disseminate the plan to the partners identified under subsection (c)(1) and to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate.

(e) REVIEW.—Not later than two years after the date on which the plan is disseminated under subsection (d), and biennially thereafter, the Secretary, acting through the Administrator and in coordination with the Chief Medical Officer of the Department, shall review the plan and, after consultation with the partners identified under subparagraphs (A) through (D) of subsection (c)(1), update the plan as appropriate.

§ 11527. Aviation security directives and emergency amendments

(a)IN GENERAL.—The Administrator shall develop and implement guidelines with respect to domestic and last point of departure airports to—

(1) ensure the inclusion, as appropriate, of air carriers, domestic airport operators, and other transportation security stakeholders in the development and implementation of security directives and emergency amendments;

(2) document input provided by air carriers, domestic airport operators, and other transportation security stakeholders during the security directive and emergency amendment, development, and implementation processes;

(3) define a process, including timeframes, and with the inclusion of feedback from air carriers, domestic airport operators, and other transportation security stakeholders, for cancelling or incorporating security directives and emergency amendments into security programs;

(4) conduct engagement with foreign partners on the implementation of security directives and emergency amendments, as appropriate, including recognition if existing security measures at a last point of departure airport are found to provide commensurate security as intended by potential new security directives and emergency amendments; and

(5) ensure that new security directives and emergency amendments are focused on defined security outcomes.

(b) BRIEFING TO CONGRESS.—The Administrator shall brief the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on the guidelines described in paragraph (1).

(c) DECISIONS NOT SUBJECT TO JUDICIAL REVIEW.—Notwithstanding any other provision of law, any action of the Administrator under paragraph (1) is not subject to judicial review.

Subchapter II—Acquisition Improvements

§ 11541. Definitions

In this subchapter:

(1) PLAN.—The term ''Plan'' means the strategic 5-year technology investment plan the Administrator develops under section 11542 of this title.

(2) SECURITY-RELATED TECHNOLOGY.—The term ''security-related technology'' means any technology that assists the Transportation Security Administration in the prevention of, or defense against, threats to United States transportation systems, including threats to people, property, and information.

§ 11542. Technology investment plan

(a) IN GENERAL.—The Administrator—

(1) shall develop and submit to Congress a strategic 5-year technology investment plan that may include a classified addendum to report sensitive transportation security risks, technology vulnerabilities, or other sensitive security information; and

(2) to the extent possible, shall publish the Plan in an unclassified format in the public domain after it is approved by the Secretary.

(b) CONSULTATION.—The Administrator shall develop the Plan in consultation with—

(1) the Under Secretary for Management;

(2) the Under Secretary for Science and Technology;

(3) the Chief Information Officer; and

(4) the aviation stakeholder advisory committee established by the Administrator.

(c) CONTENTS.—The Plan shall include—

(1) an analysis of transportation security risks and the associated capability gaps that would be best addressed by security-related technology, including consideration of the most recent quadrennial homeland security review under section 11706 of this title;

(2) a set of security-related technology acquisition needs that—

(A) is prioritized based on risk and associated capability gaps identified under paragraph (1); and

(B) includes planned technology programs and projects with defined objectives, goals, timelines, and measures;

(3) an analysis of current and forecast trends in domestic and international passenger travel;

(4) an identification of currently deployed security-related technologies that are at or near the end of their lifecycles;

(5) an identification of test, evaluation, modeling, and simulation capabilities, including target methodologies, rationales, and timelines necessary to support the acquisition of the security-related technologies expected to meet the needs under paragraph (2);

(6) an identification of opportunities for public-private partnerships, small and disadvantaged company participation, intragovernment collaboration, university centers of excellence, and national laboratory technology transfer;

(7) an identification of the Transportation Security Administration's acquisition workforce needs for the management of planned security-related technology acquisitions, including consideration of leveraging acquisition expertise of other Federal agencies;

(8) an identification of the security resources, including information security resources, that will be required to protect security-related technology from physical or cyber theft, diversion, sabotage, or attack;

(9) an identification of initiatives to streamline the Transportation Security Administration's acquisition process and provide greater predictability and clarity to small, medium, and large businesses, including the timelines for testing and evaluation;

(10) an assessment of the impact on commercial aviation passengers;

(11) a strategy for consulting airport management, air carrier representatives, and Federal security directors when an acquisition will lead to the removal of equipment at airports, and how the strategy for consulting with those officials of the relevant airports will address potential negative impacts on commercial passengers or airport operations; and

(12) in consultation with the National Institute of Standards and Technology, an identification of security-related technology interface standards, in existence or if implemented, that could promote more interoperable passenger, baggage, and cargo screening systems.

(d) LEVERAGING THE PRIVATE SECTOR.—To the extent practicable, and in a manner that is consistent with fair and equitable practices, the Plan shall—

(1) leverage emerging technology trends and research and development investment trends in the public and private sectors;

(2) incorporate private-sector input, including from the aviation industry stakeholder advisory committee established by the Administrator, through requests for information, industry days, and other innovative means consistent with the Federal Acquisition Regulation; and

(3) in consultation with the Under Secretary for Science and Technology, identify technologies in existence or in development that, with or without adaptation, are expected to be suitable in meeting mission needs.

(e) DISCLOSURE.—The Administrator shall include with the Plan a list of nongovernment persons that contributed to the writing of the Plan.

(f) UPDATE AND REPORT.—The Administrator shall, in collaboration with relevant industry and government stakeholders, annually submit to Congress in an appendix to the budget request and publish in an unclassified format in the public domain—

(1) an update of the Plan;

(2) a report on the extent to which each security-related technology the Transportation Security Administration has acquired since the last issuance or update of the Plan is consistent with the planned technology programs and projects identified under subsection (c)(2) for that security-related technology; and

(3) information about acquisitions completed during the fiscal year preceding the fiscal year during which the report is submitted.

(g) ADDITIONAL UPDATE REQUIREMENTS.—Updates and reports under subsection (f) shall—

(1) be prepared in consultation with—

(A) the individuals described in subsection (b); and

(B) the Surface Transportation Security Advisory Committee established under section 40722 of this title; and

(2) include—

(A) information relating to technology investments by the Transportation Security Administration and the private sector that the Department supports with research, development, testing, and evaluation for aviation, including air cargo, and surface transportation security;

(B) information about acquisitions completed during the fiscal year preceding the fiscal year during which the report is submitted;

(C) information relating to equipment of the Transportation Security Administration that is in operation after the end of the lifecycle of the equipment specified by the manufacturer of the equipment; and

(D) to the extent practicable, a classified addendum to report sensitive transportation security risks and associated capability gaps that would be best addressed by security-related technology described in subparagraph (A).

(h) NOTICE OF COVERED CHANGES TO PLAN.—

(1) DEFINITION OF COVERED CHANGE.—In this subsection, the term ''covered change'' means—

(A) an increase or decrease in the dollar amount allocated to the procurement of a technology; or

(B) an increase or decrease in the number of a technology.

(2) NOTICE REQUIRED.—The Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives notice of a covered change to the Plan not later than 90 days after the date that the covered change is made.

§ 11543. Acquisition justification and reports and certification

(a) ACQUISITION JUSTIFICATION.—Before the Transportation Security Administration implements any security-related technology acquisition, the Administrator, in accordance with the Department's policies and directives, shall determine whether the acquisition is justified by conducting an analysis that includes—

(1) an identification of the scenarios and level of risk to transportation security from those scenarios that would be addressed by the security-related technology acquisition;

(2) an assessment of how the proposed acquisition aligns with the Plan;

(3) a comparison of the total expected lifecycle cost against the total expected quantitative and qualitative benefits to transportation security;

(4) an analysis of alternative security solutions, including policy or procedure solutions, to determine if the proposed security-related technology acquisition is the most effective and cost-efficient solution based on cost-benefit considerations;

(5) an assessment of the potential privacy and civil liberties implications of the proposed acquisition that includes, to the extent practicable, consultation with organizations that advocate for the protection of privacy and civil liberties;

(6) a determination that the proposed acquisition is consistent with fair information practice principles issued by the Privacy Officer of the Department;

(7) confirmation that there are no significant risks to human health or safety posed by the proposed acquisition; and

(8) an estimate of the benefits to commercial aviation passengers.

(b) REPORTS AND CERTIFICATION.—

(1) IN GENERAL.—Not later than the end of the 30-day period preceding the award by the Transportation Security Administration of a contract for any security-related technology acquisition exceeding $30,000,000, the Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives—

(A) the results of the comprehensive acquisition justification under subsection (a); and

(B) a certification by the Administrator that the benefits to transportation security justify the contract cost.

(2) REDUCTION DUE TO IMMINENT TERRORIST THREAT.—If there is a known or suspected imminent threat to transportation security, the Administrator—

(A) may reduce the 30-day period under paragraph (1) to 5 days to rapidly respond to the threat; and

(B) shall immediately notify the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives of the known or suspected imminent threat.

§ 11544. Baseline establishment and reports

(a) BASELINE REQUIREMENTS.–

(1) IN GENERAL.—Before the Transportation Security Administration implements any security-related technology acquisition, the appropriate acquisition official of the Department shall establish and document a set of formal baseline requirements. The requirements shall—

(A) include the estimated costs (including lifecycle costs), schedule, and performance milestones for the planned duration of the acquisition;

(B) identify the acquisition risks and a plan for mitigating those risks; and

(C) assess the personnel necessary to manage the acquisition process, manage the ongoing program, and support training and other operations as necessary.

(2) FEASIBILITY.—In establishing the performance milestones under paragraph (1)(A), the appropriate acquisition official of the Department, to the extent possible and in consultation with the Under Secretary for Science and Technology, shall ensure that achieving those milestones is technologically feasible.

(3) TEST AND EVALUATION PLAN.—The Administrator, in consultation with the Under Secretary for Science and Technology, shall develop a test and evaluation plan that describes—

(A) the activities that are expected to be required to assess acquired technologies against the performance milestones established under paragraph (1)(A);

(B) the necessary and cost-effective combination of laboratory testing, field testing, modeling, simulation, and supporting analysis to ensure that the technologies meet the Transportation Security Administration's mission needs;

(C) an efficient planning schedule to ensure that test and evaluation activities are completed without undue delay; and

(D) if commercial aviation passengers are expected to interact with the security-related technology, methods that could be used to ensure passenger acceptance of and familiarization with the security-related technology.

(4) VERIFICATION AND VALIDATION.—The appropriate acquisition official of the Department—

(A) subject to subparagraph (B), shall utilize independent reviews to verify and validate the performance milestones and cost estimates developed under paragraph (1) for a security-related technology that pursuant to section 11542(c)(2) of this title has been identified as a high priority need in the most recent Plan; and

(B) shall ensure that the use of independent reviewers does not unduly delay the schedule of any acquisition.

(5) STREAMLINING ACCESS FOR INTERESTED VENDORS.—The Administrator shall establish a streamlined process for an interested vendor of a security-related technology to request and receive appropriate access to the baseline requirements and test and evaluation plans that are necessary for the vendor to participate in the acquisition process for that technology.

(b) REVIEW OF BASELINE REQUIREMENTS AND DEVIATION; REPORT.—

(1) REVIEW.—

(A) IN GENERAL.—The appropriate acquisition official of the Department shall review and assess each implemented acquisition to determine if the acquisition is meeting the baseline requirements established under subsection (a).

(B) ASSESSMENT.—The review shall include an assessment of whether—

(i) the planned testing and evaluation activities have been completed; and

(ii) the results of that testing and evaluation demonstrate that the performance milestones are technologically feasible.

(2) REPORT.—Not later than 30 days after making a finding described in clause (i), (ii), or (iii) of subparagraph (A), the Administrator shall submit a report to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives that includes—

(A) the results of any assessment that finds that—

(i) the actual or planned costs exceed the baseline costs by more than 10 percent;

(ii) the actual or planned schedule for delivery has been delayed by more than 180 days; or

(iii) there is a failure to meet any performance milestone that directly impacts security effectiveness;

(B) the cause for the excessive costs, delay, or failure; and

(C) a plan for corrective action.

§11545. Inventory utilization

(a) USE OF EXISTING INVENTORY.—Before the procurement of additional quantities of equipment to fulfill a mission need, the Administrator, to the extent practicable, shall utilize any existing units in the Transportation Security Administration's inventory to meet that need.

(b) TRACKING OF INVENTORY.—

(1) IN GENERAL.—The Administrator shall establish a process for tracking—

(A) the location of security-related technology in the inventory under subsection (a);

(B) the utilization status of security-related technology in the inventory under subsection (a); and

(C) the quality of security-related equipment in the inventory under subsection (a).

(2) INTERNAL CONTROLS.—The Administrator shall implement internal controls to ensure up-to-date accurate data on security-related technology owned, deployed, and in use.

(c) LOGISTICS MANAGEMENT.—

(1) IN GENERAL.—The Administrator shall establish logistics principles for managing inventory in an effective and efficient manner.

(2) LIMITATION ON JUST-IN-TIME LOGISTICS.—The Administrator may not use just-in-time logistics if doing so—

(A) would inhibit necessary planning for large-scale delivery of equipment to airports or other facilities; or

(B) would unduly diminish surge capacity for response to a terrorist threat.

§ 11546. Small business contracting goals

Not later than March 18 of each year, the Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives a report that includes—

(1) the Transportation Security Administration's performance record with respect to meeting its published small-business contracting goals during the preceding fiscal year;

(2) if the goals described in paragraph (1) were not met or the Transportation Security Administration's performance was below the published small-business contracting goals of the Department—

(A) a list of challenges, including deviations from the Transportation Security Administration's subcontracting plans, and factors that contributed to the level of performance during the preceding fiscal year;

(B) an action plan, with benchmarks, for addressing each of the challenges identified in subparagraph (A) that—

(i) is prepared after consultation with the Secretary of Defense and the heads of Federal departments and agencies that achieved their published goals for prime contracting with small and minority-owned businesses, including small and disadvantaged 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.

§ 11547. 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.

§ 11548. Diversified security technology industry marketplace

(a) DEFINITIONS.—In this section:

(1) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(2) SMALL BUSINESS CONCERN.—The term ''small business concern'' has the meaning described under section 3 of the Small Business Act (15 U.S.C. 632).

(3) SMALL BUSINESS INNOVATOR.—The term ''small business innovator'' means a small business concern that has an advanced transportation security technology or capability.

(b) DEVELOPMENT OF STRATEGY.—Not later than 120 days after October 5, 2018, the Administrator shall develop and submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives a strategy to promote a diverse security technology industry marketplace on which the Administrator can rely to acquire advanced transportation security technologies or capabilities, including by increased participation of small business innovators.

(c) CONTENTS OF STRATEGY.—The strategy required under subsection (b) shall include the following:

(1) Information on how existing Transportation Security Administration solicitation, testing, evaluation, piloting, acquisition, and procurement processes impact the Administrator's ability to acquire from the security technology industry marketplace, including small business innovators that have not previously provided technology to the Transportation Security Administration, innovative technologies or capabilities with the potential to enhance transportation security.

(2) Specific actions that the Administrator will take, including modifications to the processes described in paragraph (1), to foster diversification in the security technology industry marketplace.

(3) Projected timelines for implementing the actions described in paragraph (2).

(4) Plans for how the Administrator could, to the extent practicable, assist a small business innovator periodically during the processes, including when a small business innovator lacks adequate resources to participate in the processes, to facilitate an advanced transportation security technology or capability being developed and acquired by the Administrator.

(5) An assessment of the feasibility of partnering with an organization described in section 501(c)(3) of the Internal Revenue Code of 1986 (26 U.S.C. 501(c)(3)) and exempt from tax under section 501(a) of the Internal Revenue Code of 1986 (26 U.S.C. 501(a)) to provide venture capital to businesses, particularly small business innovators, for commercialization of innovative transportation security technologies

that are expected to be ready for commercialization in the near term and within 36 months.

(d) FEASIBILITY ASSESSMENT.—In conducting the feasibility assessment under subsection (c)(5), the Administrator shall consider the following:

(1) Establishing an organization described in section 501(c)(3) of the Internal Revenue Code of 1986 (26 U.S.C. 501(c)(3)) and exempt from tax under section 501(a) of the Internal Revenue Code of 1986 (26 U.S.C. 501(a)) as a venture capital partnership between the private sector and the intelligence community to help businesses, particularly small business innovators, commercialize innovative security-related technologies.

(2) Enhanced engagement through the Science and Technology Directorate of the Department.

(e) RULE OF CONSTRUCTION.—Nothing in this section may be construed as requiring changes to the Transportation Security Administration standards for security technology.

§ 11549. Third party testing and verification of screening technology

(a) IN GENERAL.—In carrying out the responsibilities under section 11501(c)(9) of this title, the Administrator shall develop and implement, not later than 1 year after October 5, 2018, a program to enable a vendor of related security screening technology to obtain testing and verification, including as an alternative to the Transportation Security Administration's test and evaluation process, by an appropriate third party, of the technology before procurement or deployment.

(b) DETECTION TESTING.—

(1) IN GENERAL.—The third party testing and verification program authorized under subsection (a) shall include detection testing to evaluate the performance of the security screening technology system regarding the probability of false alarm and other indicators that the system is able to meet the Transportation Security Administration's mission needs.

(2) RESULTS.—The results of the third party detection testing under paragraph (1) shall be considered final if the results are approved by the Administration in accordance with approval standards developed by the Administrator.

(3) COORDINATION WITH FINAL TESTING.—To the extent practicable, but without compromising the integrity of the Transportation Security Administration test and evaluation process, the Administrator shall coordinate the third party detection testing under paragraph (1) with any subsequent, final Federal Government testing.

(4) INTERNATIONAL TESTING.—To the extent practicable and permissible under law and considering the national security interest of the United States, the Administrator shall—

(A) share detection testing information and standards with appropriate international partners; and

(B) coordinate with appropriate international partners to align Transportation Security Administration testing and evaluation with relevant international standards to maximize the capability to detect explosives and other threats.

(c) OPERATIONAL TESTING.—

(1) IN GENERAL.—Subject to paragraph (2), the third party testing and verification program authorized under subsection (a) shall include operation testing.

(2) LIMITATION.—Third party operational testing under paragraph (1) may not exceed 1 year.

(d) THIRD PARTY TESTING AS AN ALTERNATIVE.—Third party testing under subsection (a) shall replace as an alternative, at the discretion of the Administrator, the testing at the Transportation Security Administration Systems Integration Facility, including testing for—

(1) health and safety factors;

(2) operator interface;

(3) human factors;

(4) environmental factors;

(5) throughput;

(6) reliability, maintainability, and availability factors; and

(7) interoperability.

(e) TESTING AND VERIFICATION FRAMEWORK.—

(1) IN GENERAL.—The Administrator shall—

(A) establish a framework for third party testing and for verifying a security technology is operationally effective and able to meet the Transportation Security Administration's mission needs before it may enter or re-enter, as applicable, the operational context at an airport or other transportation facility;

(B) use phased implementation to allow the Transportation Security Administration and the third party to establish best practices; and

(C) oversee the third party testing and evaluation framework.

(2) RECOMMENDATIONS.—The Administrator shall request the Aviation Security Advisory Committee's Security Technology Subcommittee, in consultation with representatives of the security manufacturers in-

dustry, to develop and submit to the Administrator recommendations for the third party testing and verification framework.

(f) FIELD TESTING.—The Administrator shall prioritize the field testing and evaluation, including by third parties, of security technology and equipment at airports and on site at security technology manufacturers when possible as an alternative to the Transportation Security Administration Systems Integration Facility.

(g) APPROPRIATE THIRD PARTIES.—

(1) CITIZENSHIP REQUIREMENT.—An appropriate third party under subsection (a) shall be—

(A) if an individual, a citizen of the United States; or

(B) if an entity, owned and controlled by a citizen of the United States.

(2) WAIVER.—The Administrator may waive the requirement under paragraph (1)(B) of a parent company that has implemented a foreign ownership, control, or influence mitigation plan that has been approved by the Defense Security Service of the Department of Defense before applying to provide third party testing. The Administrator may reject an application to provide third party testing under subsection (a) submitted by an entity that requires a waiver under this paragraph.

(3) ENSURING NO CONFLICT OF INTEREST.—The Administrator shall ensure, to the extent possible, that an entity providing third party testing under this section does not have a contractual, business, or other pecuniary interest (exclusive of the testing) in—

(A) the security screening technology subject to the testing; or

(B) the vendor of the technology.

(h) REVIEW BY COMPTROLLER GENERAL.—

(1) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate congressional committees'' means—

(A) the Committee on Commerce, Science, and Transportation of the Senate;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Homeland Security of the House of Representatives.

(2) IN GENERAL.—Not later than 2 years after October 5, 2018, the Comptroller General shall submit to the appropriate committees of Congress a study on the third party testing program developed under this section.

(3) REVIEW.—The study under paragraph (2) shall include the following:

(A) Efficiencies or gains in effectiveness achieved in Transportation Security Administration operations, including technology acquisition or screening operations, as a result of the program.

(B) The degree to which the Transportation Security Administration conducts timely and regular oversight of the appropriate third parties engaged in the testing.

(C) The effect of the program on the following:

(i) The introduction of innovative detection technologies into security screening operations.

(ii) The availability of testing for technologies developed by small to medium sized businesses.

(D) Vulnerabilities associated with the program, including with respect to the following:

(i) National security.

(ii) Conflicts of interest between the appropriate third parties engaged in the testing and the entities providing the technologies to be tested.

(iii) Waste, fraud, and abuse.

§ 11550. Transportation Security Administration Systems Integration Facility

(a) IN GENERAL.—The Administrator shall continue to operate the Transportation Security Administration Systems Integration Facility (in this section referred to as the ''TSIF'') for the purposes of testing and evaluating advanced transportation security screening technologies related to the mission of the Transportation Security Administration.

(b) REQUIREMENTS.—The TSIF shall—

(1) evaluate the technologies described in subsection (a) to enhance the security of transportation systems through screening and threat mitigation and detection;

(2) test the technologies described in subsection (a) to support identified mission needs of the Transportation Security Administration and to meet requirements for acquisitions and procurement;

(3) to the extent practicable, provide original equipment manufacturers with test plans to minimize requirement interpretation disputes and adhere to provided test plans;

(4) collaborate with other technical laboratories and facilities for purposes of augmenting the capabilities of TSIF;

(5) deliver advanced transportation security screening technologies that enhance the overall security of domestic transportation systems; and

(6) to the extent practicable, provide funding and promote efforts to enable participation by a small business concern (as the term is described under section 3 of the Small Business Act (15 U.S.C. 632)) that—

(A) has an advanced technology or capability; but

(B) does not have adequate resources to participate in testing and evaluation processes.

(c) STAFFING AND RESOURCE ALLOCATION.—The Administrator shall ensure adequate staffing and resource allocations for the TSIF in a manner that—

(1) prevents unnecessary delays in the testing and evaluation of advanced transportation security screening technologies for acquisitions and procurement determinations;

(2) ensures the issuance of final paperwork certification no later than 45 days after the date the testing and evaluation has concluded; and

(3) ensures collaboration with technology stakeholders to close capabilities gaps in transportation security.

(d) NOTIFICATION OF TESTING AND EVALUATION EXCEEDING 180 DAYS.—

(1) DEFINITIONS.—In this subsection:

(A) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(i) the Committee on Commerce, Science, and Transportation of the Senate;

(ii) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(iii) the Committee on Homeland Security of the House of Representatives.

(B) DELIVERY DATE.—The term ''delivery date'' means the date that the owner of an advanced transportation security screening technology—

(i) after installation, delivers the technology to the Transportation Security Administration for testing and evaluation; and

(ii) submits to the Administrator, in such form and manner as the Administrator prescribes, a signed notification of the delivery described in clause (i).

(2) IN GENERAL.—The Administrator shall notify the appropriate committees of Congress if testing and evaluation by the TSIF of an advance transportation security screening technology under this section exceeds 180 days from the delivery date.

(3) NOTIFICATION.—The notification under paragraph (2) shall include—

(A) information relating to the delivery date;

(B) a justification for why the testing and evaluation process has exceeded 180 days; and

(C) the estimated date for completion of the testing and evaluation.

(e) RETESTING AND EVALUATION.—Advanced transportation security screening technology that fails testing and evaluation by the TSIF may be retested and evaluated at the discretion of the Administrator.

(f) RULE OF CONSTRUCTION.—Nothing in this section may be construed to affect the authority or responsibility of an officer of the Department, or an officer of another Federal department or agency, with respect to research, development, testing, and evaluation of technologies, including the authorities or responsibilities of the Under Secretary for Science and Technology and the Assistant Secretary of the Countering Weapons of Mass Destruction Office.

Subchapter III—Maintenance of Security-Related Technology

§ 11561. Preventive maintenance validation process for security-related technology deployed to airports

(a) IN GENERAL.—Not later than 180 days after October 5, 2018, the Administrator shall develop and implement a preventive maintenance validation process for security-related technology deployed to airports.

(b) MAINTENANCE BY TRANSPORTATION SECURITY ADMINISTRATION PERSONNEL AT AIRPORTS.—For maintenance to be carried out by Transportation Security Administration personnel at airports, the process referred to in subsection (a) shall include the following:

(1) Guidance to Transportation Security Administration personnel at airports specifying how to conduct and document preventive maintenance actions.

(2) Mechanisms for the Transportation Security Administration to verify compliance with the guidance issued pursuant to paragraph (1).

(c) MAINTENANCE BY CONTRACTORS AT AIRPORTS.—For maintenance to be carried out by a contractor at airports, the process referred to in subsection (a) shall require the following:

(1) Provision of monthly preventative maintenance schedules to appropriate Transportation Security Administration personnel at each airport that includes information on each action to be completed by a contractor.

(2) Notification to appropriate Transportation Security Administration personnel at each airport when maintenance action is completed by a contractor.

(3) A process for independent validation by a third party of contractor maintenance.

(d) PENALTIES FOR NONCOMPLIANCE.—The Administrator shall require maintenance for contracts entered into 60 days after October 5, 2018, or later for security-related technology deployed to airports to include penalties for noncompliance when it is determined that either preventive or corrective maintenance has not been completed according to contractual requirements and manufacturers' specifications.

Chapter 117—Management

§ 11701. Under Secretary for Management

(a) DEFINITION OF INTEROPERABLE COMMUNICATIONS.—In this section, the term ''interoperable communications'' has the same meaning given that term in section 10912(a) of this title.

(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.

(5) Facilities, property, equipment, and other material resources.

(6) Security for personnel, information technology and communications systems, facilities, property, equipment, and other material resources.

(7) Strategic management planning and annual performance planning and identification and tracking of performance measures relating to the responsibilities of the Department.

(8) Grants and other assistance management programs.

(9) The management integration and transformation in each functional management discipline of the Department, including information technology, financial management, acquisition management, and human capital management, to ensure an efficient and orderly consolidation of functions and personnel in the Department, including—

(A) the development of centralized data sources and connectivity of information systems to the greatest extent practicable to enhance program visibility, transparency, and operational effectiveness and coordination;

(B) the development of standardized and automated management information to manage and oversee programs and make informed decisions to improve the efficiency of the Department;

(C) the development of effective program management and regular oversight mechanisms, including clear roles and processes for program governance, sharing of best practices, and access to timely, reliable, and evaluated data on all acquisitions and investments; and

(D) the overall supervision, including the conduct of internal audits and management analyses, of the programs and activities of the Department, including establishment of oversight procedures to ensure a full and effective review of the efforts by components of the Department to implement policies and procedures of the Department for management integration and transformation.

(10) The development of a transition and succession plan, before December 1 of each year in which a Presidential election is held, to guide the transition of Department functions to a new Presidential administration, and making the plan available to the next Secretary and Under Secretary for Management and to the congressional homeland security committees.

(11) Reporting to the Government Accountability Office every 6 months to demonstrate measurable, sustainable progress made in implementing the corrective action plans of the Department to address the designation of the management functions of the Department on the bi-annual high-risk list of the Government Accountability Office, until the Comptroller General of the United States submits to the appropriate congressional committees written notification of removal of the high-risk designation.

(12) The conduct of internal audits and management analyses of the programs and activities of the Department.

(13) Any other management duties that the Secretary may designate.

(c) WAIVERS FOR CONDUCTING BUSINESS WITH SUSPENDED OR DEBARRED CONTRACTORS.—Not later than 5 days after the date on which the Chief Procurement Officer or Chief Financial Officer of the Department issues a waiver of the requirement that an agency not engage in business with a contractor or other recipient of funds listed as a party suspended or debarred from receiving contracts, grants, or other types of Federal assistance in the System for Award Management maintained by the General Services Administration, or any successor, the Under Secretary for Management shall submit to the congressional homeland security committees and the Inspector General of the Department notice of the waiver and an explanation of the finding by the Under Secretary that a compelling reason exists for the waiver.

(d) VEHICLE FLEETS.—

(1) DEFINITIONS.—In this subsection:

(A) COMPONENT HEAD.—The term ''component head'' means the head of a component of the Department with a vehicle fleet.

(B) EXCESS VEHICLE.—The term ''excess vehicle'' means a vehicle that is not essential to support mission requirements of a component.

(C) OPTIMAL FLEET SIZE.—The term ''optimal fleet size'' means, with respect to a particular component, the appropriate number of vehicles to support mission requirements of the component.

(D) VEHICLE FLEET.—The term ''vehicle fleet'' means all owned, commercially leased, or Government-leased vehicles of the Department or of a component of the Department, including vehicles used for law enforcement and other purposes.

(2) IN GENERAL.—In carrying out responsibilities regarding vehicle fleets pursuant to subsection (b)(5), the Under Secretary for Manage-

ment shall be responsible for overseeing and managing vehicle fleets throughout the Department. The Under Secretary shall also be responsible for the following:

(A) Ensuring that components are in compliance with Federal law, Federal regulations, executive branch guidance, and Department policy (including associated guidance) relating to fleet management and use of vehicles from home to work.

(B) Developing and distributing a standardized vehicle allocation methodology and fleet management plan for components to use to determine optimal fleet size in accordance with paragraph (5).

(C) Ensuring that components formally document fleet management decisions.

(D) Approving component fleet management plans, vehicle leases, and vehicle acquisitions.

(3) COMPONENT RESPONSIBILITIES.—

(A) IN GENERAL.—Component heads—

(i) shall—

(I) comply with Federal law, Federal regulations, executive branch guidance, and Department policy (including associated guidance) relating to fleet management and use of vehicles from home to work;

(II) ensure that data related to fleet management is accurate and reliable;

(III) use the data to develop a vehicle allocation tool derived by using the standardized vehicle allocation methodology provided by the Under Secretary for Management to determine the optimal fleet size for the next fiscal year and a fleet management plan; and

(IV) use vehicle allocation methodologies and fleet management plans to develop annual requests for funding to support vehicle fleets pursuant to paragraph (7); and

(ii) may not, except as provided in subparagraph (B), lease or acquire new vehicles or replace existing vehicles without prior approval from the Under Secretary for Management pursuant to paragraph (6)(B).

(B) EXCEPTION REGARDING CERTAIN LEASING AND ACQUISITIONS.—If exigent circumstances warrant, a component head may lease or acquire a new vehicle or replace an existing vehicle without prior approval from the Under Secretary for Management. If

under the exigent circumstances a component head leases, acquires, or replaces a vehicle, the component head shall provide to the Under Secretary an explanation of the circumstances.

(4) ONGOING OVERSIGHT.—

(A) QUARTERLY MONITORING.—In accordance with paragraph (5), the Under Secretary for Management shall collect, on a quarterly basis, information regarding component vehicle fleets, including information on fleet size, composition, cost, and vehicle utilization.

(B) AUTOMATED INFORMATION.—The Under Secretary for Management shall seek to achieve a capability to collect, on a quarterly basis, automated information regarding component vehicle fleets, including the number of trips, miles driven, hours and days used, and the associated costs of the mileage for leased vehicles.

(C) MONITORING.—The Under Secretary for Management shall track and monitor component information provided pursuant to subparagraph (A) and, as appropriate, subparagraph (B), to ensure that component vehicle fleets are the optimal fleet size and cost effective. The Under Secretary shall use the information to inform the annual component fleet analyses referred to in paragraph (5).

(5) ANNUAL REVIEW OF COMPONENT FLEET ANALYSIS.—

(A) IN GENERAL.—To determine the optimal fleet size and associated resources needed for each fiscal year, component heads shall annually submit to the Under Secretary for Management a vehicle allocation tool and fleet management plan using information described in paragraph (4)(A). The tools and plans may be submitted in classified form if a component head determines that it is necessary to protect operations or mission requirements.

(B) VEHICLE ALLOCATION TOOL.—Component heads shall develop a vehicle allocation tool in accordance with subclause (III) of paragraph (3)(A)(i) that includes an analysis of the following:

(i) Vehicle utilization data, including the number of trips, miles driven, hours and days used, and the associated costs of the mileage for leased vehicles, in accordance with paragraph (3)(A)(i).

(ii) The role of vehicle fleets in supporting mission requirements for each component.

(iii) Any other information determined relevant by the component heads.

(C) FLEET MANAGEMENT PLANS.—Component heads shall use information described in subparagraph (B) to develop a fleet management plan for each component. The fleet management plans shall include the following:

(i) A plan for how each component may achieve optimal fleet size determined by the vehicle allocation tool required under subparagraph (B), including the elimination of excess vehicles in accordance with paragraph (6), if applicable.

(ii) A cost-benefit analysis supporting the plan.

(iii) A schedule each component will follow to obtain optimal fleet size.

(iv) Any other information determined relevant by component heads.

(D) REVIEW.—The Under Secretary for Management shall review and make a determination on the results of each component's vehicle allocation tool and fleet management plan under this paragraph to ensure each component's vehicle fleets are the optimal fleet size and that components are in compliance with applicable Federal law, Federal regulations, executive branch guidance, and Department policy (including associated guidance) pursuant to paragraph (3) relating to fleet management and use of vehicles from home to work. The Under Secretary shall use the tools and plans when reviewing annual component requests for vehicle fleet funding in accordance with paragraph (7).

(6) GUIDANCE TO DEVELOP FLEET MANAGEMENT PLANS.—The Under Secretary for Management shall provide guidance, pursuant to paragraph (2)(B) on how component heads may achieve optimal fleet size in accordance with paragraph (5), including processes for the following:

(A) Leasing or acquiring additional vehicles or replacing existing vehicles, if determined necessary.

(B) Disposing of excess vehicles that the Under Secretary determines should not be reallocated under subparagraph (C).

(C) Reallocating excess vehicles to other components that may need temporary or long-term use of additional vehicles.

(7) ANNUAL REVIEW OF VEHICLE FLEET FUNDING REQUESTS.—As part of the annual budget process, the Under Secretary for Management shall review and make determinations regarding annual component requests for funding for vehicle fleets. If component heads have not taken steps in furtherance of achieving optimal fleet size in the prior fiscal year pursuant to paragraphs (5) and (6), the Under Sec-

retary shall provide rescission recommendations to the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives and the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate regarding the component vehicle fleets.

(8) ACCOUNTABILITY FOR VEHICLE FLEET MANAGEMENT.—

(A) PROHIBITION ON VEHICLE LEASES, ACQUISITIONS, OR REPLACEMENTS.—The Under Secretary for Management and component heads may not approve in a fiscal year a vehicle lease, acquisition, or replacement request if the component heads did not comply in the prior fiscal year with paragraph (5).

(B) PROHIBITION ON PERFORMANCE COMPENSATION.—No Department official with vehicle fleet management responsibilities may receive annual performance compensation in pay in a fiscal year if the official did not comply in the prior fiscal year with paragraph (5).

(C) PROHIBITION ON CAR SERVICES.—No senior executive service official of the Department whose office has a vehicle fleet may receive access to a car service in a fiscal year if the official did not comply in the prior fiscal year with paragraph (5).

(9) MOTOR POOL.—

(A) IN GENERAL.—The Under Secretary for Management may determine the feasibility of operating a vehicle motor pool to permit components to share vehicles as necessary to support mission requirements to reduce the number of excess vehicles in the Department.

(B) REQUIREMENTS.—The determination of feasibility of operating a vehicle motor pool under subparagraph (A) shall—

(i) include—

(I) regions in the United States in which multiple components with vehicle fleets are located in proximity to one another, or a significant number of employees with authorization to use vehicles are located; and

(II) law enforcement vehicles;

(ii) cover the National Capital Region; and

(iii) take into account different mission requirements.

(C) REPORT.—The Secretary shall include in the Department's next annual performance report required under current law the results of the determination under this paragraph.

(e) APPOINTMENT AND EVALUATION.—The Under Secretary for Management—

(1) is appointed by the President, by and with the advice and consent of the Senate, from among individuals who have—

(A) extensive executive level leadership and management experience in the public or private sector;

(B) strong leadership skills;

(C) a demonstrated ability to manage large and complex organizations; and

(D) a proven record in achieving positive operational results;

(2) shall enter into an annual performance agreement with the Secretary that shall set forth measurable individual and organizational goals; and

(3) is subject to an annual performance evaluation by the Secretary, who shall determine as part of each evaluation whether the Under Secretary for Management has made satisfactory progress toward achieving the goals set out in the performance agreement required under paragraph (2).

(f) SYSTEM FOR AWARD MANAGEMENT CONSULTATION.—The Under Secretary for Management shall require that all Department contracting and grant officials consult the System for Award Management (or successor system) as maintained by the General Services Administration prior to awarding a contract or grant or entering into other transactions to ascertain whether the selected contractor is excluded from receiving Federal contracts, certain subcontracts, and certain types of Federal financial and non-financial assistance and benefits.

(g) WORKFORCE HEALTH AND MEDICAL SUPPORT.—

(1) IN GENERAL.—The Under Secretary for Management shall be responsible for workforce-focused health and medical activities of the Department. The Under Secretary for Management may further delegate responsibility for those activities, as appropriate.

(2) RESPONSIBILITIES.—The Under Secretary for Management, in coordination with the Chief Medical Officer, shall—

(A) provide oversight and coordinate the medical and health activities of the Department for the human and animal personnel of the Department;

(B) establish medical, health, veterinary, and occupational health exposure policy, guidance, strategies, and initiatives for the human and animal personnel of the Department;

(C) as considered appropriate by the Under Secretary for Management, provide medical liaisons to the components of the Department, on a reimbursable basis, to provide subject matter expertise on occupational and public health issues;

(D) serve as the primary representative for the Department on agreements regarding the detail of Commissioned Corps officers of the Public Health Service of the Department of Health and Human Services to the Department, except that components of the Department shall retain authority for funding, determination of specific duties, and supervision of the detailed Commissioned Corps officers; and

(E) perform other duties relating to the responsibilities described in this paragraph as the Secretary may require.

§ 11702. Chief Financial Officer

(a) IN GENERAL.—The Chief Financial Officer shall—

(1) perform functions as specified in chapter 9 of title 31; and

(2) report to the Under Secretary for Management with respect to those functions described in paragraph (1) and other responsibilities that may be assigned.

(b) PROGRAM ANALYSIS AND EVALUATION FUNCTION.—-

(1) ESTABLISHMENT OF OFFICE OF PROGRAM ANALYSIS AND EVALUATION.—The Secretary shall establish an Office of Program Analysis and Evaluation (in this section referred to as the ''Office'') in the Department.

(2) RESPONSIBILITIES.—The Office shall—

(A) analyze and evaluate plans, programs, and budgets of the Department in relation to United States homeland security objectives, projected threats, vulnerability assessments, estimated costs, resource constraints, and the most recent homeland security strategy developed under section 10396(b)(2) of this title;

(B) develop and perform analyses and evaluations of alternative plans, programs, personnel levels, and budget submissions for the Department in relation to United States homeland security objectives, projected threats, vulnerability assessments, estimated costs, resource constraints, and the most recent homeland security strategy developed under section 10396(b)(2) of this title;

(C) establish policies for, and oversee the integration of, the planning, programming, and budgeting system of the Department;

(D) review and ensure that the Department meets performance-based budget requirements established by the Office of Management and Budget;

(E) provide guidance for, and oversee the development of, the Future Years Homeland Security Program of the Department, as specified under section 10396 of this title;

(F) ensure that the costs of Department programs, including classified programs, are presented accurately and completely;

(G) oversee the preparation of the annual performance plan for the Department and the program and performance section of the annual report on program performance for the Department, consistent with sections 1115 and 1116, respectively, of title 31;

(H) provide leadership in developing and promoting improved analytical tools and methods for analyzing homeland security planning and the allocation of resources; and

(I) perform other responsibilities delegated by the Secretary consistent with an effective program analysis and evaluation function.

(3) DIRECTOR OF PROGRAM ANALYSIS AND EVALUATION.—There is a Director of Program Analysis and Evaluation. The Director—

(A) is a principal staff assistant to the Chief Financial Officer of the Department for program analysis and evaluation; and

(B) shall report to an official no lower than the Chief Financial Officer.

(4) REORGANIZATION.—

(A) IN GENERAL.—The Secretary may allocate or reallocate the functions of the Office, or discontinue the Office, under section 10341(b)(1) of this title.

(B) EXEMPTION FROM LIMITATIONS.—Section 10341(b)(2) of this title does not apply to an action by the Secretary under this paragraph.

(c) NOTIFICATION REGARDING TRANSFER OR REPROGRAMMING OF FUNDS.—In a case in which appropriations available to the Department or an officer of the Department are transferred or reprogrammed and notice of the transfer or reprogramming is submitted to Congress (including an officer, office, or committee of Congress), the Chief Financial Officer shall simultaneously submit the notice to the Committee on Homeland Security and the Committee on Oversight and Government Reform of the House of Representatives, and to the Committee on Homeland Security and Governmental Affairs of the Senate.

§ 11703. Chief Information Officer

(a) IN GENERAL.—The Chief Information Officer shall report to the Secretary, or to another official of the Department, as the Secretary may direct.

(b) GEOSPATIAL INFORMATION FUNCTIONS.—

(1) DEFINITIONS.—In this subsection:

(A) GEOSPATIAL INFORMATION.—The term ''geospatial information'' means graphical or digital data depicting natural or man-made physical features, phenomena, or boundaries of the earth and information related thereto, including surveys, maps, charts, remote sensing data, and images.

(B) GEOSPATIAL TECHNOLOGY.—The term ''geospatial technology'' means technology utilized by analysts, specialists, surveyors, photogrammetrists, hydrographers, geodesists, cartographers, architects, or engineers for the collection, storage, retrieval, or dissemination of geospatial information, including—

(i) global satellite surveillance systems;

(ii) global position systems;

(iii) geographic information systems;

(iv) mapping equipment;

(v) geocoding technology; and

(vi) remote sensing devices.

(2) OFFICE OF GEOSPATIAL MANAGEMENT.—

(A) ESTABLISHMENT.—There is in the Office of the Chief Information Officer the Office of Geospatial Management.

(B) GEOSPATIAL INFORMATION OFFICER.—

(i) IN GENERAL.—The Geospatial Information Officer administers the Office of Geospatial Management. The Geospatial Information Officer is appointed by the Secretary. The Geospatial Information Officer serves under the direction of the Chief Information Officer.

(ii) ASSISTS CHIEF INFORMATION OFFICER.—The Geospatial Information Officer assists the Chief Information Officer in carrying out all functions under this section and in coordinating the geospatial information needs of the Department.

(C) COORDINATION OF GEOSPATIAL INFORMATION.—The Chief Information Officer shall establish and carry out a program to provide for the efficient use of geospatial information, which shall include—

(i) providing necessary geospatial information to implement the critical infrastructure protection programs;

(ii) providing leadership and coordination in meeting the geospatial information requirements of those responsible for planning, prevention, mitigation, assessment, and response to emergencies, critical infrastructure protection, and other functions of the Department; and

(iii) coordinating with users of geospatial information within the Department to ensure interoperability and prevent unnecessary duplication.

(D) RESPONSIBILITIES.—In carrying out this subsection, the responsibilities of the Chief Information Officer include—

(i) coordinating the geospatial information needs and activities of the Department;

(ii) implementing standards, as adopted by the Director of the Office of Management and Budget under the processes established under section 216 of the E-Government Act of 2002 (Public Law 107–347, 44 U.S.C. 3501 note), to facilitate the interoperability of geospatial information pertaining to homeland security among all users of the information in—

(I) the Department;

(II) State and local government; and

(III) the private sector;

(iii) coordinating with the Federal Geographic Data Committee and carrying out the responsibilities of the Department pursuant to Office of Management and Budget Circular A-16 and Executive Order 12906 (59 Fed. Reg. 17671, 43 U.S.C. 1457 note); and

(iv) making recommendations to the Secretary and the Executive Director of the Office for State and Local Government Coordination and Preparedness on awarding grants to—

(I) fund the creation of geospatial data; and

(II) execute information sharing agreements regarding geospatial data with State, local, and tribal governments.

§ 11704. Chief Human Capital Officer

(a) REPORTING AUTHORITY.—The Chief Human Capital Officer of the Department shall report directly to the Under Secretary for Management.

(b) RESPONSIBILITIES.—In addition to the responsibilities set forth in chapter 14 of title 5 and other applicable law, the Chief Human Capital Officer of the Department shall—

(1) develop and implement strategic workforce planning policies, including with respect to leader development and employee engagement, that are consistent with Government-wide leading principles, in line with Department strategic human capital goals and priorities, and informed by best practices within the Federal Government and the private sector,taking into account the special requirements of members of the armed forces serving in the Coast Guard;

(2) use performance measures to evaluate, on an ongoing basis,Department-wide strategic workforce planning efforts;

(3) develop, improve, and implement policies that, to the extent practicable, are informed by employee feedback, including compensation flexibilities available to Federal agencies where appropriate, to recruit, hire, train, and retain the workforce of the Department, in coordination with all components of the Department;

(4) identify methods for managing and overseeing human capital programs and initiatives, including leader development and employee engagement programs, in coordination with the head of each component of the Department;

(5) develop a career path framework and create opportunities for leader development in coordination with all components of the Department that is informed by an assessment, carried out by the Chief Human Capital Officer, of the learning and developmental needs of employees in supervisory and nonsupervisory roles across the Department and appropriate workforce planning initiatives;

(6) lead the efforts of the Department for managing employee resources, including training and development opportunities, in coordination with each component of the Department;

(7) work to ensure the Department is implementing human capital programs and initiatives and effectively educating each component of the Department about these programs and initiatives;

(8) identify and eliminate unnecessary and duplicative human capital policies and guidance;

(9) maintain a catalogue of available employee development opportunities, including the Homeland Security Rotation Program pursuant tosection 10366 of this title, departmental leadership development programs, interagency development programs, and other rotational programs;

(10) ensure that employee discipline and adverse action programs comply with the requirements of all pertinent laws, rules, regulations, and Federal guidance, and ensure due process for employees;

(11) analyze each Department or Government-wide Federal workforce satisfaction or morale survey not later than 90 days after the date of the publication of each survey and submit to the Secretary analysis, including, as appropriate, recommendations to improve workforce satisfaction or morale in the Department;

(12) review and approve all component employee engagement action plans to ensure the plans include initiatives responsive to the root cause

of employee engagement challenges, as well as outcome-based performance measures and targets to track the progress of the initiatives;

(13) provide input concerning the hiring and performance of the Chief Human Capital Officer or comparable official in each component of the Department; and

(14) ensure that all employees of the Department are informed of their rights and remedies under chapters 12 and 23 of title 5.

(c) COMPONENT STRATEGIES.—

(1) IN GENERAL.—Each component of the Department shall, in coordination with the Chief Human Capital Officer of the Department, develop a 5-year workforce strategy for the component that will support the goals, objectives, and performance measures of the Department for determining the proper balance of Federal employees and private labor resources.

(2) STRATEGY REQUIREMENTS.—In developing the strategy required under paragraph (1), each component shall consider the effect on human resources associated with creating additional Federal full-time equivalent positions, converting private contractors to Federal employees, or relying on the private sector for goods and services.

(d) CHIEF LEARNING AND ENGAGEMENT OFFICER.—The Chief Human Capital Officer may designate an employee of the Department to serve as a Chief Learning and Engagement Officer to assist the Chief Human Capital Officer in carrying out this section.

(e) ANNUAL SUBMISSION.—Not later than 90 days after the date on which the Secretary submits the annual budget justification for the Department, the Secretary shall submit to the congressional homeland security committees a report that includes a table, delineated by component with actual and enacted amounts, including—

(1) information on the progress in the Department of fulfilling the workforce strategies developed under subsection (c);

(2) information on employee development opportunities catalogued pursuant to subsection (b)(9) and any available data on participation rates, attrition rates, and impacts on retention and employee satisfaction;

(3) information on the progress of Departmentwide strategic workforce planning efforts as determined under subsection (b)(2);

(4) information on the activities of the steering committee established pursuant tosection 11710(a) of this title, including the number of meetings, types of materials developed and distributed, and recommendations made to the Secretary;

(5) the number of on-board staffing for Federal employees from the prior fiscal year;

(6) the total contract hours submitted by each prime contractor as part of the service contract inventory required under section 743 of the Financial Services and General Government Appropriations Act, 2010 (Public Law 111–117, div. C, 31 U.S.C. 501 note); and

(7) the number of full-time equivalent personnel identified under the Intergovernmental Personnel Act of 1970 (42 U.S.C. 4701 et seq.).

(f) LIMITATION.—Nothing in this section overrides or otherwise affects the requirements specified in section 10312 of this title.

§ 11705. Officer for Civil Rights and Civil Liberties

(a) IN GENERAL.—The Officer for Civil Rights and Civil Liberties, who shall report directly to the Secretary, shall—

(1) review and assess information concerning abuses of civil rights, civil liberties, and profiling on the basis of race, ethnicity, or religion, by employees and officials of the Department;

(2) make public through the Internet, radio, television, or newspaper advertisements information on the responsibilities and functions of, and how to contact, the Officer;

(3) assist the Secretary, directorates, and offices of the Department to develop, implement, and periodically review Department policies and procedures to ensure that the protection of civil rights and civil liberties is appropriately incorporated into Department programs and activities;

(4) oversee compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by the programs and activities of the Department;

(5) coordinate with the Privacy Officer to ensure that—

(A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and

(B) Congress receives appropriate reports regarding the programs, policies, and procedures; and

(6) investigate complaints and information indicating possible abuses of civil rights or civil liberties, unless the Inspector General of the Department determines that the complaint or information should be investigated by the Inspector General.

(b) REPORT.—The Secretary shall submit to the President of the Senate, the Speaker of the House of Representatives, and the appropriate committees and subcommittees of Congress on an annual basis a report—

(1) on the implementation of this section, including the use of funds appropriated to carry out this section; and

(2) detailing allegations of abuses described under subsection (a)(1) and actions taken by the Department in response to the allegations.

§ 11706. Quadrennial homeland security review

(a) REQUIREMENT.—

(1) QUADRENNIAL REVIEWS REQUIRED.—In fiscal year 2025, and every 4 years thereafter, the Secretary shall conduct a review of the homeland security of the Nation (in this section referred to as a ''quadrennial homeland security review'').

(2) SCOPE OF REVIEW.—Each quadrennial homeland security review shall be a comprehensive examination of the homeland security strategy of the Nation, including recommendations regarding the long-term strategy and priorities of the Nation for homeland security and guidance on the programs, assets, capabilities, budget, policies, and authorities of the Department.

(3) CONSULTATION.—The Secretary shall conduct each quadrennial homeland security review under this subsection in consultation with—

(A) the heads of other Federal agencies, including the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of the Treasury, the Secretary of Agriculture, the Secretary of Energy, and the Director of National Intelligence;

(B) key officials of the Department, including the Under Secretary for Strategy, Policy, and Plans;

(C) representatives from appropriation advisory committees established pursuant to section 10391 of this title, including the Homeland Security Advisory Council and the Homeland Security Science and Technology Advisory Council, or otherwise established, including the Aviation Security Advisory Committee established pursuant to section 40963 of this title; and

(D) other relevant governmental and nongovernmental entities, including State, local, and tribal government officials, members of Congress, private-sector representatives, academics, and other policy experts.

(4) RELATIONSHIP WITH FUTURE YEARS HOMELAND SECURITY PROGRAM.—The Secretary shall ensure that each review conducted under this section is coordinated with the Future Years Homeland Security Program required under section 10396 of this title.

(b) CONTENTS OF REVIEW.—In each quadrennial homeland security review, the Secretary shall—

(1) delineate and update, as appropriate, the national homeland security strategy, consistent with appropriate national and Department strategies, strategic plans, and Homeland Security Presidential Directives, including the National Strategy for Homeland Security, the National Response Plan, and the Department Security Strategic Plan;

(2) outline and prioritize the full range of the critical homeland security mission areas of the Nation, based on the risk assessment required pursuant to subsection (c)(2)(B);

(3) describe, to the extent practicable, the interagency cooperation, preparedness of Federal response assets, infrastructure, resources required, and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy, required to execute successfully the full range of missions called for in the national homeland security strategy described in paragraph (1) and the homeland security mission areas outlined under paragraph (2);

(4) identify, to the extent practicable, resources required to execute the full range of missions called for in the national homeland security strategy described in paragraph (1) and the homeland security mission areas outlined under paragraph (2), including any resources identified from redundant, wasteful, or unnecessary capabilities or capacities that may be redirected to better support other existing capabilities or capacities, as the case may be; and

(5) include an assessment of the organizational alignment of the Department with the national homeland security strategy referred to in paragraph (1) and the homeland security mission areas outlined under paragraph (2).

(c) REPORTING.—

(1) IN GENERAL.—Not later than 60 days after the date of the President's budget for the fiscal year after the fiscal year in which a quadrennial homeland security review is conducted, the Secretary shall submit to Congress a report regarding that quadrennial homeland security review.

(2) CONTENTS OF REPORT.—Each report submitted under paragraph (1) shall include—

(A) the results of the quadrennial homeland security review;

(B) a risk assessment of the assumed or defined national homeland security interests of the Nation that were examined for the purposes of that review or for purposes of the quadrennial EMP and GMD risk assessment under section 10918(d)(2)(E) of this title;

(C) the national homeland security strategy, including a prioritized list of the critical homeland security missions of the Nation, as required under subsection (b)(2);

(D) to the extent practicable, a description of the interagency cooperation, preparedness of Federal response assets, infrastructure, resources required, and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy, required to execute successfully the full range of missions called for in the applicable national homeland security strategy referred to in subsection (b)(1) and the homeland security mission areas outlined under subsection (b)(2);

(E) an assessment of the organizational alignment of the Department with the applicable national homeland security strategy referred to in subsection (b)(1) and the homeland security mission areas outlined under subsection (b)(2), including the Department's organizational structure, management systems, budget and accounting systems, human resources systems, procurement systems, and physical and technical infrastructure;

(F) to the extent practicable, a discussion of cooperation among Federal agencies in the effort to promote national homeland security;

(G) to the extent practicable, a discussion of cooperation between the Federal Government and State, local, and tribal governments in preventing terrorist attacks and preparing for emergency response to threats and risks to national homeland security; and

(H) any other matter the Secretary considers appropriate.

(3) DOCUMENTATION.—The Secretary shall retain and on request provided to Congress the following documentation regarding each quadrennial homeland security review:

(A) Records regarding the consultation carried out pursuant to subsection (a)(3), including the following:

(i) All written communications, including communications sent out by the Secretary and feedback submitted to the Secretary through technology, online communications tools, in-person discussions, and the interagency process.

(ii) Information on how feedback received by the Secretary informed each quadrennial homeland security review.

(B) Information regarding the risk assessment required pursuant subsection (c)(2)(B), including the following:

(i) The risk model utilized to generate the risk assessment.

(ii) Information, including data used in the risk model utilized to generate the risk assessment.

(iii) Sources of information, including other risk assessments, utilized to generate the risk assessment.

(iv) Information on assumptions, weighing factors, and subjective judgments utilized to generate the risk assessment, together with information on the rationale or basis of the assumptions, weighing factors, and subjective judgments.

(4) PUBLIC AVAILABILITY.—The Secretary shall, consistent with the protection of national security and other sensitive matters, make each report submitted under paragraph (1) publicly available on the Internet website of the Department.

(d) REVIEW.—Not later than 90 days after the submission of each report required under subsection (c)(1), the Secretary shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the degree to which the findings and recommendations developed in the quadrennial homeland security review that is the subject of the report were integrated into the acquisition strategy and expenditure plans for the Department.

§ 11707. Interoperable communications

(a) DEFINITION OF INTEROPERABLE COMMUNICATIONS.—The term ''interoperable communications'' has the same meaning given that term in section 10912(a) of this title.

(b) APPLICATION.—Subsections (c) through (e) shall apply only with respect to the interoperable communications capabilities in the Department and components of the Department to communicate with the Department.

(c) STRATEGY FOR ACHIEVING AND MAINTAINING INTEROPERABLE COMMUNICATIONS AMONG THE COMPONENTS OF THE DEPARTMENT.—The Under Secretary for Management shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a strategy, which shall be updated as necessary, for achieving and sustaining interoperable communications among the components of the Department, including for daily operations, planned events, and emergencies, with corresponding milestones, that includes the following:

(1) An assessment of interoperability gaps in radio communications among the components of the Department, as of July 6, 2015.

(2) Information on efforts and activities, including current and planned policies, directives, and training, of the Department since November 1, 2012, to achieve and maintain interoperable communications

among the components of the Department, and planned efforts and activities of the Department to achieve and maintain the interoperable communications.

(3) An assessment of obstacles and challenges to achieving and maintaining interoperable communications among the components of the Department.

(4) Information on, and an assessment of, the adequacy of mechanisms available to the Under Secretary for Management to enforce and compel compliance with interoperable communications policies and directives of the Department.

(5) Guidance provided to the components of the Department to implement interoperable communications policies and directives of the Department.

(6) The total amount of funds expended by the Department since November 1, 2012, and projected future expenditures, to achieve interoperable communications, including on equipment, infrastructure, and maintenance.

(7) Dates on which Department-wide interoperability is projected to be achieved for voice, data, and video communications, respectively, and interim milestones that correspond to the achievement of each of those modes of communications.

(d) SUPPLEMENTARY MATERIAL.—Together with the strategy required under subsection (c), the Under Secretary for Management shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on—

(1) any intra-agency effort or task force that has been delegated certain responsibilities by the Under Secretary for Management relating to achieving and maintaining interoperable communications among the components of the Department by the dates referred to in subsection (c)(7); and

(2) who in each component is responsible for implementing polices and directives issued by the Under Secretary for Management to achieve and maintain the interoperable communications.

(e) REPORT.–Not later than 100 days after the date on which the strategy required under subsection (c) is submitted, and every 2 years afterwards for 6 years, the Under Secretary for Management shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the status of efforts to implement the strategy required under subsection (c), including the following:

(1) Progress on each interim milestone referred to in subsection (c)(7) toward achieving and maintaining interoperable communications among the components of the Department.

(2) Information on any policies, directives, guidance, and training established by the Under Secretary for Management.

(3) An assessment of the level of compliance, adoption, and participation among the components of the Department with the policies, directives, guidance, and training established by the Under Secretary for Management to achieve and maintain interoperable communications among the components.

(4) Information on any additional resources or authorities needed by the Under Secretary for Management.

§ 11708. Joint Task Forces

(a) DEFINITION OF SITUATIONAL AWARENESS.—In this section, the term ''situational awareness'' means knowledge and unified understanding of unlawful cross-border activity, including—

(1) threats and trends concerning illicit trafficking and unlawful crossings;

(2) the ability to forecast future shifts in the threats and trends;

(3) the ability to evaluate the threats and trends at a level sufficient to create actionable plans; and

(4) the operational capability to conduct continuous and integrated surveillance of the air, land, and maritime borders of the United States.

(b) ESTABLISHMENT.—The Secretary may establish and operate departmental Joint Task Forces to conduct joint operations using personnel and capabilities of the Department for the purposes specified in subsection (d).

(c) DIRECTOR, DEPUTY DIRECTOR, AND STAFF.—

(1) DIRECTOR.—

(A) APPOINTMENT.–Each Joint Task Force shall be headed by a Director, appointed by the President, for a term of not more than 2 years. The Secretary shall submit to the President recommendations for the appointment after consulting with the heads of the components of the Department with membership on any Joint Task Force. A Director shall be—

(i) a current senior official of the Department with not less than 1 year of significant leadership experience at the Department; or

(ii) if no suitable candidate is available at the Department, an individual with—

(I) not less than 1 year of significant leadership experience in a Federal agency since the establishment of the Department; and

(II) a demonstrated ability in, knowledge of, and significant experience working on, the issues to be addressed by the Joint Task Force.

(B) EXTENSION.—The Secretary may extend the appointment of a Director of a Joint Task Force for not more than 2 years if the Secretary determines that the extension is in the best interest of the Department.

(2) DEPUTY DIRECTOR.—For each Joint Task Force, the Secretary shall appoint a Deputy Director, who shall be an official of a different component or office of the Department than the Director.

(3) STAFF.—

(A) IN GENERAL.—Each Joint Task Force shall have a staff, composed of personnel from relevant components and offices of the Department, to assist the Director in carrying out the mission and responsibilities of the Joint Task Force.

(B) INFORMATION TO BE INCLUDED IN REPORT.—The Secretary shall include in the report submitted under subsection (f)(6)—

(i) the number of personnel of each component or office permanently assigned to each Joint Task force; and

(ii) the number of personnel of each component or office assigned on a temporary basis to each Joint Task Force

(d) PURPOSES.—

(1) IN GENERAL.—Subject to paragraph (2), the purposes referred to in subsection (b) are or relate to the following:

(A) Securing the land and maritime borders of the United States.

(B) Addressing homeland security crises.

(C) Establishing regionally based operations.

(2) LIMITATION.—

(A) IN GENERAL.—The Secretary may not establish a Joint Task Force for any major disaster or emergency declared under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) or an incident for which the Federal Emergency Management Agency has primary responsibility for management of the response under chapter 113 of this title, including section 11303(a)(3)(A), unless the responsibilities of the Joint Task Force—

(i) do not include operational functions relating to incident management, including coordination of operations; and

(ii) are consistent with the requirements of paragraphs (1) and (2)(A) of section 11302(b) and section 11309 of this title and section 302 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5143).

(B) RESPONSIBILITIES AND FUNCTIONS OF AGENCY AND ADMINISTRATOR NOT REDUCED.—Nothing in this section may be construed to reduce the responsibilities or functions of the Federal Emergency Management Agency or the Administrator of the Federal Emergency Management Agency under chapter 111 of this title or any other provision of law, including the diversion of an asset, function, or mission from the Federal Emergency Management Agency or the Administrator of the Federal Emergency Management Agency pursuant to section 11306 of this title.

(e) RESPONSIBILITIES.—The Director of a Joint Task Force, subject to the oversight, direction, and guidance of the Secretary, shall—

(1) when the Joint Task Force is established for the purpose referred to in subsection (d)(1)(A), maintain situational awareness in the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(2) provide operational plans and requirements for standard operating procedures and contingency operations in the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(3) plan and execute joint task force activities in the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(4) set and accomplish strategic objectives through integrated operational planning and execution;

(5) exercise operational direction over personnel and equipment from components and offices of the Department allocated to the Joint Task Force to accomplish the objectives of the Joint Task Force;

(6) when the Joint Task Force is established for the purpose referred to in subsection (d)(1)(A), establish operational and investigative priorities in the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(7) coordinate with foreign governments and other Federal, State, and local agencies, as appropriate, to carry out the mission of the Joint Task Force; and

(8) carry out other duties and powers the Secretary determines appropriate.

(f) PERSONNEL AND RESOURCES.—

(1) TEMPORARY ALLOCATION.—The Secretary, on request of the Director of a Joint Task Force and giving appropriate consideration of risk to the other primary missions of the Department, may allocate to the Joint Task Force on a temporary basis personnel and equipment of components and offices of the Department.

(2) COST NEUTRALITY.—A Joint Task Force may not require more resources than would have otherwise been required by the Department to carry out the duties assigned to the Joint Task Force if the Joint Task Force had not been established.

(3) LOCATION OF OPERATIONS.—In establishing a location of operations for a Joint Task Force, the Secretary shall, to the extent practicable, use existing facilities that integrate efforts of components of the Department and State, local, tribal, or territorial law enforcement or military entities.

(4) CONSIDERATION OF IMPACT.—When reviewing requests for allocation of component personnel and equipment under paragraph (1), the Secretary shall consider the impact of the allocation on the ability of the donating component or office to carry out the primary missions of the Department, and in the case of the Coast Guard, the missions specified in section 10312 of this title.

(5) LIMITATION.—Personnel and equipment of the Coast Guard allocated under this subsection may be used only to carry out operations and investigations relating to the missions specified in section 10312 of this title.

(6) REPORT.—The Secretary, at the time the budget of the President for a fiscal year is submitted to Congress under section 1105(a) of title 31, shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a report on the total funding, personnel, and other resources that each component or office of the Department allocated under this subsection to each Joint Task Force to carry out the mission of the Joint Task Force during the fiscal year immediately preceding each report, and a description of the degree to which the resources drawn from each component or office impact the primary mission of the component or office.

(g) COMPONENT RESOURCE AUTHORITY.—As directed by the Secretary—

(1) each Director of a Joint Task Force shall be provided sufficient resources from relevant components and offices of the Department and

the authority necessary to carry out the missions and responsibilities of the Joint Task Force required under this section;

(2) the resources referred to in paragraph (1) shall be under the operational authority, direction, and control of the Director of the Joint Task Force to which the resources are assigned; and

(3) the personnel and equipment of each Joint Task Force shall remain under the administrative direction of the head of the component or office of the Department that provided the personnel or equipment.

(h) MISSION; ESTABLISHMENT OF PERFORMANCE METRICS.—The Secretary shall—

(1) using leading practices in performance management and lessons learned by other law enforcement task forces and joint operations, establish—

(A) the mission, strategic goals, and objectives of each Joint Task Force;

(B) the criteria for terminating each Joint Task Force; and

(C) outcome-based and other appropriate performance metrics for evaluating the effectiveness of each Joint Task Force with respect to the mission, strategic goals, and objectives established pursuant to subparagraph (A), including—

(i) targets for each Joint Task Force to achieve by not later than 1 and 3 years after the establishment under this paragraph; and

(ii) a description of the methodology used to establish the metrics.

(2) not later than 120 days after December 23, 2022, and 120 days after the establishment of a new Joint Task Force, as appropriate, submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate the mission, strategic goals, objectives, and metrics established under paragraph (1); and

(3) not later than December 23, 2023, and annually thereafter, submit to the committees specified in paragraph (2) a report that contains information on the progress in implementing the outcome-based and other appropriate performance metrics established pursuant to paragraph (1)(C).

(i) JOINT DUTY TRAINING PROGRAM.—

(1) IN GENERAL.—The Secretary shall—

(A) establish a joint duty training program in the Department for the purposes of—

(i) enhancing coordination in the Department; and

(ii) promoting workforce professional development; and

(B) tailor the joint duty training program to improve joint operations as part of the Joint Task Forces.

(2) ELEMENTS.—The joint duty training program established under paragraph (1) shall address, at a minimum, the following topics:

(A) National security strategy.

(B) Strategic and contingency planning.

(C) Command and control of operations under joint command.

(D) International engagement.

(E) The homeland security enterprise.

(F) Interagency collaboration.

(G) Leadership.

(H) Specific subject matters relevant to the Joint Task Force, including matters relating to the missions specified in section 10312 of this title, to which the joint duty training program is assigned.

(3) TRAINING REQUIRED.—

(A) DIRECTORS AND DEPUTY DIRECTORS.—Except as provided in subparagraphs (C) and (D), an individual shall complete the joint duty training program before being appointed Director or Deputy Director of a Joint Task Force.

(B) STAFF.—Each official serving on the staff of a Joint Task Force shall complete the joint duty training program in the 1st year of assignment to the Joint Task Force.

(C) EXCEPTION.—Subparagraph (A) does not apply to the 1st Director or Deputy Director appointed to a Joint Task Force on or after December 23, 2016.

(D) WAIVER.—The Secretary may waive the application of subparagraph (A) if the Secretary determines that the waiver is in the interest of homeland security or necessary to carry out the mission for which a Joint Task Force was established.

(j) NOTIFICATION OF JOINT TASK FORCE FORMATION OR TERMINATION.—

(1) IN GENERAL.—Not later than 7 days after establishing or terminating a Joint Task Force under this section, the Secretary shall submit to the majority leader of the Senate, the minority leader of the Senate, The Speaker of the House of Representatives, the majority leader of the House of Representatives, the minority leader of the

House of Representatives, the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a notification regarding the establishment or termination. The contents of the notification shall include the following:

(A) The criteria and conditions required to establish or terminate the Joint Task Force at issue.

(B) The primary mission, strategic goals, objectives, and plan of operations of the Joint Task Force.

(C) If the notification is a notification of termination, information on the effectiveness of the Joint Task Force as measured by the outcome-based performance metrics and other appropriate performance metrics established pursuant to subsection (h)(1)(C).

(D) The funding and resources required to establish or terminate the Joint Task Force.

(E) The number of personnel of each component or office permanently assigned to the Joint Task Force.

(F) The number of personnel of each component and office assigned on a temporary basis to the Joint Task Force.

(G) If the notification is a notification of establishment, the anticipated costs of establishing and operating the Joint Task Force.

(H) If the notification is a notification of termination, funding allocated in the immediately preceding fiscal year to the Joint Task Force for—

(i) operations, notwithstanding the termination; and

(ii) activities associated with the termination.

(I) The anticipated establishment or actual termination date of the Joint Task Force, as the case may be.

(2) WAIVER AUTHORITY.—The Secretary may waive the requirement under paragraph (1) in the event of an emergency circumstance that imminently threatens the protection of human life or property.

(k) REVIEW.—Not later than December 23, 2023, the Comptroller General shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate an assessment of the effectiveness of the Secretary's utilization of the authority provided under this section for the purposes specified in subsection (d) as among the range of options available to the Secretary to con-

duct joint operations among department components and offices and a review of the Joint Task Forces established under this section. The review shall include—

(1) an assessment of methodology utilized to determine whether to establish or determine each Joint Task Force; and

(2) an assessment of the effectiveness of oversight over each Joint Task Force, with specificity regarding the Secretary's utilization of outcome-based or other appropriate performance metrics (established pursuant to subsection (h)(1)(C)) to evaluate the effectiveness of each Joint Task Force in measuring progress with respect to the mission, strategic goals, and objectives (established pursuant to subsection (h)(1)(A)) of the Joint Task Force.

(l) JOINT DUTY ASSIGNMENT PROGRAM.—After establishing the joint duty training program under subsection (i), the Secretary shall establish a joint duty assignment program in the Department for the purposes of enhancing coordination in the Department and promoting workforce professional development.

(m) SUNSET.—This section expires on September 30, 2024.

§ 11709. Office of Strategy, Policy, and Plans

(a) IN GENERAL.—The Under Secretary for Strategy, Policy, and Plans is the principal policy advisor to the Secretary.

(b) FUNCTIONS.—The Under Secretary for Strategy, Policy, and Plans shall—

(1) lead, conduct, and coordinate Department-wide policy development and implementation and strategic planning;

(2) develop and coordinate policies to promote and ensure quality, consistency, and integration for the programs, components, offices, and activities across the Department;

(3) develop and coordinate strategic plans and long-term goals of the Department with risk-based analysis and planning to improve operational mission effectiveness, including consultation with the Secretary regarding the quadrennial homeland security review under section 11706 of this title;

(4) manage Department leadership councils and provide analytics and support to the councils;

(5) manage international coordination and engagement for the Department;

(6) review and incorporate, as appropriate, external stakeholder feedback into Department policy; and

(7) carry out such other responsibilities as the Secretary determines appropriate.

(c) COORDINATION BY DEPARTMENT COMPONENTS.—To ensure consistency with the policy priorities of the Department, the head of each component of the Department shall coordinate with the Office of Strategy, Policy, and Plans in establishing or modifying policies or strategic planning guidance with respect to each component.

(d) HOMELAND SECURITY STATISTICS AND JOINT ANALYSIS.—

(1) HOMELAND SECURITY STATISTICS.—The Under Secretary for Strategy, Policy, and Plans shall—

(A) establish standards of reliability and validity for statistical data collected and analyzed by the Department;

(B) be provided by the heads of all components of the Department with statistical data maintained by the Department regarding the operations of the Department.

(C) conduct or oversee analysis and reporting of the data by the Department as required by law or as directed by the Secretary; and

(D) ensure the accuracy of metrics and statistical data provided to Congress.

(2) TRANSFER OF RESPONSIBILITIES.—There shall be transferred to the Under Secretary for Strategy, Policy, and Plans the maintenance of all immigration statistical information of U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Citizenship and Immigration Services, which shall include information and statistics of the type contained in the publication entitled ''Yearbook of Immigration Statistics'' prepared by the Office of Immigration Statistics, including region-by-region statistics on the aggregate number of applicants and petitions filed by an alien (or filed on behalf of an alien) and denied, and the reasons for the denial, disaggregated by category of denial and application or petition type.

(e) LIMITATION.—Nothing in this section overrides or otherwise affects the requirements specified in section 10312 of this title.

§ 11710. Employee engagement

(a) STEERING COMMITTEE.—Not later than 120 days after December 27, 2021, the Secretary shall establish an employee engagement steering committee, including representatives from operational components, headquarters, and field personnel, including supervisory and nonsupervisory personnel, and employee labor organizations that represent Department employees, and chaired by the Under Secretary for Management, to carry out the following activities:

(1) Identify factors that have a negative impact on employee engagement, morale, and communications in the Department, such as percep-

tions about limitations on career progression, mobility, or development opportunities, collected through employee feedback platforms, including through annual employee surveys, questionnaires, and other communications, as appropriate.

(2) Identify, develop, and distribute initiatives and best practices to improve employee engagement, morale, and communications in the Department, including through annual employee surveys, questionnaires, and other communications, as appropriate.

(3) Monitor efforts of each component to address employee engagement, morale, and communications based on employee feedback provided through annual employee surveys, questionnaires, and other communications, as appropriate.

(4) Advise the Secretary on efforts to improve employee engagement, morale, and communications in specific components and across the Department.

(5) Conduct regular meetings and report, not less than once per quarter, to the Under Secretary for Management, the head of each component, and the Secretary on Departmentwide efforts to improve employee engagement, morale, and communications.

(b) ACTION PLAN; REPORTING.—The Secretary, acting through the Chief Human Capital Officer, shall—

(1) not later than 120 days after the date of the establishment of the employee engagement steering committee under subsection (a), issue a Departmentwide employee engagement action plan, reflecting input from the steering committee and employee feedback provided through annual employee surveys, questionnaires, and other communications in accordance with subsection(a)(1), to execute strategies to improve employee engagement, morale, and communications in the Department; and

(2) require the head of each component to—

(A) develop and implement a component-specific employee engagement plan to advance the action plan required under paragraph (1) that includes performance measures and objectives, is informed by employee feedback provided through annual employee surveys, questionnaires, and other communications, as appropriate, and sets forth how employees and, where applicable, their labor representatives are to be integrated in developing programs and initiatives;

(B) monitor progress on implementation of the action plan; and

(C) provide to the Chief Human Capital Officer and the steering committee quarterly reports on actions planned and progress made under this paragraph.

(c) TERMINATION.—This section shall terminate on December 27, 2026.

§ 11711. Acquisition professional career program

(a) DEFINITIONS.—In this section:

(1) HISPANIC-SERVING INSTITUTION.— The term ''Hispanic-serving institution'' has the meaning given that term insection 502 of the Higher Education Act of 1965 (20 U.S.C. 1101a).

(2) HISTORICALLY BLACK COLLEGES AND UNIVERSITIES.—The term ''historically Black colleges and universities'' has the meaning given the term ''part B institution'' in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

(3) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given that term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

(b) ESTABLISHMENT.—There is in the Department an acquisition professional career program to develop a cadre of acquisition professionals within the Department.

(c) ADMINISTRATION.—The Under Secretary for Management shall administer the acquisition professional career program established pursuant to subsection (a).

(d) PROGRAM REQUIREMENTS.—The Under Secretary for Management shall carry out the following with respect to the acquisition professional career program:

(1) Designate the occupational series, grades, and number of acquisition positions throughout the Department to be included in the program and manage centrally those positions.

(2) Establish and publish on the Department's website eligibility criteria for candidates to participate in the program.

(3) Carry out recruitment efforts to attract candidates—

(A) from institutions of higher education, including those institutions with established acquisition specialties and courses of study, historically Black colleges and universities, and Hispanic-serving institutions;

(B) with diverse work experience outside of the Federal Government; or

(C) with military service.

(4) Hire eligible candidates for designated positions under the program.

(5) Develop a structured program comprised of acquisition training, on-the-job experience, Department-wide rotations, mentorship, shadowing, and other career development opportunities for program participants.

(6) Provide, beyond required training established for program participants, additional specialized acquisition training, including small business contracting and innovative acquisition techniques training.

(e) REPORTS.—Not later than December 27, 2022, and annually thereafter through 2027, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the acquisition professional career program. Each report shall include the following information:

(1) The number of candidates approved for the program.

(2) The number of candidates who commenced participation in the program, including generalized information on the candidates' backgrounds with respect to education and prior work experience, but not including personally identifiable information.

(3) A breakdown of the number of participants hired under the program by type of acquisition position.

(4) A list of Department components and offices that participated in the program and information regarding length of time of each program participant in each rotation at the components or offices.

(5) Program attrition rates and post-program graduation retention data, including information on how the data compare to the prior year's data, as available.

(6) The Department's recruiting efforts for the program.

(7) The Department's efforts to promote retention of program participants.

Chapter 119—Coordination With Other Entities

Sec.

§ 11901. Responsibilities of Office for State and Local Government Coordination

The Office for State and Local Government Coordination oversees and coordinates departmental programs for and relationships with State and local governments. The Office shall—

(1) coordinate the activities of the Department relating to State and local government;

(2) assess, and advocate for, the resources needed by State and local government to implement the national strategy for combating terrorism;

(3) provide State and local government with regular information, research, and technical support to assist local efforts at securing the homeland; and

(4) develop a process for receiving meaningful input from State and local government to assist the development of the national strategy for combating terrorism and other homeland security activities.

§ 11902. Responsibilities of Office for National Capital Region Coordination

(a) IN GENERAL.—The Office for National Capital Region Coordination oversees and coordinates Federal programs for and relationships with State, local, and regional authorities in the National Capital Region, as defined under section 2674(f)(2) of title 10.

(b) COOPERATION WITH NATIONAL CAPITAL REGION OFFICIALS.—

(1) IN GENERAL.—The Secretary shall cooperate with the Mayor of the District of Columbia, the Governors of Maryland and Virginia, and other State, local, and regional officers in the National Capital Region to integrate the District of Columbia, Maryland, and Virginia into the planning, coordination, and execution of the activities of the Federal Government for the enhancement of domestic preparedness against the consequences of terrorist attacks.

(2) INCORPORATION OF GOVERNORS OF WEST VIRGINIA AND PENNSYLVANIA.—For purposes of planning, coordination, execution, and decision making related to mass evacuation during a disaster, the Governors of Pennsylvania, or their designees, shall be incorporated into efforts to integrate the activities of Federal, State, and local governments in the National Capital Region.

(c) RESPONSIBILITIES.—The Office for National Capital Region Coordination shall—

(1) coordinate the activities of the Department relating to the National Capital Region, including cooperation with the Office for State and Local Government Coordination;

(2) assess, and advocate for, the resources needed by State, local, and regional authorities in the National Capital Region to implement efforts to secure the homeland;

(3) provide State, local, and regional authorities in the National Capital Region with regular information, research, and technical support to assist the efforts of State, local, and regional authorities in the National Capital Region in securing the homeland;

(4) develop a process for receiving meaningful input from State, local, and regional authorities and the private sector in the National Capital Region to assist in the development of the homeland security plans and activities of the Federal Government;

(5) coordinate with Federal agencies in the National Capital Region on terrorism preparedness, to ensure adequate planning, information sharing, training, and execution of the Federal role in domestic preparedness activities;

(6) coordinate with Federal, State, local, and regional agencies, and the private sector in the National Capital Region on terrorism preparedness to ensure adequate planning, information sharing, training, and execution of domestic preparedness activities among these agencies and entities; and

(7) serve as a liaison between the Federal Government and State, local, and regional authorities, and private-sector entities in the National Capital Region to facilitate access to Federal grants and other programs.

(d) ANNUAL REPORT.—The Office for National Capital Region Coordination shall submit an annual report to Congress that includes—

(1) the identification of the resources required to fully implement homeland security efforts in the National Capital Region;

(2) an assessment of the progress made by the National Capital Region in implementing homeland security efforts; and

(3) recommendations to Congress regarding the additional resources needed to fully implement homeland security efforts in the National Capital Region.

(e) LIMITATION.—Nothing contained in this section shall be construed as limiting the power of State and local governments.

§ 11903. Joint Interagency Task Force

The Secretary may establish and operate a permanent Joint Interagency Homeland Security Task Force composed of representatives from military and civilian agencies of the United States Government for the purposes of anticipating terrorist threats against the United States and taking appropriate actions to prevent harm to the United States.

§ 11904. Coordination with Department of Health and Human Services under the Public Health Service Act

(a) IN GENERAL.—The annual Federal response plan developed by the Department shall be consistent with section 319 of the Public Health Service Act (42 U.S.C. 247d).

(b) DISCLOSURES AMONG RELEVANT AGENCIES.—

(1) IN GENERAL.—Full disclosure among relevant agencies shall be made under this subsection.

(2) PUBLIC HEALTH EMERGENCY.—During the period in which the Secretary of Health and Human Services has declared the existence of a public health emergency under section 319(a) of the Public Health Service Act (42 U.S.C. 247d(a)), the Secretary of Health and Human Services shall keep relevant agencies, including the Department, the Department of Justice, and the Federal Bureau of Investigation, fully and currently informed.

(3) POTENTIAL PUBLIC HEALTH EMERGENCY.—In cases involving, or potentially involving, a public health emergency, but in which no determination of an emergency by the Secretary of Health and Human Services under section 319(a) of the Public Health Service Act (42 U.S.C. 247d(a)) has been made, all relevant agencies, including the Department, the Department of Justice, and the Federal Bureau of Investigation, shall keep the Secretary of Health and Human Services and the Director of the Centers for Disease Control and Prevention fully and currently informed.

§ 11905. Aviation security

(a) CONSULTATION WITH FEDERAL AVIATION ADMINISTRATION.—The Secretary and other officials in the Department shall consult with the Administrator of the Federal Aviation Administration before taking an action that might affect aviation safety, air carrier operations, aircraft airworthiness, or the use of airspace. The Secretary shall establish a liaison office in the Department to consult with the Administrator of the Federal Aviation Administration.

(b) LIMITATIONS ON STATUTORY CONSTRUCTION.—

(1) GRANT OF AUTHORITY.—Nothing in this subtitle may be construed to vest in the Secretary or another official in the Department authority over transportation security that is not vested in the Administrator of the Transportation Security Administration, or that was not vested in the Secretary of Transportation under chapter 449 of title 49 on November 24, 2002.

(2) OBLIGATION OF AIRPORT IMPROVEMENT PROGRAM FUNDS.—Nothing in this subtitle may be construed to authorize the Secretary or any other official in the Department to obligate amounts made available under section 48103 of title 49.

§ 11906. Investigation of violent acts, shootings, and mass killings

(a) DEFINITIONS.—In this section:

(1) MASS KILLINGS.—The term ''mass killings'' means 3 or more killings in a single incident.

(2) PLACE OF PUBLIC USE.—The term ''place of public use'' has the meaning given the term under section 2332f(e)(6) of title 18.

(b) PROVIDING ASSISTANCE.—At the request of an appropriate law enforcement official of a State or political subdivision, the Secretary, through deployment of the Secret Service or U.S. Immigration and Customs Enforcement, may assist in the investigation of violent acts and shootings occurring in a place of public use, and in the investigation of mass killings and attempted mass killings. Any assistance provided by the Secretary under this subsection shall be presumed to be within the scope of a Federal office or of Federal employment.

§ 11907. Facilitating homeland security information sharing procedures

(a) DEFINITIONS.—In this section:

(1) HOMELAND SECURITY INFORMATION.—The term ''homeland security information'' means information possessed by a Federal, State, or local agency that—

(A) relates to the threat of terrorist activity;

(B) relates to the ability to prevent, interdict, or disrupt terrorist activity;

(C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or

(D) would improve the response to a terrorist act.

(2) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(3) STATE AND LOCAL PERSONNEL.—The term ''State and local personnel'' means any of the following persons involved in the prevention of, preparation for, or response to terrorist attack:

(A) State Governors, mayors, and other locally elected officials.

(B) State and local law enforcement personnel and firefighters.

(C) Public health and medical professionals.

(D) Regional, State, and local emergency management agency personnel, including State adjutant generals.

(E) Other appropriate emergency response agency personnel.

(F) Employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed under this section.

(b) PROCEDURES FOR DETERMINING EXTENT OF SHARING OF HOMELAND SECURITY INFORMATION.—

(1) ESTABLISHMENT OF PROCEDURES.—The President shall prescribe and implement procedures under which relevant Federal agencies—

(A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel;

(B) identify and safeguard homeland security information that is sensitive but unclassified; and

(C) to the extent the information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which personnel it may be shared after the information is removed.

(2) APPLICABILITY.—The President shall ensure that the procedures apply to all agencies of the Federal Government.

(3) NO CHANGE IN SUBSTANTIVE REQUIREMENTS.—The procedures shall not change the substantive requirements for the classification and safeguarding of classified information.

(4) NO CHANGE IN PROTECTIVE AUTHORITIES.—The procedures shall not change the requirements and authorities to protect sources and methods.

(c) PROCEDURES FOR SHARING OF HOMELAND SECURITY INFORMATION.—

(1) IN GENERAL.—Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent the information may be shared, as determined under subsection (b), together with assessments of the credibility of the information.

(2) SYSTEM CAPABILITIES.—Each information sharing system through which information is shared under paragraph (1) shall—

(A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ;

(B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know the information;

(C) be configured to allow the efficient and effective sharing of information; and

(D) be accessible to appropriate State and local personnel.

(3) USE CONDITIONS.—The procedures prescribed under paragraph (1) shall establish conditions on the use of information shared under paragraph (1)—

(A) to limit the re-dissemination of the information to ensure that the information is not used for an unauthorized purpose;

(B) to ensure the security and confidentiality of the information;

(C) to protect the constitutional and statutory rights of individuals who are subjects of the information; and

(D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(4) INCLUSION OF EXISTING SYSTEMS.—The procedures prescribed under paragraph (1) shall ensure, to the greatest extent practicable, that the information sharing system through which information is shared under that paragraph include existing information sharing systems, including the National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation.

(5) AGENCY ACCESS.—Each appropriate Federal agency, as determined by the President, shall have access to each information sharing system through which information is shared under paragraph (1), and shall therefore have access to all information, as appropriate, shared under that paragraph.

(6) SHARING INFORMATION.—The procedures prescribed under paragraph (1) shall ensure that appropriate State and local personnel are authorized to use the information sharing systems—

(A) to access information shared with the personnel; and

(B) to share, with others who have access to the information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.

(7) ASSESSMENT AND INTEGRATION OF INFORMATION.—Under procedures prescribed jointly by the Director of National Intelligence and the Attorney General, each appropriate Federal agency, as determined by the President, shall review and assess the information shared under paragraph (6) and integrate the information with existing intelligence.

(d) SHARING OF CLASSIFIED INFORMATION AND SENSITIVE BUT UNCLASSIFIED INFORMATION WITH STATE AND LOCAL PERSONNEL.—

(1) IN GENERAL.—The President shall prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate State and local personnel homeland security information that remains classified or otherwise protected after the determinations prescribed under the procedures set forth in subsection (b) are made.

(2) TRAINING PROGRAM.—

(A) ESTABLISHMENT.—The Secretary shall establish a program to provide appropriate training to officials described in subparagraph (B) in order to assist the officials in—

(i) identifying sources of potential terrorist threats through the methods the Secretary determines are appropriate;

(ii) reporting information relating to the potential terrorist threats to the appropriate Federal agencies in the appropriate form and manner;

(iii) assuring that all reported information is systematically submitted to and passed on by the Department for use by appropriate Federal agencies; and

(iv) understanding the mission and roles of the intelligence community to promote more effective information sharing among Federal, State, and local officials and representatives of the private sector to prevent terrorist attacks against the United States.

(B) TRAINING COVERAGE.—The officials referred to in subparagraph (A) are officials of State and local government agencies and representatives of private-sector entities with responsibilities relating to the oversight and management of first responders, counterterrorism activities, or critical infrastructure.

(C) CONSULTATION WITH ATTORNEY GENERAL.—The Secretary shall consult with the Attorney General to ensure that the training program established in subparagraph (A) does not duplicate the training program established in section 908 of the USA PATRIOT Act (Public Law 107–56, 28 U.S.C. 509 note).

(D) OTHER CONSULTATION.—The Secretary shall carry out this paragraph in consultation with the Director of National Intelligence and the Attorney General.

(e) RESPONSIBLE OFFICIALS.—For each affected Federal agency, the head of the agency shall designate an official to administer this subtitle with respect to the agency.

(f) FEDERAL CONTROL OF INFORMATION.—Under procedures prescribed under this section, information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring a government to disclose information shall not apply to the information.

(g) CONSTRUCTION.—Nothing in this subtitle shall be construed as authorizing a department, bureau, agency, officer, or employee of the Federal Government to request, receive, or transmit to another Government entity or any Government personnel, or transmit to a State or local entity or State or local personnel otherwise authorized by the Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2135) to receive homeland security information, information collected by the Federal Government solely for statistical purposes in violation of any other provision of law relating to the confidentiality of the information.

§ 11908. Information sharing

(a) DEFINITIONS.—In this section:

(1) HOMELAND SECURITY INFORMATION.—The term ''homeland security information'' has the meaning given the term in section 11907(a) of this title.

(2) INFORMATION SHARING COUNCIL.—The term ''Information Sharing Council'' means the Information Sharing Council established by Executive Order 13388 (Oct. 25, 2005, 70 F.R. 62023), or any successor body designated by the President, and referred to under subsection (e).

(3) INFORMATION SHARING ENVIRONMENT; ISE.—The terms ''information sharing environment'' and ''ISE'' mean an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section.

(4) PROGRAM MANAGER.—The term ''program manager'' means the program manager designated under subsection (d).

(5) TERRORISM INFORMATION.—The term ''terrorism information''—

(A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

(i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

(ii) threats posed by these groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

(iii) communications of or by these groups or individuals; or

(iv) other groups or individuals reasonably believed to be assisting or associated with these groups or individuals; and

(B) includes weapons of mass destruction information.

(6) WEAPONS OF MASS DESTRUCTION INFORMATION.—The term ''weapons of mass destruction information'' means information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States, including information about the location of a stockpile of nuclear materials that could be exploited for use in a weapon that could be used by a terrorist or a terrorist organization against the United States.

(b) INFORMATION SHARING ENVIRONMENT.—

(1) ESTABLISHMENT.—The President shall—

(A) create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties;

(B) designate the organizational and management structures that will be used to operate and manage the ISE; and

(C) determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.

(2) ATTRIBUTES.—The President shall, through the structures described in subparagraphs (B) and (C) of paragraph (1), ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The President shall, to the greatest extent practicable, ensure

that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that—

(A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;

(B) ensures direct and continuous online electronic access to information;

(C) facilitates the availability of information in a form and manner that makes easier its use in analysis, investigations, and operations;

(D) builds upon existing systems capabilities currently in use across the Government;

(E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;

(F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals' privacy and civil liberties;

(I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls;

(J) integrates the information within the scope of the information sharing environment, including information in legacy technologies;

(K) integrates technologies, including all legacy technologies, through Internet-based services, consistent with appropriate security protocols and safeguards, to enable connectivity among required users at the Federal, State, and local levels;

(L) allows the full range of analytic and operational activities without the need to centralize information within the scope of the information sharing environment;

(M) permits analysts to collaborate both independently and in a group (commonly known as ''collective and noncollective collaboration''), and across multiple levels of national security information and controlled unclassified information;

(N) provides a resolution process that enables changes by authorized officials regarding rules and policies for the access, use,

and retention of information within the scope of the information sharing environment; and

(O) incorporates continuous, real-time, and immutable audit capabilities, to the maximum extent practicable.

(3) DELEGATION.—The President may delegate responsibility for carrying out this subsection, except that the President may not delegate that responsibility to the Director of National Intelligence.

(c) GUIDELINES AND REQUIREMENTS.—The President shall—

(1) leverage all ongoing efforts consistent with establishing the ISE and issue guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained;

(2) in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee), issue guidelines that—

(A) protect privacy and civil liberties in the development and use of the ISE; and

(B) shall be made public, unless nondisclosure is clearly necessary to protect national security; and

(3) require the heads of Federal departments and agencies to promote a culture of information sharing by—

(A) reducing disincentives to information sharing, including over-classification of information and unnecessary requirements for originator approval, consistent with applicable laws and regulations; and

(B) providing affirmative incentives for information sharing.

(d) PROGRAM MANAGER.—

(1) DESIGNATION.—Each individual designated as the program manager shall be appointed by the Director of National Intelligence. The program manager, in consultation with the head of an affected department or agency, shall have and exercise Government-wide authority over the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by all Federal departments, agencies, and components, irrespective of the Federal department, agency, or component in which the program manager may be administratively located, except as otherwise expressly provided by law.

(2) DUTIES AND RESPONSIBILITIES.—

(A) IN GENERAL.—The program manager shall, in consultation with the Information Sharing Council—

(i) plan for and oversee the implementation of, and manage, the ISE;

(ii) assist in the development of policies, as appropriate, to foster the development and proper operation of the ISE;

(iii) consistent with the direction and policies issued by the President, the Director of National Intelligence, and the Director of the Office of Management and Budget, issue Government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE;

(iv) identify and resolve information sharing disputes between Federal departments, agencies, and components; and

(v) assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency, and policy compliance; and regularly report the findings to Congress.

(B) CONTENT OF POLICIES, PROCEDURES, GUIDELINES, INSTRUCTIONS, AND STANDARDS.—The policies, procedures, guidelines, instructions, and standards under clauses (ii) and (iii) of subparagraph (A) shall—

(i) take into account the varying missions and security requirements of agencies participating in the ISE;

(ii) address development, implementation, and oversight of technical standards and requirements;

(iii) take into account ongoing and planned efforts that support development, implementation, and management of the ISE;

(iv) address and facilitate information sharing between and among departments and agencies of the intelligence community, the Department of Defense, the homeland security community, and the law enforcement community;

(v) address and facilitate information sharing between Federal departments and agencies and State, tribal, and local governments;

(vi) address and facilitate, as appropriate, information sharing between Federal departments and agencies and the private sector;

(vii) address and facilitate, as appropriate, information sharing between Federal departments and agencies with foreign partners and allies; and

(viii) ensure the protection of privacy and civil liberties.

(e) INFORMATION SHARING COUNCIL.—

(1) ESTABLISHMENT.—There is in the Department the Information Sharing Council that assists the President and the program manager in their duties under this section. The Information Sharing Council serves until removed from service or replaced by the President (at the sole discretion of the President) with a successor body.

(2) SPECIFIC DUTIES.—In assisting the President and the program manager in their duties under this section, the Information Sharing Council shall—

(A) advise the President and the program manager in developing policies, procedures, guidelines, instructions, and standards necessary to establish, implement, and maintain the ISE;

(B) work to ensure coordination among the Federal departments and agencies participating in the ISE in the establishment, implementation, and maintenance of the ISE;

(C) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used by Federal departments and agencies to share information, and recommend, as appropriate, the redirection of existing resources to support the ISE;

(D) identify gaps, if any, between existing technologies, programs, and systems used by Federal departments and agencies to share information and the parameters of the proposed information sharing environment;

(E) recommend solutions to address gaps identified under subparagraph (D);

(F) recommend means by which the ISE can be extended to allow interchange of information between Federal departments and agencies and appropriate authorities of State and local governments;

(G) assist the program manager in identifying and resolving information sharing disputes between Federal departments, agencies, and components;

(H) identify appropriate personnel for assignment to the program manager to support staffing needs identified by the program manager; and

(I) recommend whether or not, and by which means, the ISE should be expanded so as to allow future expansion encompassing other relevant categories of information.

(3) CONSULTATION.—In performing its duties, the Information Sharing Council shall consider input from persons and entities outside the Federal Government having significant experience and expertise in policy, technical matters, and operational matters relating to the ISE.

(4) INAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—The Information Sharing Council (including a subsidiary group of the Council) is not subject to the requirements of chapter 10 of title 5.

(5) DETAILEES.—On a request by the Director of National Intelligence, the departments and agencies represented on the Information Sharing Council shall detail to the program manager, on a reimbursable basis, appropriate personnel identified under paragraph (2)(H).

(f) AGENCY RESPONSIBILITIES.—The head of each department or agency that possesses or uses intelligence or terrorism information, operates a system in the ISE, or otherwise participates (or expects to participate) in the ISE shall—

(1) ensure full department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards established under subsections (b) and (d);

(2) ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE;

(3) ensure full department or agency cooperation in the development of the ISE to implement Government-wide information sharing; and

(4) submit, at the request of the President or the program manager, reports on the implementation of the requirements of the ISE within the department or agency.

(g) ADDITIONAL POSITIONS.—The program manager may hire not more than 40 full-time employees to assist the program manager in—

(1) activities associated with the implementation of the information sharing environment, including—

(A) implementing the requirements under subsection (b)(2); and

(B) any additional implementation initiatives to enhance and expedite the creation of the information sharing environment; and

(2) identifying and resolving information sharing disputes between Federal departments, agencies, and components under subsection (d)(2)(A)(iv).

§ 11909. Prohibition of Terrorism Information and Prevention System

All activities of the Federal Government to implement the proposed component program of the Citizen Corps Division known as Operation TIPS (Terrorism Information and Prevention System) are prohibited.

§ 11910. Prevention of international child abduction

(a) PROGRAM ESTABLISHED.—The Secretary, through the Commissioner of U.S. Customs and Border Protection, in coordination with the Secretary of State, the Attorney General, and the Director of the Federal Bureau of Investigation, shall establish a program that—

(1) seeks to prevent a child (as defined in section 1204(b)(1) of title 18) from departing from the territory of the United States if a parent or legal guardian of the child presents a court order from a court of competent jurisdiction prohibiting the removal of the child from the United States to a U.S. Customs and Border Protection Officer in sufficient time to prevent the departure for the duration of the court order; and

(2) leverages other existing authorities and processes to address the wrongful removal and return of a child.

(b) INTERAGENCY COORDINATION.—

(1) IN GENERAL.—The Secretary of State shall convene and chair an interagency working group to prevent international parental child abduction. The group shall be composed of presidentially appointed, Senate-confirmed officials from—

(A) the Department of State;

(B) the Department of Homeland Security, including U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement; and

(C) the Department of Justice, including the Federal Bureau of Investigation.

(2) DEPARTMENT OF DEFENSE.—The Secretary of Defense shall designate an official in the Department of Defense—

(A) to coordinate with the Department of State on international child abduction issues; and

(B) to oversee activities designed to prevent or resolve international child abduction cases relating to active duty military service members.

§ 11911. Limitation of liability

A person who has completed a security awareness training course approved by or operated under a cooperative agreement with the Department, who is enrolled in a program recognized or acknowledged by an Information

Sharing and Analysis Center and who reports a situation, activity, or incident pursuant to that program to an appropriate authority, shall not be liable for damages in an action brought in a Federal or State court which result from an act or omission unless the person is guilty of gross negligence or willful misconduct.

§ 11912. Transnational Criminal Investigative Units

(a) IN GENERAL.—The Secretary, with the concurrence of the Secretary of State, shall operate Transnational Criminal Investigative Units within Homeland Security Investigations.

(b) COMPOSITION.—Each Transnational Criminal Investigative Unit shall be composed of trained foreign law enforcement officials who shall collaborate with Homeland Security Investigations to investigate and prosecute individuals involved in transnational criminal activity.

(c) VETTING REQUIREMENT.—

(1) IN GENERAL.—Before entry into a Transnational Criminal Investigative Unit, and at periodic intervals while serving in a Transnational Criminal Investigate Unit, foreign law enforcement officials shall be required to pass certain security evaluations, which may include a background check, a polygraph examination, a urinalysis test, or other measures that the Secretary determines to be appropriate.

(2) LEAHY VETTING REQUIRED.—No member of a foreign law enforcement unit may join a Transnational Criminal Investigative Unit if the Secretary, in coordination with the Secretary of State, has credible information that the foreign law enforcement unit has committed a gross violation of human rights, consistent with the limitations set forth insection 620M of the Foreign Assistance Act of 1961 (22 U.S.C. 2378d).

(3) APPROVAL AND CONCURRENCE.— The establishment and continued support of the Transnational Criminal Investigative Units that are assigned under paragraph (1)—

(A) shall be performed with the approval of the chief of mission to the foreign country to which the personnel are assigned;

(B) shall be consistent with the duties and powers of the Secretary of State and the chief of mission for a foreign country undersection 103 of the Diplomatic Security Act (22 U.S.C. 4802) andsection 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927), respectively; and

(C) shall not be established without the concurrence of the Assistant Secretary of State for International Narcotics and Law Enforcement Affairs.

(4) REPORT.—The Executive Associate Director of Homeland Security Investigations shall submit a report to the Committee on Foreign Relations of the Senate, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on the Judiciary of the Senate, the Committee on Foreign Affairs of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the Committee on the Judiciary of the House of Representatives that describes—

(A) the procedures used for vetting Transnational Criminal Investigative Unit members to include compliance with the vetting required under this subsection; and

(B) any additional measures that should be implemented to prevent personnel in vetted units from being compromised by criminal organizations.

(d) MONETARY STIPEND.—The Executive Associate Director of Homeland Security Investigations may pay vetted members of a Transnational Criminal Investigative Unit a monetary stipend in an amount associated with their duties dedicated to unit activities.

(e) ANNUAL BRIEFING.—The Executive Associate Director of Homeland Security Investigations, during the 5-year period beginning on December 23, 2022, shall provide an annual unclassified briefing to the congressional committees referred to in subsection (c)(4), which may include a classified session, if necessary, that identifies—

(1) the number of vetted members of Transnational Criminal Investigative Unit in each country;

(2) the amount paid in stipends to the members, disaggregated by country;

(3) relevant enforcement statistics, such as arrests and progress made on joint investigations, in each country; and

(4) whether any vetted members of the Transnational Criminal Investigative Unit in each country were involved in any unlawful activity, including human rights abuses or significant acts of corruption.

§ 11913. Reciprocal information sharing with foreign government

Acting in accordance with a bilateral or multilateral arrangement, the Secretary, in the Secretary's discretion and on the basis of reciprocity, may provide information from the National Sex Offender Registry relating to a conviction for a sex offense against a minor (as the terms are defined in section 111 of the Sex Offender Registration and Notification Act (34 U.S.C. 20911)to a foreign government on the request of the foreign govern-

ment, and may receive comparable information from the foreign government.

Chapter 121—Homeland Security Council

§ 12101. Establishment

There is in the Executive Office of the President the Homeland Security Council to advise the President on homeland security matters.

§ 12102. Membership

(a) MEMBERS.—The members of the Homeland Security Council are the following:

(1) The President.

(2) The Vice President.

(3) The Secretary.

(4) The Attorney General.

(5) The Secretary of Defense.

(6) Other individuals who may be designated by the President.

(b) ATTENDANCE OF CHAIRMAN OF JOINT CHIEFS OF STAFF AT MEETINGS.—The Chairman of the Joint Chiefs of Staff (or, in the absence of the Chairman, the Vice Chairman of the Joint Chiefs of Staff) may, in the role of the Chairman of the Joint Chiefs of Staff as principal military adviser to the Homeland Security Council and subject to the direction of the President, attend and participate in meetings of the Council.

§ 12103. Functions and activities

To effectively coordinate the policies and functions of the United States Government relating to homeland security, the Homeland Security Council shall—

(1) assess the objectives, commitments, and risks of the United States in the interest of homeland security and make resulting recommendations to the President;

(2) oversee and review homeland security policies of the Federal Government and make resulting recommendations to the President; and

(3) perform other functions that the President may direct.

§ 12104. Staff

(a) HEADED BY EXECUTIVE SECRETARY.—The Homeland Security Council has a staff, the head of which is a civilian Executive Secretary appointed by the President.

(b) PAY OF EXECUTIVE SECRETARY.—The President shall fix the pay of the Executive Secretary at a rate not to exceed the rate of pay payable to the Executive Secretary of the National Security Council.

§ 12105. Joint meetings with National Security Council

The President may convene joint meetings of the Homeland Security Council and the National Security Council with participation by members of either Council or as the President may otherwise direct.

Chapter 123—Emergency Communications

Sec.

§ 12301. Definitions; rule of construction

(a) DEFINITIONS OF INTEROPERABLE COMMUNICATIONS AND INTEROPERABLE EMERGENCY COMMUNICATIONS.—In this chapter, the terms ''interoperable communications'' and ''interoperable emergency communications'' have the meaning given the term ''interoperable communications'' under section 10912(a) of this title.

(b) RULE OF CONSTRUCTION.—Nothing in this chapter or in sections 10913 or 10914 of this title shall be construed to transfer to the Office of Emergency Communications any function, personnel, asset, component, authority, grant program, or liability of the Federal Emergency Management Agency as constituted on June 1, 2006.

§ 12302. Responsibilities of Executive Assistant Director for Emergency Communications

(a) IN GENERAL.—The Executive Assistant Director for Emergency Communications shall—

(1) assist the Secretary in developing and implementing the program described in section 10912(b)(1) of this title, except as provided in section 10913 of this title;

(2) administer the Department's responsibilities and authorities relating to the SAFECOM Program, excluding elements related to research, development, testing, and evaluation and standards;

(3) administer the Department's responsibilities and authorities relating to the Integrated Wireless Network program;

(4) conduct extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government

officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(5) conduct extensive, nationwide outreach and foster the development of interoperable emergency communications capabilities by State, regional, local, and tribal governments and public safety agencies, and by regional consortia thereof;

(6) provide technical assistance to State, regional, local, and tribal government officials with respect to the use of interoperable emergency communications capabilities;

(7) coordinate with the Regional Administrators regarding the activities of Regional Emergency Communications Coordination Working Groups under section 12306 of this title;

(8) promote the development of standard operating procedures and best practices with respect to use of interoperable emergency communications capabilities for incident response, and facilitate the sharing of information on best practices for achieving, maintaining, and enhancing interoperable emergency communications capabilities for response;

(9) coordinate, in cooperation with the National Communications System, the establishment of a national response capability with initial and ongoing planning, implementation, and training for the deployment of communications equipment for relevant State, local, and tribal governments and emergency response providers in the event of a catastrophic loss of local and regional emergency communications services;

(10) assist the President, the National Security Council, the Homeland Security Council, and the Director of the Office of Management and Budget in ensuring the continued operation of the telecommunications functions and responsibilities of the Federal Government, excluding spectrum management;

(11) establish, in coordination with the Director of the Office for Interoperability and Compatibility, requirements for interoperable emergency communications capabilities, which shall be nonproprietary where standards for the capabilities exist, for all public safety radio and data communications systems and equipment purchased using homeland security assistance administered by the Department, excluding any alert and warning device, technology, or system;

(12) review, in consultation with the Assistant Secretary for Grants and Training, all interoperable emergency communications plans of Federal, State, local, and tribal governments, including statewide and tactical interoperability plans, developed pursuant to homeland security

assistance administered by the Department, but excluding spectrum allocation and management related to the plans;

(13) develop and update periodically, as appropriate, a National Emergency Communications Plan under section 12303 of this title;

(14) perform other duties of the Department necessary to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(15) perform other duties of the Department necessary to achieve the goal of, and maintain and enhance, interoperable emergency communications capabilities; and

(16) fully participate in the mechanisms required under section 10702(a)(1)(G) of this title.

(b) PERFORMANCE OF PREVIOUSLY TRANSFERRED FUNCTIONS.—The Secretary shall administer through the Executive Assistant Director for Emergency Communications the following programs and responsibilities:

(1) The SAFECOM Program, excluding elements related to research, development, testing, and evaluation and standards.

(2) The responsibilities of the Chief Information Officer related to the implementation of the Integrated Wireless Network.

(3) The Interoperable Communications Technical Assistance Program.

(c) COORDINATION.—The Executive Assistant Director for Emergency Communications shall coordinate—

(1) as appropriate, with the Director of the Office for Interoperability and Compatibility with respect to the responsibilities described in section 10913 of this title; and

(2) with the Administrator of the Federal Emergency Management Agency with respect to the responsibilities described in this chapter.

§ 12303. National Emergency Communications Plan

(a) IN GENERAL.—The Secretary, acting through the Assistant Director for Emergency Communications, and in cooperation with the National Communications System Office of the Department (as appropriate), shall, in cooperation with State, local, and tribal governments, Federal departments and agencies, emergency response providers, and the private sector, develop, and periodically update, a National Emergency Communications Plan to provide recommendations regarding how the United States should—

(1) support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(2) ensure, accelerate, and attain interoperable emergency communications nationwide.

(b) COORDINATION.—The Emergency Communications Preparedness Center under section 12307 of this title shall coordinate the development of the Federal aspects of the National Emergency Communications Plan.

(c) CONTENTS.—The National Emergency Communications Plan shall—

(1) include recommendations developed in consultation with the Federal Communications Commission and the National Institute of Standards and Technology for a process for expediting national voluntary consensus standards for emergency communications equipment for the purchase and use by public safety agencies of interoperable emergency communications equipment and technologies;

(2) identify the appropriate capabilities necessary for emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(3) identify the appropriate interoperable emergency communications capabilities necessary for Federal, State, local, and tribal governments in the event of natural disasters, acts of terrorism, and other man-made disasters;

(4) recommend both short-term and long-term solutions for ensuring that emergency response providers and relevant government officials can continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(5) recommend both short-term and long-term solutions for deploying interoperable emergency communications systems for Federal, State, local, and tribal governments throughout the Nation, including through the provision of existing and emerging technologies;

(6) identify how Federal departments and agencies that respond to natural disasters, acts of terrorism, and other man-made disasters can work effectively with State, local, and tribal governments, in all States, and with other entities;

(7) identify obstacles to deploying interoperable emergency communications capabilities nationwide and recommend short-term and long-term measures to overcome those obstacles, including recommendations for multijurisdictional coordination among Federal, State, local, and tribal governments;

(8) recommend goals and time frames for the deployment of emergency, command-level communications systems based on new and existing equipment across the United States and develop a timetable for the

deployment of interoperable emergency communications systems nationwide;

(9) recommend appropriate measures that emergency response providers should employ to ensure the continued operation of relevant governmental communications infrastructure in the event of natural disasters, acts of terrorism, or other man-made disasters; and

(10) set a date, including interim benchmarks, as appropriate, by which State, local, and tribal governments, Federal departments and agencies, and emergency response providers expect to achieve a baseline level of national interoperable communications, as that term is defined under section 10912(a) of this title.

§ 12304. Assessments and reports

(a) BASELINE ASSESSMENT.—The Secretary, acting through the Assistant Director for Emergency Communications, shall conduct an assessment of Federal, State, local, and tribal governments every 5 years, that—

(1) defines the range of capabilities needed by emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(2) defines the range of interoperable emergency communications capabilities needed for specific events;

(3) assesses the currently available capabilities to meet the communications needs;

(4) identifies the gap between current capabilities and defined requirements; and

(5) includes a national interoperable emergency communications inventory to be completed by the Secretary, the Secretary of Commerce, and the Chairman of the Federal Communications Commission that—

(A) identifies for each Federal department and agency—

(i) the channels and frequencies used;

(ii) the nomenclature used to refer to each channel or frequency used; and

(iii) the types of communications systems and equipment used; and

(B) identifies the interoperable emergency communications systems in use by public safety agencies in the United States.

(b) CLASSIFIED ANNEX.—The baseline assessment under this section may include a classified annex, including information provided under subsection (a)(5)(A).

(c) SAVINGS CLAUSE.—In conducting the baseline assessment under this section, the Secretary may incorporate findings from assessments conducted before, or ongoing on, October 4, 2006.

(d) PROGRESS REPORTS.—Not later than 1 year after October 4, 2006, and biennially thereafter, the Secretary, acting through the Assistant Director for Emergency Communications, shall submit to Congress a report on the progress of the Department in achieving the goals of, and carrying out its responsibilities under, this chapter, including—

(1) a description of the findings of the most recent baseline assessment conducted under subsection (a);

(2) a determination of the degree to which interoperable emergency communications capabilities have been attained to date and the gaps that remain for interoperability to be achieved;

(3) an evaluation of the ability to continue to communicate and to provide and maintain interoperable emergency communications by emergency managers, emergency response providers, and relevant government officials in the event of—

(A) natural disasters, acts of terrorism, or other man-made disasters, including Incidents of National Significance declared by the Secretary under the National Response Plan; and

(B) a catastrophic loss of local and regional communications services;

(4) a list of best practices relating to the ability to continue to communicate and to provide and maintain interoperable emergency communications in the event of natural disasters, acts of terrorism, or other man-made disasters; and

(5) an evaluation of the feasibility and desirability of the Department's developing, on its own or in conjunction with the Department of Defense, a mobile communications capability, modeled on the Army Signal Corps, that could be deployed to support emergency communications at the site of natural disasters, acts of terrorism, or other man-made disasters.

§ 12305. Coordination of Department emergency communications grant programs

(a) COORDINATION OF GRANTS AND STANDARDS PROGRAMS.—The Secretary, acting through the Assistant Director for Emergency Communications, shall ensure that grant guidelines for the use of homeland security assistance administered by the Department relating to interoperable emergency communications are coordinated and consistent with the goals and recommendations in the National Emergency Communications Plan under section 12303 of this title.

(b) DENIAL OF ELIGIBILITY FOR GRANTS.—

(1) IN GENERAL.—The Secretary, acting through the Assistant Secretary for Grants and Planning, and in consultation with the Assistant Director for Emergency Communications, may prohibit any State, local, or tribal government from using homeland security assistance administered by the Department to achieve, maintain, or enhance emergency communications capabilities, if—

(A) the government has not complied with the requirement to submit an Interoperable Communications Plan as required by section 10912(e) of this title;

(B) the government has proposed to upgrade or purchase new equipment or systems that do not meet or exceed any applicable national voluntary consensus standards and has not provided a reasonable explanation of why the equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed the standards; and

(C) as of the date that is 3 years after the date of the completion of the initial National Emergency Communications Plan under section 12303 of this title, national voluntary consensus standards for interoperable emergency communications capabilities have not been developed and promulgated.

(2) STANDARDS.—The Secretary, in coordination with the Federal Communications Commission, the National Institute of Standards and Technology, and other Federal departments and agencies responsible for standards, shall support the development, promulgation, and updating as necessary of national voluntary consensus standards for interoperable emergency communications.

§ 12306. Regional Emergency Communications Coordination

(a) IN GENERAL.—There is in each Regional Office a Regional Emergency Communications Coordination Working Group (in this section referred to as an ''RECC Working Group''). Each RECC Working Group shall report to the relevant Regional Administrator and coordinate its activities with the relevant Regional Advisory Council.

(b) MEMBERSHIP.—Each RECC Working Group consists of the following:

(1) Organizations representing the interests of the following:

(A) State officials.

(B) Local government officials, including sheriffs.

(C) State police departments.

(D) Local police departments.

(E) Local fire departments.

(F) Public safety answering points (9-1-1 services).

(G) State emergency managers, homeland security directors, or representatives of State administrative agencies.

(H) Local emergency managers or homeland security directors.

(I) Other emergency response providers as appropriate.

(2) Representatives from the Department, the Federal Communications Commission, and other Federal departments and agencies with responsibility for coordinating interoperable emergency communications with, or providing emergency support services to, State, local, and tribal governments.

(c) COORDINATION.—Each RECC Working Group shall coordinate its activities with the following:

(1) Communications equipment manufacturers and vendors (including broadband data service providers).

(2) Local exchange carriers.

(3) Local broadcast media.

(4) Wireless carriers.

(5) Satellite communications services.

(6) Cable operators.

(7) Hospitals.

(8) Public utility services.

(9) Emergency evacuation transit services.

(10) Ambulance services.

(11) HAM and amateur radio operators.

(12) Representatives from other private-sector entities and nongovernmental organizations as the Regional Administrator determines appropriate.

(d) DUTIES.—The duties of each RECC Working Group include—

(1) assessing the survivability, sustainability, and interoperability of local emergency communications systems to meet the goals of the National Emergency Communications Plan;

(2) reporting annually to the relevant Regional Administrator, the Assistant Director for Emergency Communications, the Chairman of the Federal Communications Commission, and the Assistant Secretary for Communications and Information of the Department of Commerce on the status of its region in building robust and sustainable interoperable voice and data emergency communications networks and, not later than 60 days after the completion of the initial National Emergency Communications Plan under section 12303 of this title, on the progress of the region in meeting the goals of the plan;

(3) ensuring a process for the coordination of effective multijurisdictional, multi-agency emergency communications networks for use

during natural disasters, acts of terrorism, and other man-made disasters through the expanded use of emergency management and public safety communications mutual aid agreements; and

(4) coordinating the establishment of Federal, State, local, and tribal support services and networks designed to address the immediate and critical human needs in responding to natural disasters, acts of terrorism, and other man-made disasters.

§ 12307. Emergency Communications Preparedness Center

(a) ESTABLISHMENT.—There is the Emergency Communications Preparedness Center.

(b) OPERATION.—The Secretary, the Chairman of the Federal Communications Commission, the Secretary of Defense, the Secretary of Commerce, the Attorney General, and the heads of other Federal departments and agencies or their designees shall jointly operate the Emergency Communications Preparedness Center in accordance with the Memorandum of Understanding entitled, ''Emergency Communications Preparedness Center (ECPC) Charter''.

(c) FUNCTIONS.—The Emergency Communications Preparedness Center shall—

(1) serve as the focal point for interagency efforts and as a clearinghouse with respect to all relevant intergovernmental information to support and promote (including specifically by working to avoid duplication, hindrances, and counteractive efforts among the participating Federal departments and agencies)—

(A) the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(B) interoperable emergency communications;

(2) prepare and submit to Congress annually a strategic assessment regarding the coordination efforts of Federal departments and agencies to advance—

(A) the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(B) interoperable emergency communications;

(3) consider, in preparing the strategic assessment under paragraph (2), the goals stated in the National Emergency Communications Plan under section 12303 of this title; and

(4) perform other functions provided in the ECPC Charter described in subsection (b).

§ 12308. Urban and other high-risk area communications capabilities

(a) IN GENERAL.—The Secretary, in consultation with the Chairman of the Federal Communications Commission and the Secretary of Defense, and with appropriate State, local, and tribal government officials, shall provide technical guidance, training, and other assistance, as appropriate, to support the rapid establishment of consistent, secure, and effective interoperable emergency communications capabilities in the event of an emergency in urban and other areas determined by the Secretary to be at consistently high levels of risk from natural disasters, acts of terrorism, and other man-made disasters.

(b) MINIMUM CAPABILITIES.—The interoperable emergency communications capabilities established under subsection (a) shall ensure the ability of all levels of government, emergency response providers, the private sector, and other organizations with emergency response capabilities—

(1) to communicate with each other in the event of an emergency;

(2) to have appropriate and timely access to the information sharing environment described in section 11908 of this title; and

(3) to be consistent with any applicable State or urban area homeland strategy or plan.

§ 12309. Interoperable Emergency Communications Grant Program

(a) ESTABLISHMENT.—The Secretary shall establish the Interoperable Emergency Communications Grant Program to make grants to States to carry out initiatives to improve local, tribal, statewide, regional, national, and, where appropriate, international interoperable emergency communications, including communications in collective response to natural disasters, acts of terrorism, and other man-made disasters.

(b) POLICY.—The Assistant Director for Emergency Communications shall ensure that a grant awarded to a State under this section is consistent with the policies established pursuant to the responsibilities and authorities of the Emergency Communications Division under this chapter, including ensuring that activities funded by the grant—

(1) comply with the statewide plan for that State required by section 10912(e) of this title; and

(2) comply with the National Emergency Communications Plan under section 12303 of this title, when completed.

(c) ADMINISTRATION.—

(1) IN GENERAL.—The Administrator of the Federal Emergency Management Agency shall administer the Interoperable Emergency Communications Grant Program pursuant to the responsibilities and authorities of the Administrator under chapter 113 of this title.

(2) GUIDANCE.—In administering the grant program, the Administrator shall ensure that the use of grants is consistent with guidance established by the Assistant Director for Emergency Communications under section 10912(b)(1)(H) of this title.

(d) USE OF FUNDS.—A State that receives a grant under this section shall use the grant to implement that State's Interoperable Communications Plan required under section 10912(e) of this title and approved under subsection (e) of this section, and to assist with activities determined by the Secretary to be integral to interoperable emergency communications.

(e) APPROVAL OF PLANS.—

(1) APPROVAL AS CONDITION OF GRANT.—Before a State may receive a grant under this section, the Assistant Director for Emergency Communications shall approve the State's Interoperable Communications Plan required under section 10912(e) of this title.

(2) PLAN REQUIREMENTS.—In approving a plan under this subsection, the Assistant Director for Emergency Communications shall ensure that the plan—

(A) is designed to improve interoperability at the city, county, regional, State, and interstate level;

(B) considers any applicable local or regional plan; and

(C) complies, to the maximum extent practicable, with the National Emergency Communications Plan under section 12303 of this title.

(3) APPROVAL OF REVISIONS.—The Assistant Director for Emergency Communications may approve revisions to a State's plan if the Assistant Director for Emergency Communications determines that doing so is likely to further interoperability.

(f) LIMITATIONS ON USES OF FUNDS.—

(1) IN GENERAL.—The recipient of a grant under this section may not use the grant—

(A) to supplant State or local funds;

(B) for any State or local government cost-sharing contribution; or

(C) for recreational or social purposes.

(2) PENALTIES.—In addition to other remedies currently available, the Secretary may take necessary actions to ensure that recipients of

grant funds are using the funds for the purpose for which they were intended.

(g) LIMITATIONS ON AWARD OF GRANTS.—

(1) NATIONAL EMERGENCY COMMUNICATIONS PLAN REQUIRED.—The Secretary may not award a grant under this section before the date on which the Secretary completes and submits to Congress the National Emergency Communications Plan required under section 12303 of this title.

(2) VOLUNTARY CONSENSUS STANDARDS.—The Secretary may not award a grant to a State under this section for the purchase of equipment that does not meet applicable voluntary consensus standards, unless the State demonstrates that there are compelling reasons for the purchase.

(h) AWARD OF GRANTS.—In approving applications and awarding grants under this section, the Secretary shall consider—

(1) the risk posed to each State by natural disasters, acts of terrorism, or other man-made disasters, including—

(A) the likely need of a jurisdiction within the State to respond to the risk in nearby jurisdictions;

(B) the degree of threat, vulnerability, and consequences related to critical infrastructure (from all critical infrastructure sectors) or key resources identified by the Administrator or the State homeland security and emergency management plans, including threats to, vulnerabilities of, and consequences from damage to critical infrastructure and key resources in nearby jurisdictions;

(C) the size of the population and density of the population of the State, including appropriate consideration of military, tourist, and commuter populations;

(D) whether the State is on or near an international border;

(E) whether the State encompasses an economically significant border crossing; and

(F) whether the State has a coastline bordering an ocean, a major waterway used for interstate commerce, or international waters; and

(2) the anticipated effectiveness of the State's proposed use of grant funds to improve interoperability.

(i) OPPORTUNITY TO AMEND APPLICATIONS.—In considering applications for grants under this section, the Administrator shall provide applicants with a reasonable opportunity to correct defects in the application, if any, before making final awards.

(j) MINIMUM GRANT AMOUNTS.—

(1) STATES.—In awarding grants under this section, the Secretary shall ensure that for each fiscal year, except as provided in paragraph (2), no State receives a grant in an amount that is less than 0.35 percent of the total amount appropriated for grants under this section for that fiscal year.

(2) TERRITORIES.—In awarding grants under this section, the Secretary shall ensure that for each fiscal year, American Samoa, the Northern Mariana Islands, Guam, and the Virgin Islands each receive grants in amounts that are not less than 0.08 percent of the total amount appropriated for grants under this section for that fiscal year.

(k) CERTIFICATION.—Each State that receives a grant under this section shall certify that the grant is used for the purpose for which the funds were intended and in compliance with the State's approved Interoperable Communications Plan.

(l) STATE RESPONSIBILITIES.—

(1) AVAILABILITY OF FUNDS TO LOCAL AND TRIBAL GOVERNMENTS.—Not later than 45 days after receiving grant funds, a State that receives a grant under this section shall obligate or otherwise make available to local and tribal governments—

(A) not less than 80 percent of the grant funds;

(B) with the consent of local and tribal governments, eligible expenditures having a value of not less than 80 percent of the amount of the grant; or

(C) grant funds combined with other eligible expenditures having a total value of not less than 80 percent of the amount of the grant.

(2) ALLOCATION OF FUNDS.—A State that receives a grant under this section shall allocate grant funds to tribal governments in the State to assist tribal communities in improving interoperable communications, in a manner consistent with the State's Interoperable Communications Plan. A State may not impose unreasonable or unduly burdensome requirements on a tribal government as a condition of providing grant funds or resources to the tribal government.

(3) PENALTIES.—If a State violates the requirements of this subsection, in addition to other remedies available to the Secretary, the Secretary may terminate or reduce the amount of the grant awarded to that State or transfer grant funds previously awarded to the State directly to the appropriate local or tribal government.

(m) REPORTS.—

(1) ANNUAL REPORTS BY STATE GRANT RECIPIENTS.—A State that receives a grant under this section shall annually submit to the Assist-

ant Director for Emergency Communications a report on the progress of the State in implementing that State's Interoperable Communications Plan required under section 10912(e) of this title and achieving interoperability at the city, county, regional, State, and interstate levels. The Assistant Director for Emergency Communications shall make the reports publicly available, including by making them available on the Internet website of the Cybersecurity and Infrastructure Security Agency, subject to any redactions that the Assistant Director for Emergency Communications determines are necessary to protect classified or other sensitive information.

(2) ANNUAL REPORTS TO CONGRESS.—At least once each year, the Assistant Director for Emergency Communications shall submit to Congress a report on the use of grants awarded under this section and any progress in implementing Statewide Interoperable Communications Plans and improving interoperability at the city, county, regional, State, and interstate level, as a result of the award of the grants.

(n) RULE OF CONSTRUCTION.—Nothing in this section shall be construed or interpreted to preclude a State from using a grant awarded under this section for interim or long-term Internet Protocol-based interoperable solutions.

§ 12310. Border interoperability demonstration project

(a) IN GENERAL.—

(1) ESTABLISHMENT.—The Secretary, acting through the Assistant Director for Emergency Communications, and in coordination with the Federal Communications Commission and the Secretary of Commerce, shall establish an International Border Community Interoperable Communications Project (in this section referred to as the ''demonstration project'').

(2) MINIMUM NUMBER OF COMMUNITIES.—The Assistant Director for Emergency Communications shall select no fewer than 6 communities to participate in the demonstration project.

(3) LOCATION OF COMMUNITIES.—No fewer than 3 of the communities selected under paragraph (2) shall be located on the northern border of the United States and no fewer than 3 of the communities selected under paragraph (2) shall be located on the southern border of the United States.

(b) CONDITIONS.—The Assistant Director for Emergency Communications, in coordination with the Federal Communications Commission and the Secretary of Commerce, shall ensure that the demonstration project is carried out as soon as adequate spectrum is available as a result of the 800 megahertz rebanding process in border areas, and shall ensure that the bor-

der projects do not impair or impede the rebanding process, but under no circumstances shall funds be distributed under this section unless the Federal Communications Commission and the Secretary of Commerce agree that these conditions have been met.

(c) DEMONSTRATION PROJECT REQUIREMENTS.—Consistent with the responsibilities of the Emergency Communications Division under section 12302 of this title, the Assistant Director for Emergency Communications shall foster local, tribal, State, and Federal interoperable emergency communications, as well as interoperable emergency communications with appropriate Canadian and Mexican authorities in the communities selected for the demonstration project. The Assistant Director for Emergency Communications shall—

(1) identify solutions to facilitate interoperable communications across national borders expeditiously;

(2) help ensure that emergency response provides can communicate with each other in the event of natural disasters, acts of terrorism, and other man-made disasters;

(3) provide technical assistance to enable emergency response providers to deal with threats and contingencies in a variety of environments;

(4) identify appropriate joint-use equipment to ensure communications access;

(5) identify solutions to facilitate communications between emergency response providers in communities of differing population densities; and

(6) take other actions or provide equipment as the Assistant Director for Emergency Communications considers appropriate to foster interoperable emergency communications.

(d) DISTRIBUTION OF FUNDS.—

(1) TO EACH PARTICIPATING COMMUNITY.—The Secretary shall distribute funds under this section to each community participating in the demonstration project through the State in which each community is located.

(2) TO LOCAL AND TRIBAL GOVERNMENTS AND EMERGENCY PROVIDERS SELECTED TO PARTICIPATE.—A State shall make the funds available promptly to the local and tribal government and emergency response providers selected by the Secretary to participate in the demonstration project.

(3) REPORT.—Not later than 90 days after a State receives funds under this subsection, the States shall report to the Assistant Director

for Emergency Communications on the status of the distribution of the funds to local and tribal governments.

(e) MAXIMUM PERIOD OF GRANTS.—The Assistant Director for Emergency Communications may not fund a participant under the demonstration project for more than 3 years.

(f) TRANSFER OF INFORMATION AND KNOWLEDGE.—The Assistant Director for Emergency Communications shall establish mechanisms to ensure that the information and knowledge gained by participants in the demonstration project are transferred among the participants and to other interested parties, including other communities that submitted applications to participate in the project.

Chapter 125—Countering Weapons of Mass Destruction Office

Sec.

§ 12501. Definitions

In this chapter:

(1) ASSISTANT SECRETARY.—The term ''Assistant Secretary'' means the Assistant Secretary for the Countering Weapons of Mass Destruction Office.

(2) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(3) OFFICE.—The term ''Office'' means the Countering Weapons of Mass Destruction Office.

(4) WEAPONS OF MASS DESTRUCTION.—The term ''weapons of mass destruction'' has the meaning given the term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

§ 12502. Mission

The Office is responsible for coordinating with other Federal efforts and developing a strategy and policy for the Department to plan for, detect, and protect against the importation, possession, storage, transportation, development, or use of unauthorized chemical, biological, radiological, or nuclear

materials, devices, or agents in the United States and to protect against an attack using those materials, devices, or agents against the people, territory, or interests of the United States.

§ 12503. Relationship to other Department components and Federal agencies

(a) IN GENERAL.—The authority of the Assistant Secretary under this chapter shall not affect the authorities or responsibilities of an officer of the Department or of an officer of another department or agency of the United States with respect to the command, control, or direction of the functions, personnel, funds, assets, and liabilities of a component in the Department or of a Federal department or agency.

(b) OFFICE FOR STRATEGY, POLICY, AND PLANS.—Not later than 1 year after December 21, 2018, the Assistant Secretary, in coordination with the Under Secretary for Strategy, Plans, and Policy, shall submit to the appropriate congressional committees a strategy and implementation plan to direct programs in the Office and to integrate those programs with other programs and activities of the Department.

(c) FEDERAL EMERGENCY MANAGEMENT AGENCY.—Nothing in this chapter or other provision of law may be construed to affect or reduce the responsibilities of the Federal Emergency Management Agency or the Administrator of the Federal Emergency Management Agency, including the diversion of an asset, function, or mission of the Federal Emergency Management Agency or the Administrator of the Federal Emergency Management Agency.

§ 12504. Responsibilities

(a) ASSISTANT SECRETARY.—The Assistant Secretary shall serve as the Secretary's principal advisor on—

(1) weapons of mass destruction matters and strategies; and

(2) the coordination of the efforts of the Department to counter weapons of mass destruction.

(b) OFFICE.—

(1) DEFINITIONS.—In this subsection:

(A) ALASKA NATIVE-SERVING INSTITUTION.—The term ''Alaska Native-serving institution'' has the meaning given the term in section 317 of the Higher Education Act of 1965 (20 U.S.C. 1059d).

(B) ASIAN AMERICAN AND NATIVE AMERICAN PACIFIC ISLANDER-SERVING INSTITUTION.—The term ''Asian American and Native American Pacific Islander-serving institution'' has the meaning given the term in section 320 of the Higher Education Act of 1965 (20 U.S.C. 1059g).

(C) HISPANIC-SERVING INSTITUTION.—The term ''Hispanic-serving institution'' has the meaning given the term in section 502 of the Higher Education Act of 1965 (20 U.S.C. 1101a).

(D) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term ''historically Black college or university'' has the meaning given the term ''part B institution'' in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

(E) NATIVE HAWAIIAN-SERVING INSTITUTION.—The term ''Native Hawaiian-serving institution'' has the meaning given the term in section 317 of the Higher Education Act of 1965 (20 U.S.C. 1059d).

(F) TRIBAL COLLEGE OR UNIVERSITY.—The term ''Tribal College or University'' has the meaning given the term in section 316(b) of the Higher Education Act of 1965 (20 U.S.C. 1059c(b)).

(2) IN GENERAL.—The Office is responsible for coordinating Federal efforts to detect and protect against the unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material in the United States, and to protect against attack using those devices or materials against the people, territory, or interests of the United States and, to this end, shall—

(A) serve as the primary entity of the United States Government to further develop, acquire, and support the deployment of an enhanced domestic system to detect and report on attempts to import, possess, store, transport, develop, or use an unauthorized nuclear explosive device, fissile material, or radiological material in the United States, and to improve that system over time;

(B) enhance and coordinate the nuclear detection efforts of Federal, State, local, and tribal governments and the private sector to ensure a managed, coordinated response;

(C) establish, with the approval of the Secretary and in coordination with the Attorney General, the Secretary of Defense, and the Secretary of Energy, additional protocols and procedures for use within the United States to ensure that the detection of unauthorized nuclear explosive devices, fissile material, or radiological material is promptly reported to the Attorney General, the Secretary, the Secretary of Defense, the Secretary of Energy, and other appropriate officials or their respective designees for appropriate action by law enforcement, military, emergency response, or other authorities;

(D) develop, with the approval of the Secretary and in coordination with the Attorney General, the Secretary of State, the Secretary of Defense, and the Secretary of Energy, an enhanced global nuclear detection architecture with implementation under which—

(i) the Office will be responsible for the implementation of the domestic portion of the global architecture;

(ii) the Secretary of Defense will retain responsibility for implementation of Department of Defense requirements within and outside the United States; and

(iii) the Secretary of State, the Secretary of Defense, and the Secretary of Energy will maintain their respective responsibilities for policy guidance and implementation of the portion of the global architecture outside the United States, which will be implemented consistent with applicable law and relevant international arrangements;

(E) ensure that the expertise necessary to accurately interpret detection data is made available in a timely manner for all technology deployed by the Domestic Nuclear Detection Office to implement the global nuclear detection architecture;

(F) conduct, support, coordinate, and encourage an aggressive, expedited, evolutionary, and transformational program of research and development to generate and improve technologies to detect and prevent the illicit entry, transport, assembly, or potential use within the United States of a nuclear explosive device or fissile or radiological material, and coordinate with the Under Secretary for Science and Technology on basic and advanced or transformational research and development efforts relevant to the mission of both organizations;

(G) carry out a program to test and evaluate technology for detecting a nuclear explosive device and fissile or radiological material, in coordination with the Secretary of Defense and the Secretary of Energy, as appropriate, and establish performance metrics for evaluating the effectiveness of individual detectors and detection systems in detecting such devices or material—

(i) under realistic operational and environmental conditions; and

(ii) against realistic adversary tactics and countermeasures;

(H) support and enhance the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other govern-

ment agencies, and foreign governments, as well as provide appropriate information to the entities;

(I) further enhance and maintain continuous awareness by analyzing information from all Domestic Nuclear Detection Office mission-related detection systems;

(J) lead the development and implementation of the national strategic five-year plan for improving the nuclear forensic and attribution capabilities of the United States required under section 1036 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84, 123 Stat. 2450);

(K) establish in the Office the National Technical Nuclear Forensics Center to provide centralized stewardship, planning, assessment, gap analysis, exercises, improvement, and integration for all Federal nuclear forensics and attribution activities—

(i) to ensure an enduring national technical nuclear forensics capability to strengthen the collective response of the United States to nuclear terrorism or other nuclear attacks; and

(ii) to coordinate and implement the national strategic five-year plan referred to in subparagraph (J);

(L) establish a National Nuclear Forensics Expertise Development Program, which—

(i) is devoted to developing and maintaining a vibrant and enduring academic pathway from undergraduate to post-doctorate study in nuclear and geochemical science specialties directly relevant to technical nuclear forensics, including radiochemistry, geochemistry, nuclear physics, nuclear engineering, materials science, and analytical chemistry;

(ii) shall—

(I) make available for undergraduate study, student scholarships with a duration of up to 4 years per student, which shall include, if possible, at least one summer internship at a national laboratory or appropriate Federal agency in the field of technical nuclear forensics during the course of the student's undergraduate career;

(II) make available for doctoral study, student fellowships with a duration of up to 5 years per student, which shall—

(aa) include, if possible, at least two summer internships at a national laboratory or appropriate Federal agency in the field of technical nuclear

forensics during the course of the student's graduate career; and

(bb) require each recipient to commit to serve for 2 years in a post-doctoral position in a technical nuclear forensics-related specialty at a national laboratory or appropriate Federal agency after graduation;

(III) make available to faculty, awards with a duration of 3 to 5 years each, to ensure faculty and their graduate students have a sustained funding stream; and

(IV) place a particular emphasis on reinvigorating technical nuclear forensics programs while encouraging the participation of undergraduate students, graduate students, and university faculty from historically Black colleges and universities, Hispanic-serving institutions, Tribal Colleges and Universities, Asian American and Native American Pacific Islander-serving institutions, Alaska Native-serving institutions, and Native Hawaiian-serving institutions; and

(iii) shall—

(I) provide for the selection of individuals to receive scholarships or fellowships under this section through a competitive process primarily on the basis of academic merit and the nuclear forensics and attribution needs of the United States Government;

(II) provide for the setting aside of up to 10 percent of the scholarships or fellowships awarded under this section for individuals who are Federal employees to enhance the education of the employees in areas of critical nuclear forensics and attribution needs of the United States Government, for doctoral education under the scholarship or fellowship on a full-time or part-time basis;

(III) provide that the Secretary may enter into a contractual agreement with an institution of higher education under which the amounts provided for a scholarship under this section for tuition, fees, and other authorized expenses are paid directly to the institution with respect to which the scholarship is awarded;

(IV) require scholarship recipients to maintain satisfactory academic progress; and

(V) require that—

(aa) a scholarship recipient who fails to maintain a high level of academic standing, as defined by the Secretary, who is dismissed for disciplinary reasons from the educational institution the recipient is attending, or who voluntarily terminates academic training before graduation from the educational program for which the scholarship was awarded is liable to the United States for repayment within 1 year after the date of default of all scholarship funds paid to the recipient and to the institution of higher education on the behalf of the recipient, provided that the repayment period may be extended by the Secretary if the Secretary determines it necessary, as established by regulation; and

(bb) a scholarship recipient who, for any reason except death or disability, fails to begin or complete the post-doctoral service requirements in a technical nuclear forensics-related specialty at a national laboratory or appropriate Federal agency after completion of academic training is liable to the United States for an amount equal to—

(AA) the total amount of the scholarship received by the recipient under this section; and

(BB) the interest on the amounts which would be payable if at the time the scholarship was received the scholarship was a loan bearing interest at the maximum legally prevailing rate;

(M) provide an annual report to Congress on the activities carried out under subparagraphs (J), (K), and (L); and

(N) perform other duties assigned by the Secretary.

(c) CHIEF MEDICAL OFFICER.—The Chief Medical Officer has the 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 on medical and public health issues to the Secretary, the Administrator of the Federal Emergency Management Agency, the Assistant Secretary, and other Department officials;

(2) providing operational medical support to all components of the Department;

(3) as appropriate, providing medical liaisons to the components of the Department, on a reimbursable basis, to provide subject matter expertise on operational medical issues;

(4) coordinating with Federal, State, local, and tribal governments, the medical community, and others within and outside the Department, including the Centers for Disease Control and Prevention and the Office of Assistant Secretary for Preparedness and Response of the Department of Health and Human Services, with respect to medical and public health matters; and

(5) performing other duties relating to these responsibilities that the Secretary may require.

§ 12505. Technology research and development investment strategy for nuclear and radiological detection

(a) IN GENERAL.—The Secretary, the Secretary of Energy, the Secretary of Defense, and the Director of National Intelligence shall submit to Congress a research and development investment strategy for nuclear and radiological detection.

(b) CONTENTS.—The strategy under subsection (a) shall include—

(1) a long-term technology roadmap for nuclear and radiological detection applicable to the mission needs of the Department, the Department of Energy, the Department of Defense, and the Office of the Director of National Intelligence;

(2) budget requirements necessary to meet the roadmap; and

(3) documentation of how the Department, the Department of Energy, the Department of Defense, and the Office of the Director of National Intelligence will execute this strategy.

(c) ANNUAL REPORT.—The Assistant Secretary and the Under Secretary for Science and Technology jointly and annually shall notify Congress that the strategy and technology road map for nuclear and radiological detection developed under subsections (a) and (b) is consistent with the national policy and strategic plan for identifying priorities, goals, objectives, and policies for coordinating the Federal Government's civilian efforts to identify and develop countermeasures to terrorist threats from weapons of mass destruction that are required under section 10901(2) of this title.

§ 12506. Testing authority

(a) IN GENERAL.—The Assistant Secretary shall coordinate with the responsible Federal agency or other entity to facilitate the use by the Office, by its contractors, or by other persons or entities, of existing Government laboratories, centers, ranges, or other testing facilities for the testing of materials, equipment, models, computer software, and other items as may be related to the responsibilities identified in section 12504(b) of this title. Use

of Government facilities shall be carried out in accordance with all applicable laws, regulations, and contractual provisions, including those governing security, safety, and environmental protection, including, when applicable, section 10908 of this title. The Office may direct that private-sector entities utilizing Government facilities under this section pay an appropriate fee to the agency that owns or operates those facilities to defray additional costs to the Government resulting from private-sector use.

(b) CONFIDENTIALITY OF TEST RESULTS.—The results of tests performed with services made available shall be confidential and shall not be disclosed outside the Federal Government without the consent of the persons for whom the tests are performed.

(c) FEES.—Fees for services made available under this section shall not exceed the amount necessary to recoup the direct and indirect costs involved, such as direct costs of utilities, contractor support, and salaries of personnel that are incurred by the United States to provide for the testing.

(d) USE OF FEES.—Fees received for services made available under this section may be credited to the appropriation from which funds were expended to provide the services.

§ 12507. Personnel

(a) HIRING.—In hiring personnel for the Office, the Secretary has the hiring and management authorities provided in section 1599h of title 10. The term of appointments for employees under section 1599h(c)(1) of title 10 may not exceed 5 years before granting an extension under section 1599h(c)(2) of title 10.

(b) DETAIL.—The Secretary may request that the Secretary of Defense, the Secretary of Energy, the Secretary of State, the Attorney General, the Nuclear Regulatory Commission, and the directors of other Federal agencies, including elements of the intelligence community, provide for the reimbursable detail of personnel with relevant expertise to the Office.

§ 12508. Contracting and grant making authorities

The Secretary, acting through the Assistant Secretary, in carrying out the responsibilities under section 12504(b) of this title shall—

(1) operate extramural and intramural programs and distribute funds through grants, cooperative agreements, and other transactions and contracts;

(2) ensure that activities under section 12504(b) of this title include investigations of radiation detection equipment in configurations suitable for deployment at seaports, which may include underwater or water surface detection equipment and detection equipment that can be mounted on cranes and straddle cars used to move shipping containers; and

(3) have the authority to establish or contract with one or more federally funded research and development centers to provide independent analysis of homeland security issues and carry out other responsibilities under this chapter.

§ 12509. Joint annual interagency review of global nuclear detection architecture

(a) DEFINITION OF GLOBAL NUCLEAR DETECTION ARCHITECTURE.—In this section, the term ''global nuclear detection architecture'' means the global nuclear detection architecture developed under section 12504(b) of this title.

(b) ANNUAL REVIEW.—

(1) IN GENERAL.—The Secretary, the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Energy, and the Director of National Intelligence shall jointly ensure interagency coordination on the development and implementation of the global nuclear detection architecture by ensuring that, not less frequently than once each year—

(A) each relevant agency, office, or entity—

(i) assesses its involvement, support, and participation in the development, revision, and implementation of the global nuclear detection architecture; and

(ii) examines and evaluates components of the global nuclear detection architecture (including associated strategies and acquisition plans) relating to the operations of that agency, office, or entity, to determine whether the components incorporate and address current threat assessments, scenarios, or intelligence analyses developed by the Director of National Intelligence or other agencies regarding threats relating to nuclear or radiological weapons of mass destruction;

(B) each agency, office, or entity deploying or operating any nuclear or radiological detection technology under the global nuclear detection architecture—

(i) evaluates the deployment and operation by that agency, office, or entity of nuclear or radiological detection technologies under the global nuclear detection architecture;

(ii) identifies performance deficiencies and operational or technical deficiencies in nuclear or radiological detection technologies deployed under the global nuclear detection architecture; and

(iii) assesses the capacity of that agency, office, or entity to implement the responsibilities of that agency, office, or entity under the global nuclear detection architecture; and

(C) the Assistant Secretary and each of the relevant departments that are partners in the National Technical Forensics Center—

(i) include, as part of the assessments, evaluations, and reviews required under this paragraph, each office's or department's activities and investments in support of nuclear forensics and attribution activities and specific goals and objectives accomplished during the previous year pursuant to the national strategic five-year plan for improving the nuclear forensic and attribution capabilities of the United States required under section 1036 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84, 123 Stat. 2450);

(ii) attach, as an appendix to the Joint Interagency Annual Review, the most current version of the strategy and plan; and

(iii) include a description of new or amended bilateral and multilateral agreements and efforts in support of nuclear forensics and attribution activities accomplished during the previous year.

(2) TECHNOLOGY.—Not less frequently than once each year, the Secretary shall examine and evaluate the development, assessment, and acquisition of radiation detection technologies deployed or implemented in support of the domestic portion of the global nuclear detection architecture.

(c) ANNUAL REPORT ON JOINT INTERAGENCY REVIEW.—

(1) IN GENERAL.—Not later than March 31 of each year, the Secretary, the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Energy, and the Director of National Intelligence, shall jointly submit a report regarding the implementation of this section and the results of the reviews required under subsection (b) to—

(A) the President;

(B) the Committee on Appropriations, the Committee on Armed Services, the Select Committee on Intelligence, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Appropriations, the Committee on Armed Services, the Permanent Select Committee on Intelligence, the Committee on Homeland Security, and the Committee on Science and Technology of the House of Representatives.

(2) FORM.—The annual report submitted under paragraph (1) shall be submitted in unclassified form to the maximum extent practicable, but may include a classified annex.

§ 12510. Securing the Cities program

(a) ESTABLISHMENT.—The Secretary, through the Assistant Secretary, shall establish the Securing the Cities (in this section referred to as ''STC'') program to enhance the ability of the United States to detect and prevent terrorist attacks and other high-consequence events utilizing nuclear or other radiological materials that pose a high risk to homeland security in high-risk urban areas.

(b) ELEMENTS.—Through the STC program, the Secretary shall—

(1) assist State, local, tribal, and territorial governments in designing and implementing, or enhancing existing, architectures for coordinated and integrated detection and interdiction of nuclear or other radiological materials that are out of regulatory control;

(2) support the development of an operating capability to detect and report on nuclear and other radiological materials out of regulatory control;

(3) provide resources to enhance detection, analysis, communication, and coordination to better integrate State, local, tribal, and territorial assets into Federal operations;

(4) facilitate alarm adjudication and provide subject matter expertise and technical assistance on concepts of operation, training, exercises, and alarm response protocols;

(5) communicate with, and promote sharing of information about the presence or detection of nuclear or other radiological materials among, appropriate Federal, State, local, tribal, and territorial government agencies in a manner that ensures transparency with the jurisdictions designated under subsection (c);

(6) provide augmenting resources, as appropriate, to enable State, local, tribal, and territorial governments to sustain and refresh their capabilities developed under the STC program;

(7) monitor expenditures under the STC program and track performance in meeting the goals of the STC program; and

(8) provide any other assistance the Secretary determines appropriate.

(c) DESIGNATION OF JURISDICTIONS.—

(1) IN GENERAL.—In carrying out the STC program under subsection (a), the Secretary shall designate jurisdictions from among the high-risk urban areas under section 12703 of this title.

(2) CONGRESSIONAL NOTIFICATION.—The Secretary shall notify the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate not later than 3 days before the designation of a new jurisdiction under paragraph (1) or a change to a jurisdiction previously designated under paragraph (1).

(d) ACCOUNTABILITY.—

(1) IMPLEMENTATION.—

(A) IN GENERAL.—The Secretary shall develop, in consulation with relevant stakeholders, an implementation plan for carrying out the STC program that includes—

(i) a discussion of the goals of the STC program and a strategy to achieve those goals;

(ii) performance metrics and milestones for the STC program;

(iii) measures for achieving and sustaining capabilities under the STC program; and

(iv) costs associated with achieving the goals of the STC program.

(B) SUBMISSION TO CONGRESS.–Not later than 1 year after December 21, 2018, the Secretary shall submit to the appropriate congressional committees and the Comptroller General the implementation plan required by subparagraph (A).

(2) REPORT REQUIRED.—Not later than 1 year after the submission of the implementation plan under paragraph (1)(B), the Secretary shall submit to the appropriate congressional committees and the Comptroller General a report that includes—

(A) an assessment of the effectiveness of the STC program, based on the performance metrics and milestones required by paragraph (1)(A); and

(B) proposals for changes to the STC program, including an explanation of how those changes align with the strategy and goals of the STC program and, as appropriate, address challenges faced by the STC program.

(3) COMPTROLLER GENERAL REVIEW.—Not later than 18 months after the submission of the report required by paragraph (2), the Comptroller General shall submit to the appropriate congressional com-

mittees a report evaluating the implementation plan required by paragraph (1) and the report required by paragraph (2), including an assessment of progress made with respect to the performance metrics and milestones required by paragraph (1)(A)(ii) and the sustainment of the capabilities of the STC program.

(4) BRIEFING AND SUBMISSION REQUIREMENTS.—Before making changes to the structure or requirements of the STC program, the Assistant Secretary shall—

(A) consult with appropriate congressional committees; and

(B) provide to those committees—

(i) a briefing on the proposed changes, including a justification for the changes;

(ii) documentation relating to the changes, including plans, strategies, and resources to implement the changes; and

(iii) an assessment of the effect of the changes on the capabilities of the STC program, taking into consideration previous resource allocations and stakeholder input.

§ 12511. Medical countermeasures

(a) DEFINITION OF MEDICAL COUNTERMEASURES.—In this section, the term ''medical countermeasures'' means antibiotics, antivirals, antidotes, therapeutics, radiological countermeasures, and other countermeasures that may be deployed to protect the employees and working animals of the Department in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, other event impacting health, or pandemic.

(b) IN GENERAL.—Subject to the availability of appropriations, the Secretary shall, as appropriate, establish a medical countermeasures program within the components of the Department to—

(1) facilitate personnel readiness and protection for the employees and working animals of the Department in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, other event impacting health, or pandemic; and

(2) support the mission continuity of the Department.

(c) OVERSIGHT.—The Secretary, acting through the Chief Medical Officer, shall—

(1) provide programmatic oversight of the medical countermeasures program established under subsection (b); and

(2) develop standards for—

(A) medical countermeasure storage, security, dispensing, and documentation;

(B) maintaining a stockpile of medical countermeasures, including antibiotics, antivirals, antidotes, therapeutics, and radiological countermeasures, as appropriate;

(C) ensuring adequate partnerships with manufacturers and executive agencies that enable advance prepositioning by vendors of inventories of appropriate medical countermeasures in strategic locations nationwide, based on risk and employee density, in accordance with applicable Federal statutes and regulations;

(D) providing oversight and guidance regarding the dispensing of stockpiled medical countermeasures;

(E) ensuring rapid deployment and dispensing of medical countermeasures in a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, other event impacting health, or pandemic;

(F) providing training to employees of the Department on medical countermeasures; and

(G) supporting dispensing exercises.

(d) MEDICAL COUNTERMEASURE WORKING GROUP.—The Secretary, acting through the Chief Medical Officer, shall establish a medical countermeasures working group comprised of representatives from appropriate components and offices of the Department to ensure that medical countermeasures standards are maintained and guidance is consistent.

(e) MEDICAL COUNTERMEASURES MANAGEMENT.—NOT LATER THAN 120 DAYS AFTER THE DATE ON WHICH APPROPRIATIONS ARE MADE AVAILABLE TO CARRY OUT SUBSECTION (B), THE CHIEF MEDICAL OFFICER SHALL DEVELOP AND SUBMIT TO THE SECRETARY AN INTEGRATED LOGISTICS SUPPORT PLAN FOR MEDICAL COUNTERMEASURES, INCLUDING—

(1) a methodology for determining the ideal types and quantities of medical countermeasures to stockpile and how frequently the methodology shall be reevaluated;

(2) a replenishment plan; and

(3) inventory tracking, reporting, and reconciliation procedures for existing stockpiles and new medical countermeasure purchases.

(f) TRANSFER.—Not later than 120 days after December 27, 2021, the Secretary shall transfer all medical countermeasures-related programmatic and personnel resources from the Under Secretary for Management to the Chief Medical Officer.

(g) STOCKPILE ELEMENTS.—In determining the types and quantities of medical countermeasures to stockpile under subsection (e), the Secretary, acting through the Chief Medical Officer—

(1) shall use a risk-based methodology for evaluating types and quantities of medical countermeasures required; and

(2) may use, if available—

(A) chemical, biological, radiological, and nuclear risk assessments of the Department; and

(B) guidance on medical countermeasures of the Office of the Assistant Secretary for Preparedness and Response and the Centers for Disease Control and Prevention.

(h) BRIEFING.—Not later than 180 days after December 27, 2021, the Secretary shall provide a briefing to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives regarding—-

(1) the plan developed under subsection (e); and

(2) implementation of the requirements of this section.

§ 12512. Annual report by Secretary

Not later than 1 year after December 21, 2018, and annually thereafter, the Secretary shall provide a briefing and report to the appropriate congressional committees on—

(1) the organization and management of the chemical, biological, radiological, and nuclear activities of the Department, including research and development activities, and the location of each activity under the organizational structure of the Office;

(2) a comprehensive inventory of chemical, biological, radiological, and nuclear activities of the Department, including research and development activities, highlighting areas of collaboration between components, coordination with other agencies, and the effectiveness and accomplishments of consolidated chemical, biological, radiological, and nuclear activities of the Department, including research and development activities;

(3) information relating to how the organizational structure of the Office will enhance the development of chemical, biological, radiological, and nuclear priorities and capabilities of the Department;

(4) a discussion of any resulting cost savings and efficiencies gained through activities described in paragraphs (1) and (2);

(5) information on how the Assistant Secretary is coordinating with the Under Secretary of Science and Technology of the Department on research and development activities; and

(6) recommendations for any necessary statutory changes, or, if no statutory changes are necessary, an explanation of why no statutory or organizational changes are necessary.

Chapter 127—Homeland Security Grants

Subchapter I—Grants to States, High-Risk Urban Areas, and Nonprofit Organizations

Part A—In General

§ 12701. Definitions

In this subchapter:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Federal Emergency Management Agency.

(2) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

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

(B) those committees of the House of Representatives that the Speaker of the House of Representatives determines appropriate.

(3) CRITICAL INFRASTRUCTURE SECTORS.—The term ''critical infrastructure sectors'' means the following sectors, in both urban and rural areas:

(A) Agriculture and food.

(B) Banking and finance.

(C) Chemical industries.

(D) Commercial facilities.

(E) Commercial nuclear reactors, materials, and waste.

(F) Dams.

(G) The defense industrial base.

(H) Emergency services.

(I) Energy.

(J) Government facilities.

(K) Information technology.

(L) National monuments and icons.

(M) Postal and shipping.

(N) Public health and health care.

(O) Telecommunications.

(P) Transportation systems.

(Q) Water.

(4) DIRECTLY ELIGIBLE TRIBE.—The term ''directly eligible tribe'' means—

(A) an Indian tribe—

(i) that is located in the continental United States;

(ii) that operates a law enforcement or emergency response agency with the capacity to respond to calls for law enforcement or emergency services;

(iii) that—

(I) is located on or near an international border or a coastline bordering an ocean (including the Gulf of Mexico) or international waters;

(II) is located within 10 miles of a system or asset included on the prioritized critical infrastructure list established under section 10712(a)(2) of this title or has such a system or asset within its territory;

(III) is located within or contiguous to one of the 50 most populous metropolitan statistical areas in the United States; or

(IV) has jurisdiction over not less than 1,000 square miles of Indian country, as that term is defined in section 1151 of title 18; and

(iv) that certifies to the Secretary that a State has not provided funds under section 12703 or 12704 of this title to the Indian tribe or consortium of Indian tribes for the purpose for which direct funding is sought; and

(B) a consortium of Indian tribes, if each tribe satisfies the requirements of subparagraph (A).

(5) ELIGIBLE METROPOLITAN AREA.—The term ''eligible metropolitan area'' means any of the 100 most populous metropolitan statistical areas in the United States.

(6) HIGH-RISK URBAN AREA.—The term ''high-risk urban area'' means a high-risk urban area designated under section 12703(b)(3)(A) of this title.

(7) INDIAN TRIBE.—The term ''Indian tribe'' has the meaning given the term in section 4(e) of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b(e)).

(8) METROPOLITAN STATISTICAL AREA.—The term ''metropolitan statistical area'' means a metropolitan statistical area, as defined by the Office of Management and Budget.

(9) NATIONAL SPECIAL SECURITY EVENT.—The term ''National Special Security Event'' means a designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity.

(10) POPULATION.—The term ''population'' means population according to the most recent United States census population estimates available at the start of the relevant fiscal year.

(11) POPULATION DENSITY.—The term ''population density'' means population divided by land area in square miles.

(12) QUALIFIED INTELLIGENCE ANALYST.—The term ''qualified intelligence analyst'' means an intelligence analyst (as that term is defined in section 10512(a) of this title), including law enforcement personnel—

(A) who has successfully completed training to ensure baseline proficiency in intelligence analysis and production, as determined by the Secretary, which may include training using a curriculum developed under section 10510 of this title; or

(B) whose experience ensures baseline proficiency in intelligence analysis and production equivalent to the training required under subparagraph (A), as determined by the Secretary.

(13) TARGET CAPABILITIES.—The term ''target capabilities'' means the target capabilities for Federal, State, local, and tribal government

preparedness for which guidelines are required to be established under section 20506 of this title.

(14) TRIBAL GOVERNMENT.—The term ''tribal government'' means the government of an Indian tribe.

§ 12702. Homeland security grant programs

(a) GRANTS AUTHORIZED.—The Secretary, acting through the Administrator, may award grants under sections 12703, 12704, and 12709 of this title to State, local, and tribal governments.

(b) PROGRAMS NOT AFFECTED.—This subchapter shall not be construed to affect any of the following Federal programs:

(1) Firefighter and other assistance programs authorized under the Federal Fire Prevention and Control Act of 1974 (15 U.S.C. 2201 et seq.).

(2) Grants authorized under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

(3) Emergency Management Performance Grants under the amendments made by title II of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 294).

(4) Grants to protect critical infrastructure, including port security grants authorized under section 70107 of title 46, and grants authorized under titles XIV and XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 400, 422) and the amendments made by those titles.

(5) The Metropolitan Medical Response System authorized under section 20304 of this title.

(6) The Interoperable Emergency Communications Grant Program authorized under section 12309 of this title.

(7) Grant programs other than those administered by the Department.

(c) RELATIONSHIP TO OTHER LAWS.—

(1) IN GENERAL.—The grant programs authorized under sections 12703 and 12704 of this title supersede all grant programs authorized under section 1014 of the USA PATRIOT Act (42 U.S.C. 3714).

(2) ALLOCATION.—The allocation of grants authorized under sections 12703 and 12704 of this title is governed by the terms of this subchapter and not by any other provision of law.

§ 12703. Urban Area Security Initiative

(a) ESTABLISHMENT.—There is in the Department the Urban Area Security Initiative to provide grants to assist high-risk urban areas in preventing, preparing for, protecting against, and responding to acts of terrorism.

(b) ASSESSMENT AND DESIGNATION OF HIGH-RISK URBAN AREAS.—

(1) IN GENERAL.—The Secretary shall designate high-risk urban areas to receive grants under this section based on procedures under this subsection.

(2) INITIAL ASSESSMENT.—

(A) IN GENERAL.—For each fiscal year, the Secretary shall conduct an initial assessment of the relative threat, vulnerability, and consequences from acts of terrorism faced by each eligible metropolitan area, including consideration of—

(i) the factors set forth in subparagraphs (A) through (H) and (K) of section 12707(a)(1) of this title; and

(ii) information and materials submitted under subparagraph (B).

(B) SUBMISSION OF INFORMATION BY ELIGIBLE METROPOLITAN AREAS.—Prior to conducting each initial assessment under subparagraph (A), the Secretary shall provide each eligible metropolitan area with, and shall notify each eligible metropolitan area of, the opportunity to—

(i) submit information that the eligible metropolitan area believes to be relevant to the determination of the threat, vulnerability, and consequences it faces from acts of terrorism; and

(ii) review the risk assessment conducted by the Department of that eligible metropolitan area, including the bases for the assessment by the Department of the threat, vulnerability, and consequences from acts of terrorism faced by that eligible metropolitan area, and remedy erroneous or incomplete information.

(3) DESIGNATION OF HIGH-RISK URBAN AREAS.—

(A) IN GENERAL.—

(i) DESIGNATION.—For each fiscal year, after conducting the initial assessment under paragraph (2), and based on that assessment, the Secretary shall designate high-risk urban areas that may submit applications for grants under this section.

(ii) EXCEPTIONS.—Notwithstanding paragraph (2), the Secretary may—

(I) in any case where an eligible metropolitan area consists of more than one metropolitan division (as that term is defined by the Office of Management and Budg-

et) designate more than one high-risk urban area within a single eligible metropolitan area; and

(II) designate an area that is not an eligible metropolitan area as a high-risk urban area based on the assessment by the Secretary of the relative threat, vulnerability, and consequences from acts of terrorism faced by the area.

(iii) SECRETARY NOT REQUIRED TO DESIGNATE ALL ELIGIBLE AREAS AS HIGH-RISK URBAN AREAS.—Nothing in this subsection may be construed to require the Secretary to—

(I) designate all eligible metropolitan areas that submit information to the Secretary under paragraph (2)(B)(i) as high-risk urban areas; or

(II) designate all areas within an eligible metropolitan area as part of the high-risk urban area.

(B) JURISDICTIONS INCLUDED IN HIGH-RISK URBAN AREAS.—

(i) BY SECRETARY.—In designating high-risk urban areas under subparagraph (A), the Secretary shall determine which jurisdictions, at a minimum, shall be included in each high-risk urban area.

(ii) BY HIGH-RISK URBAN AREA.—A high-risk urban area designated by the Secretary may, in consultation with the State or States in which the high-risk urban area is located, add additional jurisdictions to the high-risk urban area.

(c) APPLICATION.—

(1) IN GENERAL.—An area designated as a high-risk urban area under subsection (b) may apply for a grant under this section.

(2) MINIMUM CONTENTS OF APPLICATION.—In an application for a grant under this section, a high-risk urban area shall submit—

(A) a plan describing the proposed division of responsibilities and distribution of funding among the local and tribal governments in the high-risk urban area;

(B) the name of an individual to serve as a high-risk urban area liaison with the Department and among the various jurisdictions in the high-risk urban area; and

(C) information in support of the application the Secretary may reasonably require.

(3) ANNUAL APPLICATIONS.—Applicants for grants under this section shall apply or reapply on an annual basis.

(4) STATE REVIEW AND TRANSMISSION.—

(A) IN GENERAL.—To ensure consistency with State homeland security plans, a high-risk urban area applying for a grant under this section shall submit its application to each State within which any part of that high-risk urban area is located for review before submission of the application to the Department.

(B) DEADLINE.—Not later than 30 days after receiving an application from a high-risk urban area under subparagraph (A), a State shall transmit the application to the Department.

(C) OPPORTUNITY FOR STATE COMMENT.—If the Governor of a State determines that an application of a high-risk urban area is inconsistent with the State homeland security plan of that State, or otherwise does not support the application, the Governor shall—

(i) notify the Secretary, in writing, of that fact; and

(ii) provide an explanation of the reason for not supporting the application at the time of transmission of the application.

(5) OPPORTUNITY TO AMEND.—In considering applications for grants under this section, the Secretary shall provide applicants with a reasonable opportunity to correct defects in the application, if any, before making final awards.

(d) DISTRIBUTION OF AWARDS.—

(1) IN GENERAL.—If the Secretary approves the application of a high-risk urban area for a grant under this section, the Secretary shall distribute the grant funds to the State or States in which that high-risk urban area is located.

(2) STATE DISTRIBUTION OF FUNDS.—

(A) IN GENERAL.—Not later than 45 days after the date on which a State receives grant funds under paragraph (1), that State shall provide the high-risk urban area awarded that grant not less than 80 percent of the grant funds. Any funds retained by a State shall be expended on items, services, or activities that benefit the high-risk urban area.

(B) FUNDS RETAINED.—A State shall provide each relevant high-risk urban area with an accounting of the items, services, or activities on which any funds retained by the State under subparagraph (A) were expended.

(3) INTERSTATE URBAN AREAS.—If parts of a high-risk urban area awarded a grant under this section are located in 2 or more States, the Secretary shall distribute to each State—

(A) a portion of the grant funds in accordance with the proposed distribution set forth in the application; or

(B) if no agreement on distribution has been reached, a portion of the grant funds determined by the Secretary to be appropriate.

(4) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO HIGH-RISK URBAN AREAS.—A State that receives grant funds under paragraph (1) shall certify to the Secretary that the State has made available to the applicable high-risk urban area the required funds under paragraph (2).

§ 12704. State Homeland Security Grant Program

(a) ESTABLISHMENT.—There is in the Department a State Homeland Security Grant Program to assist State, local, and tribal governments in preventing, preparing for, protecting against, and responding to acts of terrorism.

(b) APPLICATION.—

(1) IN GENERAL.—Each State may apply for a grant under this section and shall submit information in support of the application that the Secretary may reasonably require.

(2) MINIMUM CONTENTS OF APPLICATION.—The Secretary shall require that each State include in its application, at a minimum—

(A) the purpose for which the State seeks grant funds and the reasons why the State needs the grant to meet the target capabilities of that State;

(B) a description of how the State plans to allocate the grant funds to local governments and Indian tribes; and

(C) a budget showing how the State intends to expend the grant funds.

(3) ANNUAL APPLICATIONS.—Applicants for grants under this section shall apply or reapply on an annual basis.

(c) DISTRIBUTION TO LOCAL AND TRIBAL GOVERNMENTS.—

(1) IN GENERAL.—Not later than 45 days after receiving grant funds, any State receiving a grant under this section shall make available to local and tribal governments, consistent with the applicable State homeland security plan—

(A) not less than 80 percent of the grant funds;

(B) with the consent of local and tribal governments, items, services, or activities having a value of not less than 80 percent of the amount of the grant; or

(C) with the consent of local and tribal governments, grant funds combined with other items, services, or activities having a total value of not less than 80 percent of the amount of the grant.

(2) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO LOCAL GOVERNMENTS.—A State shall certify to the Secretary that

the State has made the distribution to local and tribal governments required under paragraph (1).

(3) EXTENSION OF PERIOD.—The Governor of a State may request in writing that the Secretary extend the period under paragraph (1) for an additional period of time. The Secretary may approve a request if the Secretary determines that the resulting delay in providing grant funding to the local and tribal governments is necessary to promote effective investments to prevent, prepare for, protect against, or respond to acts of terrorism.

(4) EXCEPTION.—Paragraph (1) does not apply to the District of Columbia, Puerto Rico, American Samoa, the Northern Mariana Islands, Guam, or the Virgin Islands.

(5) DIRECT FUNDING.—If a State fails to make the distribution to local or tribal governments required under paragraph (1) in a timely fashion, a local or tribal government entitled to receive the distribution may petition the Secretary to request that grant funds be provided directly to the local or tribal government.

(d) MULTISTATE APPLICATIONS.—

(1) IN GENERAL.—Instead of, or in addition to, any application for a grant under subsection (b), 2 or more States may submit an application for a grant under this section in support of multistate efforts to prevent, prepare for, protect against, and respond to acts of terrorism.

(2) ADMINISTRATION OF GRANT.—If a group of States applies for a grant under this section, the States shall submit to the Secretary at the time of application a plan describing—

(A) the division of responsibilities for administering the grant; and

(B) the distribution of funding among the States that are parties to the application.

(e) MINIMUM ALLOCATION.—

(1) IN GENERAL.—In allocating funds under this section, the Secretary shall ensure that—

(A) except as provided in subparagraph (B), each State receives for each fiscal year, from the funds appropriated for the State Homeland Security Grant Program established under this section, not less than 0.35 percent of the total funds appropriated for grants under this section and section 12703 of this title; and

(B) for each fiscal year, American Samoa, the Northern Mariana Islands, Guam, and the Virgin Islands each receive, from the funds appropriated for the State Homeland Security Grant Program established under this section, not less than an amount

equal to 0.08 percent of the total funds appropriated for grants under this section and section 12703 of this title.

(2) EFFECT OF MULTISTATE AWARD ON STATE MINIMUM.—Any portion of a multistate award provided to a State under subsection (d) shall be considered in calculating the minimum State allocation under this subsection.

§ 12705. Grants to directly eligible tribes

(a) IN GENERAL.—Notwithstanding section 12704(b) of this title, the Secretary, acting through the Administrator, may award grants to directly eligible tribes under section 12704 of this title.

(b) TRIBAL APPLICATIONS.—A directly eligible tribe may apply for a grant under section 12704 of this title by submitting an application to the Secretary that includes, as appropriate, the information required for an application by a State under section 12704(b) of this title.

(c) CONSISTENCY WITH STATE PLANS.—

(1) IN GENERAL.—To ensure consistency with any applicable State homeland security plan, a directly eligible tribe applying for a grant under section 12704 of this title shall provide a copy of its application to each State within which any part of the tribe is located for review before the tribe submits the application to the Department.

(2) OPPORTUNITY FOR COMMENT.—If the Governor of a State determines that the application of a directly eligible tribe is inconsistent with the State homeland security plan of that State, or otherwise does not support the application, not later than 30 days after the date of receipt of that application, the Governor shall—

(A) notify the Secretary, in writing, of that fact; and

(B) provide an explanation of the reason for not supporting the application.

(d) FINAL AUTHORITY.—The Secretary shall have final authority to approve any application of a directly eligible tribe. The Secretary shall notify each State within the boundaries of which any part of a directly eligible tribe is located of the approval of an application by the tribe.

(e) PRIORITIZATION.—The Secretary shall allocate funds to directly eligible tribes in accordance with the factors applicable to allocating funds among States under section 12707 of this title.

(f) DISTRIBUTION OF AWARDS TO DIRECTLY ELIGIBLE TRIBES.—If the Secretary awards funds to a directly eligible tribe under this section, the Secretary shall distribute the grant funds directly to the tribe and not through any State.

(g) MINIMUM ALLOCATION.—

(1) IN GENERAL.—In allocating funds under this section, the Secretary shall ensure that, for each fiscal year, directly eligible tribes collectively receive, from the funds appropriated for the State Homeland Security Grant Program established under section 12704 of this title, not less than an amount equal to 0.1 percent of the total funds appropriated for grants under sections 12703 and 12704 of this title.

(2) EXCEPTION.—This subsection shall not apply in any fiscal year in which the Secretary—

(A) receives fewer than 5 applications under this section; or

(B) does not approve at least 2 applications under this section.

(h) TRIBAL LIAISON.—A directly eligible tribe applying for a grant under section 12704 of this title shall designate an individual to serve as a tribal liaison with the Department and other Federal, State, local, and regional government officials concerning preventing, preparing for, protecting against, and responding to acts of terrorism.

(i) ELIGIBILITY FOR OTHER FUNDS.—A directly eligible tribe that receives a grant under section 12704 of this title may receive funds for other purposes under a grant from the State or States within the boundaries of which any part of the tribe is located and from any high-risk urban area of which it is a part, consistent with the homeland security plan of the State or high-risk urban area.

(j) STATE OBLIGATIONS.—

(1) IN GENERAL.—States are responsible for allocating grant funds received under section 12704 of this title to tribal governments in order to help those tribal communities achieve target capabilities not achieved through grants to directly eligible tribes.

(2) DISTRIBUTION OF GRANT FUNDS.—With respect to a grant to a State under section 12704 of this title, an Indian tribe shall be eligible for funding directly from that State, and shall not be required to seek funding from any local government.

(3) IMPOSITION OF REQUIREMENTS.—A State may not impose unreasonable or unduly burdensome requirements on an Indian tribe as a condition of providing the Indian tribe with grant funds or resources under section 12704 of this title.

(k) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to affect the authority of an Indian tribe that receives funds under this subchapter.

§ 12706. Terrorism prevention

(a) LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM.—

(1) IN GENERAL.—The Secretary, acting through the Administrator, shall ensure that not less than 25 percent of the total combined funds

appropriated for grants under sections 12703 and 12704 of this title is used for law enforcement terrorism prevention activities.

(2) LAW ENFORCEMENT TERRORISM PREVENTION ACTIVITIES.—Law enforcement terrorism prevention activities include—

(A) information sharing and analysis;

(B) target hardening;

(C) threat recognition;

(D) terrorist interdiction;

(E) training exercises to enhance preparedness for and response to mass casualty and active shooter incidents and security events at public locations, including airports and mass transit systems;

(F) overtime expenses consistent with a State homeland security plan, including for the provision of enhanced law enforcement operations in support of Federal agencies, including for increased border security and border crossing enforcement;

(G) establishing, enhancing, and staffing with appropriately qualified personnel, State, local, and regional fusion centers that comply with the guidelines established under section 10512(j) of this title;

(H) paying salaries and benefits for personnel, including individuals employed by the grant recipient on the date of the relevant grant application, to serve as qualified intelligence analysts;

(I) any other activity permitted under the Fiscal Year 2007 Program Guidance of the Department for the Law Enforcement Terrorism Prevention Program; and

(J) any other terrorism prevention activity authorized by the Secretary.

(3) PARTICIPATION OF UNDERREPRESENTED COMMUNITIES IN FUSION CENTERS.—The Secretary shall ensure that grant funds described in paragraph (1) are used to support the participation in fusion centers, as appropriate, of law enforcement and other emergency response providers from rural and other underrepresented communities at risk from acts of terrorism.

(b) OFFICE FOR STATE AND LOCAL LAW ENFORCEMENT.—

(1) ESTABLISHMENT.—There is in the Policy Directorate of the Department the Office for State and Local Law Enforcement.

(2) ASSISTANT SECRETARY FOR STATE AND LOCAL LAW ENFORCEMENT.—The Assistant Secretary for State and Local Law Enforcement—

(A) is the head of the Office for State and Local Law Enforcement; and

(B) shall have an appropriate background with experience in law enforcement, intelligence, and other counterterrorism functions.

(3) ASSIGNMENT OF PERSONNEL.—The Secretary shall assign to the Office for State and Local Law Enforcement permanent staff and, as appropriate and consistent with sections 10311(a), 10312(b)(2), and 11306(b)(2) of this title, other appropriate personnel detailed from other components of the Department to carry out the responsibilities under this subsection.

(4) RESPONSIBILITIES.—The Assistant Secretary for State and Local Law Enforcement shall—

(A) lead the coordination of Department-wide policies relating to the role of State and local law enforcement in preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other man-made disasters within the United States;

(B) serve as a liaison between State, local, and tribal law enforcement agencies and the Department;

(C) coordinate with the Office of Intelligence and Analysis to ensure the intelligence and information sharing requirements of State, local, and tribal law enforcement agencies are being addressed;

(D) work with the Secretary to ensure that law enforcement and terrorism-focused grants to State, local, and tribal government agencies, including grants under sections 12703 and 12704 of this title, the Commercial Equipment Direct Assistance Program, and other grants administered by the Department to support fusion centers and law enforcement-oriented programs, are appropriately focused on terrorism prevention activities;

(E) coordinate with the Directorate of Science and Technology, the Federal Emergency Management Agency, the Department of Justice, the National Institute of Justice, law enforcement organizations, and other appropriate entities to support the development, promulgation, and updating, as necessary, of national voluntary consensus standards for training and personal protective equipment to be used in a tactical environment by law enforcement officers; and

(F) conduct, jointly with the Secretary, a study to determine the efficacy and feasibility of establishing specialized law enforcement deployment teams to assist State, local, and tribal governments in responding to natural disasters, acts of terrorism, or other man-

made disasters and report on the results of that study to the appropriate committees of Congress.

(5) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to diminish, supersede, or replace the responsibilities, authorities, or role of the Secretary.

§ 12707. Prioritization

(a) IN GENERAL.—In allocating funds among States and high-risk urban areas applying for grants under section 12703 or 12704 of this title, the Secretary, acting through the Administrator, shall consider, for each State or high-risk urban area—

(1) its relative threat, vulnerability, and consequences from acts of terrorism, including consideration of—

(A) its population, including appropriate consideration of military, tourist, and commuter populations;

(B) its population density;

(C) its history of threats, including whether it has been the target of a prior act of terrorism;

(D) its degree of threat, vulnerability, and consequences related to critical infrastructure (for all critical infrastructure sectors) or key resources identified by the Secretary or the State homeland security plan, including threats, vulnerabilities, and consequences related to critical infrastructure or key resources in nearby jurisdictions;

(E) the most current threat assessments available to the Department;

(F) whether the State has, or the high-risk urban area is located at or near, an international border;

(G) whether it has a coastline bordering an ocean (including the Gulf of Mexico) or international waters;

(H) its likely need to respond to acts of terrorism occurring in nearby jurisdictions;

(I) the extent to which it has unmet target capabilities;

(J) in the case of a high-risk urban area, the extent to which that high-risk urban area includes—

(i) those incorporated municipalities, counties, parishes, and Indian tribes within the relevant eligible metropolitan area, the inclusion of which will enhance regional efforts to prevent, prepare for, protect against, and respond to acts of terrorism; and

(ii) other local and tribal governments in the surrounding area that are likely to be called upon to respond to acts of terrorism within the high-risk urban area; and

(K) such other factors as are specified in writing by the Secretary; and

(2) the anticipated effectiveness of the proposed use of the grant by the State or high-risk urban area in increasing the ability of that State or high-risk urban area to prevent, prepare for, protect against, and respond to acts of terrorism, to meet its target capabilities, and to otherwise reduce the overall risk to the high-risk urban area, the State, or the Nation.

(b) TYPES OF THREAT.—In assessing threat under this section, the Secretary shall consider the following types of threat to critical infrastructure sectors and to populations in all areas of the United States, urban and rural:

(1) Biological.

(2) Chemical.

(3) Cyber.

(4) Explosives.

(5) Incendiary.

(6) Nuclear.

(7) Radiological.

(8) Suicide bombers.

(9) Other types of threat determined relevant by the Secretary.

§ 12708. Use of funds

(a) PERMITTED USES.—The Secretary, acting through the Administrator, shall permit the recipient of a grant under section 12703 or 12704 of this title to use grant funds to achieve target capabilities related to preventing, preparing for, protecting against, and responding to acts of terrorism, consistent with a State homeland security plan and relevant local, tribal, and regional homeland security plans, including by working in conjunction with a National Laboratory (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), through—

(1) developing and enhancing homeland security, emergency management, or other relevant plans, assessments, or mutual aid agreements;

(2) designing, conducting, and evaluating training and exercises, including training and exercises conducted under sections 11312 and 20508 of this title;

(3) protecting a system or asset included on the prioritized critical infrastructure list established under section 10712(a)(2) of this title;

(4) purchasing, upgrading, storing, or maintaining equipment, including computer hardware and software;

(5) ensuring operability and achieving interoperability of emergency communications;

(6) responding to an increase in the threat level under the Homeland Security Advisory System, or to the needs resulting from a National Special Security Event;

(7) establishing, enhancing, and staffing with appropriately qualified personnel, State, local, and regional fusion centers that comply with the guidelines established under section 10512(j) of this title;

(8) enhancing school preparedness;

(9) enhancing the security and preparedness of secure and nonsecure areas of eligible airports and surface transportation systems;

(10) supporting public safety answering points;

(11) paying salaries and benefits for personnel, including individuals employed by the grant recipient on the date of the relevant grant application, to serve as qualified intelligence analysts, regardless of whether the analysts are current or new full-time employees or contract employees;

(12) paying expenses directly relating to administration of the grant, except that expenses may not exceed 3 percent of the amount of the grant;

(13) participating in any activity permitted under the Fiscal Year 2007 Program Guidance of the Department for the State Homeland Security Grant Program, the Urban Area Security Initiative (including activities permitted under the full-time counterterrorism staffing pilot), or the Law Enforcement Terrorism Prevention Program;

(14) migrating an online service (as defined in section 10881(b) of this title) to the .gov internet domain; and

(15) participating in any other appropriate activity, as determined by the Secretary.

(b) LIMITATIONS ON USE OF FUNDS.—

(1) IN GENERAL.—Funds provided under section 12703 or 12704 of this title may not be used—

(A) to supplant State or local funds, except that nothing in this paragraph shall prohibit the use of grant funds provided to a State or high-risk urban area for otherwise permissible uses under subsection (a) on the basis that a State or high-risk urban area has previously used State or local funds to support the same or similar uses; or

(B) for any State or local government cost-sharing contribution.

(2) PERSONNEL.—

(A) IN GENERAL.—Not more than 50 percent of the amount awarded to a grant recipient under section 12703 or 12704 of this title in any fiscal year may be used to pay for personnel, including overtime and backfill costs, in support of the permitted uses under subsection (a).

(B) WAIVER.—At the request of the recipient of a grant under section 12703 or 12704 of this title, the Secretary may grant a waiver of the limitation under subparagraph (A).

(3) LIMITATIONS ON DISCRETION.—

(A) IN GENERAL.—With respect to the use of amounts awarded to a grant recipient under section 12703 or 12704 of this title for personnel costs under paragraph (2), the Secretary may not—

(i) impose a limit on the amount of the award that may be used to pay for personnel, or personnel-related, costs that is higher or lower than the percent limit imposed in paragraph (2)(A); or

(ii) impose any additional limitation on the portion of the funds of a recipient that may be used for a specific type, purpose, or category of personnel, or personnel-related, costs.

(B) ANALYSTS.—If amounts awarded to a grant recipient under section 12703 or 12704 of this title are used for paying salary or benefits of a qualified intelligence analyst under subsection (a)(11), the Secretary shall make the amounts available without limitations placed on the period of time that the analyst can serve under the grant.

(4) CONSTRUCTION.—

(A) IN GENERAL.—A grant awarded under section 12703 or 12704 of this title may not be used to acquire land or to construct buildings or other physical facilities.

(B) EXCEPTIONS.—

(i) IN GENERAL.—Notwithstanding subparagraph (A), nothing in this paragraph shall prohibit the use of a grant awarded under section 12703 or 12704 of this title to achieve target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism, including through the alteration or remodeling of existing buildings for the purpose of making the buildings secure against acts of terrorism.

(ii) REQUIREMENTS FOR EXCEPTION.—No grant awarded under section 12703 or 12704 of this title may be used for a purpose described in clause (i) unless—

(I) the grant is specifically approved by the Secretary;

(II) any construction work occurs under terms and conditions consistent with the requirements under section 611(j)(9) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196(j)(9)); and

(III) the amount allocated for purposes under clause (i) does not exceed the greater of $1,000,000 or 15 percent of the grant award.

(5) RECREATION.—Grants awarded under this subchapter may not be used for recreational or social purposes.

(c) MULTIPLE-PURPOSE FUNDS.—Nothing in this subchapter shall be construed to prohibit State, local, or tribal governments from using grant funds under section 12703, 12704, and 12709 of this title in a manner that enhances preparedness for disasters unrelated to acts of terrorism, if the use assists the governments in achieving target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism.

(d) REIMBURSEMENT OF COSTS.—

(1) PAID-ON-CALL OR VOLUNTEER REIMBURSEMENT.—In addition to the activities described in subsection (a), a grant under section 12703 or 12704 of this title may be used to provide a reasonable stipend to paid-on-call or volunteer emergency response providers who are not otherwise compensated for travel to, or participation in, training or exercises related to the purposes of this subchapter. Any reimbursement shall not be considered compensation for purposes of rendering an emergency response provider an employee under the Fair Labor Standards Act of 1938 (29 U.S.C. 201 et seq.).

(2) PERFORMANCE OF FEDERAL DUTY.—An applicant for a grant under section 12703 or 12704 of this title may petition the Secretary to use the funds from its grants under those sections for the reimbursement of the cost of any activity relating to preventing, preparing for, protecting against, or responding to acts of terrorism that is a Federal duty and usually performed by a Federal agency, and that is being performed by a State or local government under agreement with a Federal agency.

(e) FLEXIBILITY IN UNSPENT HOMELAND SECURITY GRANT FUNDS.—On request by the recipient of a grant under section 12703, 12704, or 12709 of this title, the Secretary may authorize the grant recipient to trans-

fer all or part of the grant funds from uses specified in the grant agreement to other uses authorized under this section, if the Secretary determines that the transfer is in the interests of homeland security.

(f) EQUIPMENT STANDARDS.—If an applicant for a grant under section 12703 or 12704 of this title proposes to upgrade or purchase, with assistance provided under that grant, new equipment or systems that do not meet or exceed any applicable national voluntary consensus standards developed under section 20507 of this title, the applicant shall include in its application an explanation of why the equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed the standards.

§ 12709. Nonprofit Security Grant Program

(a) ESTABLISHMENT.—There is in the Department the Nonprofit Security Grant Program (in this section referred to as the ''Program''). Under the Program, the Secretary, acting through the Administrator, shall make grants to eligible nonprofit organizations described in subsection (b), through the State in which the organizations are located, for target hardening and other security enhancements to protect against terrorist attacks or other threats.

(b) ELIGIBLE RECIPIENTS.—Eligible nonprofit organizations described in this subsection are organizations that are—

(1) described in section 501(c)(3) of the Internal Revenue Code of 1986 (26 U.S.C. 501(c)(3)) and exempt from tax under section 501(a) of the Internal Revenue Code of 1986 (26 U.S.C. 501(a)); and

(2) determined by the Secretary to be at risk of terrorist attacks or other threats.

(c) PERMITTED USES.—

(1) IN GENERAL.—The recipient of a grant under this section may use the grant for any of the following:

(A) Target hardening activities, including physical security enhancement equipment, inspection, and screening systems, and alteration or remodeling of existing buildings or physical facilities.

(B) Fees for security training relating to physical security and cybersecurity, target hardening, terrorism awareness, and employee awareness.

(C) Facility security personnel costs.

(D) Expenses directly related to the administration of the grant, except that those expenses may not exceed 5 percent of the amount of the grant.

(E) Any other appropriate activity, including cybersecurity resilience activities, as determined by the Administrator.

(2) RETENTION.—Each State through which a recipient receives a grant under this section may retain not more than 5 percent of each grant for expenses directly related to the administration of the grant.

(3) OUTREACH AND TECHNICAL ASSISTANCE.—

(A) IN GENERAL.—If the Administrator establishes target allocations in determining award amounts under the Program, a State may request a project to use a portion of the target allocation for outreach and technical assistance if the State does not receive enough eligible applications from nonprofit organizations located outside high-risk urban areas.

(B) PRIORITY.—Any outreach or technical assistance described in subparagraph (A) should prioritize underserved communities and nonprofit organizations that are traditionally underrepresented in the Program.

(C) PARAMETERS.—In determining grant guidelines under subsection (g), the Administrator may determine the parameters for outreach and technical assistance.

(d) AVAILABILITY.—The Administrator shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.

(e) REPORT.—The Administrator shall annually for each of fiscal years 2023 through 2028 submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report containing information on the following:

(1) The expenditure by each grant recipient of grant funds made available under this section.

(2) The number of applications submitted by eligible nonprofit organizations to each State.

(3) The number of applications submitted by each State to the Administrator.

(4) The operations of the program office of the Program, including staffing resources and efforts with respect to subparagraphs (A) through (D) of subsection (c)(1).

(f) ADMINISTRATION .—Not later than 120 days after December 23, 2022, the Administrator shall ensure that in the Federal Emergency Management Agency a program office for the program (in this subsection referred to as the ''program office'') shall—

(1) be headed by a senior official of the Federal Emergency Management Agency; and

(2) administer the Program (including, where appropriate, in coordination with States) including relating to—

(A) outreach, engagement, education, and technical assistance and support to eligible nonprofit organizations described in subsection (b), with particular attention to those organizations in underserved communities before, during, and after the awarding of grants, including web-based training videos for eligible nonprofit organizations that prepare guidance on preparing an application and the environmental planning and historic preservation process;

(B) the establishment of mechanisms to ensure program office processes are conducted in accordance with constitutional, statutory, and regulatory requirements that protect civil rights and civil liberties and advance equal access for members of underserved communities;

(C) the establishment of mechanisms for the Administrator to provide feedback to eligible nonprofit organizations that do not receive grants;

(D) the establishment of mechanisms to identifyand collect data to measure the effectiveness of grants under the Program;

(E) the establishment and enforcement of standardized baseline operational requirements for States, including requirements for States to eliminate or prevent any administrative or operational obstacles that may impact eligible nonprofit organizations described in subsection (b) from receiving grants under the Program;

(F) carrying out efforts to prevent waste, fraud, and abuse, including through audits of grantees; and

(G) promoting diversity in the types and locations of eligible nonprofit organizations that are applying for grants under the Program.

(g) GRANT GUIDELINES.—For each fiscal year, before awarding grants under this section, the Administrator—

(1) shall publish guidelines, including a notice of funding opportunity or similar announcement, as the Administrator determines appropriate; and

(2) may prohibit States from closing application processes before the publication of those guidelines.

(h) NONAPPLICATION OF CHAPTER 35 OF TITLE 44.—Chapter 35 of title 44 shall not apply to any changes to the application materials, Program forms, or other core Program documentation intended to enhance participation by eligible nonprofit organizations in the Program.

(i) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There is authorized to be appropriated $360,000,000 for each of fiscal years 2023 through 2028 under this section, of which—

(A) $180,000,000 each fiscal year shall be for recipients in high-risk urban areas that receive funding under section 12703 of this title; and

(B) $180,000,000 each fiscal year shall be for recipients in jurisdictions that do not receive funding under section 12703 of this title.

(2) OPERATION AND SUPPORT.—There is authorized to be appropriated $18,000,000 for each of fiscal years 2023 through 2028 for Operations and Support at the Federal Emergency Management Agency for costs incurred for the management and administration (including evaluation) of this section.

Part B—Administration

§ 12721. Administration and coordination

(a) REGIONAL COORDINATION.—The Administrator shall ensure that—

(1) all recipients of grants administered by the Department to prevent, prepare for, protect against, or respond to natural disasters, acts of terrorism, or other man-made disasters (excluding assistance provided under section 203 or title IV or V of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et seq., 5191 et seq.)) coordinate, as appropriate, their prevention, preparedness, and protection efforts with neighboring State, local, and tribal governments; and

(2) all high-risk urban areas and other recipients of grants administered by the Department to prevent, prepare for, protect against, or respond to natural disasters, acts of terrorism, or other man-made disasters (excluding assistance provided under section 203 or title IV or V of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et seq., 5191 et seq.)) that include or substantially affect parts or all of more than one State coordinate, as appropriate, across State boundaries, including, where appropriate, through the use of regional working groups and requirements for regional plans.

(b) PLANNING COMMITTEES.—

(1) IN GENERAL.—Any State or high-risk urban area receiving a grant under section 12703 or 12704 of this title shall establish a State planning committee or urban area working group to assist in preparation and revision of the State, regional, or local homeland security plan or the threat and hazard identification and risk assessment and to as-

sist in determining effective funding priorities for grants under sections 12703 and 12704 of this title.

(2) COMPOSITION.—

(A) IN GENERAL.—The State planning committees and urban area working groups shall include at least 1 representative from each of the following significant stakeholders:

(i) Local or tribal government officials.

(ii) Emergency response providers, which shall include representatives of fire service, law enforcement, emergency medical services, and emergency managers.

(iii) Public health officials and other appropriate medical practitioners.

(iv) Individuals representing educational institutions, including elementary schools, community colleges, and other institutions of higher learning.

(v) State and regional interoperable communications coordinators, as appropriate.

(vi) State and major urban area fusion centers, as appropriate.

(B) GEOGRAPHIC REPRESENTATION.—The members of the State planning committee or urban area working group shall be a representative group of individuals from the counties, cities, towns, and Indian tribes in the State or high-risk urban area, including, as appropriate, representatives of rural, high-population, and high-threat jurisdictions.

(3) EXISTING PLANNING COMMITTEES.—Nothing in this subsection may be construed to require that any State or high-risk urban area create a State planning committee or urban area working group if that State or high-risk urban area has established and uses a multijurisdictional planning committee or commission that meets the requirements of this subsection.

§ 12722. Accountability

(a) AUDITS OF GRANT PROGRAMS.—

(1) COMPLIANCE REQUIREMENTS.—

(A) AUDIT REQUIREMENT.—Each recipient of a grant administered by the Department that expends not less than $500,000 in Federal funds during its fiscal year shall submit to the Secretary, through the Administrator, a copy of the organization-wide financial and compliance audit report required under chapter 75 of title 31.

(B) ACCESS TO INFORMATION.—The Department and each recipient of a grant administered by the Department shall provide the Comptroller General and any officer or employee of the Government Accountability Office with full access to information regarding the activities carried out that are related to any grant administered by the Department.

(C) IMPROPER PAYMENTS.—Consistent with subchapter IV of chapter 33 of title 31, for each of the grant programs under sections 12703, 12704, and 20522 of this title, the Secretary shall specify policies and procedures for—

(i) identifying activities funded under a grant program that are susceptible to significant improper payments; and

(ii) reporting any improper payments to the Department.

(2) AGENCY PROGRAM REVIEW.—

(A) IN GENERAL.—The Secretary shall biennially conduct, for each State and high-risk urban area receiving a grant administered by the Department, a programmatic and financial review of all grants awarded by the Department to prevent, prepare for, protect against, or respond to natural disasters, acts of terrorism, or other man-made disasters, excluding assistance provided under section 203, title IV, or title V of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et seq., 5191 et seq.).

(B) CONTENTS.—Each review under subparagraph (A) shall, at a minimum, examine—

(i) whether the funds awarded were used in accordance with the law, program guidance, and State homeland security plans or other applicable plans; and

(ii) the extent to which funds awarded enhanced the ability of a grantee to prevent, prepare for, protect against, and respond to natural disasters, acts of terrorism, and other man-made disasters.

(C) AUTHORIZATION OF APPROPRIATIONS.—In addition to any other amounts authorized to be appropriated to the Secretary, there are authorized to be appropriated to the Secretary for reviews under this paragraph such sums as may be necessary.

(3) PERFORMANCE ASSESSMENT.—In order to ensure that States and high-risk urban areas are using grants administered by the Department appropriately to meet target capabilities and preparedness priorities, the Secretary shall—

(A) ensure that each State or high-risk urban area conducts or participates in exercises under section 20508(b) of this title;

(B) use performance metrics in accordance with the comprehensive assessment system under section 20509 of this title and ensure that each State or high-risk urban area regularly tests its progress against the metrics through the exercises required under subparagraph (A);

(C) use the remedial action management program under section 20510 of this title; and

(D) ensure that each State receiving a grant administered by the Department submits a report to the Administrator on its level of preparedness, as required by section 20512(c) of this title.

(4) CONSIDERATION OF ASSESSMENTS.—In conducting program reviews and performance audits under paragraph (2), the Secretary and the Inspector General of the Department shall take into account the performance assessment elements required under paragraph (3).

(5) RECOVERY AUDITS.—The Secretary shall conduct a recovery audit under section 3352(i) of title 31 for a grant administered by the Department with a total value of not less than $1,000,000, if the Secretary finds that—

(A) a financial audit has identified improper payments that can be recouped; and

(B) it is cost-effective to conduct a recovery audit to recapture the targeted funds.

(6) REMEDIES FOR NONCOMPLIANCE.—

(A) IN GENERAL.—If, as a result of a review or audit under this subsection or otherwise, the Secretary finds that a recipient of a grant under this subchapter has failed to substantially comply with any provision of law or with any regulations or guidelines of the Department regarding eligible expenditures, the Secretary shall—

(i) reduce the amount of payment of grant funds to the recipient by an amount equal to the amount of grants funds that were not properly expended by the recipient;

(ii) limit the use of grant funds to programs, projects, or activities not affected by the failure to comply;

(iii) refer the matter to the Inspector General of the Department for further investigation;

(iv) terminate any payment of grant funds to be made to the recipient; or

(v) take other actions the Secretary determines appropriate.

(B) DURATION OF PENALTY.—The Secretary shall apply an appropriate penalty under subparagraph (A) until the Secretary determines that the grant recipient is in full compliance with the law and with applicable guidelines or regulations of the Department.

(b) REPORTS BY GRANT RECIPIENTS.—

(1) QUARTERLY REPORTS ON HOMELAND SECURITY SPENDING.—

(A) IN GENERAL.—As a condition of receiving a grant under section 12703 or 12704 of this title, a State, high-risk urban area, or directly eligible tribe shall, not later than 30 days after the end of each Federal fiscal quarter, submit to the Secretary a report on activities performed using grant funds during that fiscal quarter.

(B) CONTENTS.—Each report submitted under subparagraph (A) shall at a minimum include, for the applicable State, high-risk urban area, or directly eligible tribe, and each subgrantee thereof—

(i) the amount obligated to that recipient under section 12703 or 12704 of this title in that quarter;

(ii) the amount of funds received and expended under section 12703 or 12704 of this title by that recipient in that quarter; and

(iii) a summary description of expenditures made by that recipient using the funds, and the purposes for which the expenditures were made.

(C) END–OF–YEAR REPORT.—The report submitted under subparagraph (A) by a State, high-risk urban area, or directly eligible tribe relating to the last quarter of any fiscal year shall include—

(i) the amount and date of receipt of all funds received under the grant during that fiscal year;

(ii) the identity of, and amount provided to, any subgrantee for that grant during that fiscal year;

(iii) the amount and the dates of disbursements of funds expended in compliance with section 12721(a)(1) of this title or under mutual aid agreements or other sharing arrangements that apply within the State, high-risk urban area, or directly eligible tribe, as applicable, during that fiscal year; and

(iv) an explanation of how the funds were used by each recipient or subgrantee during that fiscal year.

(2) ANNUAL STATE PREPAREDNESS REPORT.—Any State applying for a grant under section 12704 of this title shall submit to the Administrator annually a State preparedness report, as required by section 20512(c) of this title.

(3) ANNUAL REPORT ON EXPENDITURES.—

(A) DEFINITION OF HOMELAND SECURITY GRANT.—In this paragraph, the term ''homeland security grant'' means any grant made or administered by the Department, including—

(i) the State Homeland Security Grant Program;

(ii) the Urban Area Security Initiative Grant Program;

(iii) the Law Enforcement Terrorism Prevention Program;

(iv) the Citizen Corps; and

(v) the Metropolitan Medical Response System.

(B) LIST OF EXPENDITURES.—Not later than 12 months after the date of receipt of the grant, and every 12 months thereafter until all funds provided under the grant are expended, each State or local government that receives a homeland security grant shall submit a report to the Secretary that contains a list of all expenditures made by the State or local government using funds from the grant.

(c) REPORTS BY THE ADMINISTRATOR.—

(1) FEDERAL PREPAREDNESS REPORT.—The Administrator shall submit to the appropriate committees of Congress annually the Federal Preparedness Report required under section 20512(a) of this title.

(2) RISK ASSESSMENT.—

(A) IN GENERAL.—For each fiscal year, the Administrator shall provide to the appropriate committees of Congress a detailed and comprehensive explanation of the methodologies used to calculate risk and compute the allocation of funds for grants administered by the Department, including—

(i) all variables included in the risk assessment and the weights assigned to each variable;

(ii) an explanation of how each variable, as weighted, correlates to risk, and the basis for concluding there is a correlation; 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 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.

§ 12723. 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 12703 of this title, grants awarded under section 12704 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);

(B) a reassessment of the reporting requirements to identify and eliminate redundant and unnecessary requirements;

(2) the status of efforts to develop quantifiable performance measures and metrics to assess the effectiveness of the programs under which the covered grants are awarded, including—

(A) progress made in implementing the plan required under subsection (b)(2); and

(B) progress made in developing and implementing additional performance metrics and measures for grants, including as part of the comprehensive assessment system required under section 20509 of this title; and

(3) a performance assessment of each program under which the covered grants are awarded, including—

(A) a description of the objectives and goals of the program;

(B) an assessment of the extent to which the objectives and goals described in subparagraph (A) have been met, based on the quantifiable performance measures and metrics required under this section and sections 12722(a)(3) and 20509 of this title;

(C) recommendations for any program modifications to improve the effectiveness of the program, to address changed or emerging conditions; and

(D) an assessment of the experience of recipients of covered grants, including the availability of clear and accurate information, the timeliness of reviews and awards, and the provision of technical assistance, and recommendations for improving that experience.

(d) GRANTS PROGRAM MEASUREMENT STUDY.—The National Academy of Public Administration shall assist the Administrator in implementing—

(1) quantifiable performance measures and metrics to assess the effectiveness of grants administered by the Department, as required under this section and section 20509 of this title; and

(2) the plan required under subsection (b)(2).

Subchapter II—Grants To Address Cybersecurity Risks and Cybersecurity Threats to Information Systems

§ 12731. Definitions

In this subchapter:

(1) CYBERSECURITY PLAN.—The term ''Cybersecurity Plan'' means a plan submitted by an eligible entity under section 12735(a) of this title.

(2) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(3) ELIGIBLE ENTITY.—The term ''eligible entity'' means a—

(A) State; or

(B) Tribal government.

(4) MULTI-ENTITY GROUP.—The term ''multi-entity group'' means a group of 2 or more eligible entities desiring a grant under this subchapter.

(5) ONLINE SERVICE.—The term ''online service'' means an internet-facing service, including a website, email, virtual private network, or custom application.

(6) RURAL AREA.—The term ''rural area'' has the meaning given the term in section 5302 of title 49.

(7) STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.—The term ''State and Local Cybersecurity Grant Program'' means the program established under section 12732 of this title.

(8)TRIBAL GOVERNMENT.—The term ''Tribal government'' means the recognized governing body of an Indian or Alaska Native Tribe, band, nation, pueblo, village, community, component band, or component reservation, that is individually identified (including parenthetically) in the most recent list published pursuant to Section 104 of the Federally Recognized Indian Tribe List Act of 1994 (25 U.S.C. 5131).

§ 12732. Program

(a) ESTABLISHMENT.—There is in the Department a program to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, State, local, or Tribal governments.

(b) APPLICATION.—An eligible entity desiring a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

§ 12733. Administration

The State and Local Cybersecurity Grant Program shall be administered in the same office of the Department that administers grants made under sections 12702 and 12703 of this title.

§ 12734. Use of funds

An eligible entity that receives a grant under this subchapter and a local government that receives funds from a grant under this subchapter, as appropriate, shall use the grant to—

(1) implement the Cybersecurity Plan of the eligible entity;

(2) develop or revise the Cybersecurity Plan of the eligible entity;

(3) pay expenses directly relating to the administration of the grant, which shall not exceed 5 percent of the amount of the grant;

(4) assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity; or

(5) fund any other appropriate activity determined by the Secretary, acting through the Director.

§ 12735. Cybersecurity plans

(a) SUBMISSION OF PLAN TO SECRETARY.—An eligible entity applying for a grant under this subchapter shall submit to the Secretary a Cybersecurity Plan for review in accordance with section 12739 of this title.

(b) REQUIRED ELEMENTS.—A Cybersecurity Plan of an eligible entity shall—

(1) incorporate, to the extent practicable—

(A) any existing plans of the eligible entity to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, State, local, or Tribal governments; and

(B) if the eligible entity is a State, consultation and feedback from local governments and associations of local governments within the jurisdiction of the eligible entity;

(2) describe, to the extent practicable, how the eligible entity will—

(A) manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology;

(B) monitor, audit, and, track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity;

(C) enhance the preparation, response, and resiliency of information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, against cybersecurity risks and cybersecurity threats;

(D) implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the

eligible entity is a State, local governments within the jurisdiction of the eligible entity;

(E) ensure that the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, adopt and use best practices and methodologies to enhance cybersecurity, such as—

(i) the practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology;

(ii) cybersecurity supply chain risk management best practices identified by the National Institute of Standards and Technology; and

(iii) knowledge bases of adversary tools and tactics;

(F) promote the delivery of safe, recognizable, and trustworthy online services by the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, including through the use of the .gov internet domain;

(G) ensure continuity of operations of the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident;

(H) use the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity developed by the National Institute of Standards and Technology to identify and mitigate any gaps in the cybersecurity workforces of the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training;

(I) if the eligible entity is a State, ensure continuity of communications and data networks within the jurisdiction of the eligible entity between the eligible entity and local governments within the jurisdiction of the eligible entity in the event of an incident involving those communications or data networks;

(J) assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact

the performance of information systems within the jurisdiction of the eligible entity;

(K) enhance capabilities to share cyber threat indicators and related information between the eligible entity and—

(i) if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, including by expanding information sharing agreements with the Department; and

(ii) the Department;

(L) leverage cybersecurity services offered by the Department;

(M) implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;

(N) develop and coordinate strategies to address cybersecurity risks and cybersecurity threats in consultation with—

(i) if the eligible entity is a State, local governments and associations of local governments within the jurisdiction of the eligible entity; and

(ii) as applicable—

(I) eligible entities that neighbor the jurisdiction of the eligible entity or, as appropriate, members of an Information Sharing and Analysis Organization; and

(II) countries that neighbor the jurisdiction of the eligible entity;

(O) ensure adequate access to, and participation in, the services and programs described in this paragraph by rural areas within the jurisdiction of the eligible entity; and

(P) distribute funds, items, services, capabilities, or activities to local governments under 12744(b)(1) of this title, including the fraction of that distribution the eligible entity plans to distribute to rural areas under subsection 12744(b)(2) of this title;

(3) assess the capabilities of the eligible entity relating to the actions described in paragraph (2);

(4) describe, as appropriate and to the extent practicable, the individual responsibilities of the eligible entity and local governments within the jurisdiction of the eligible entity in implementing the plan;

(5) outline, to the extent practicable, the necessary resources and a timeline for implementing the plan; and

(6) describe the metrics the eligible entity will use to measure progress towards—

(A) implementing the plan; and

(B) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.

(c) DISCRETIONARY ELEMENTS.—In drafting a Cybersecurity Plan, an eligible entity may—

(1) consult with the Multi-State Information Sharing and Analysis Center;

(2) include a description of cooperative programs developed by groups of local governments within the jurisdiction of the eligible entity to address cybersecurity risks and cybersecurity threats; and

(3) include a description of programs provided by the eligible entity to support local governments and owners and operators of critical infrastructure to address cybersecurity risks and cybersecurity threats.

§ 12736. Multi-entity grants

(a) IN GENERAL.—The Secretary may award grants under this section to a multi-entity group to support multi-entity efforts to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions of the eligible entities that comprise the multi-entity group.

(b) REQUIREMENTS.—To be eligible for a multi-entity grant under this section, each eligible entity that comprises a multi-entity group shall have—

(1) a Cybersecurity Plan that has been reviewed by the Secretary in accordance with section 12739 of this title; and

(2) a cybersecurity planning committee established in accordance with section 12737 of this title.

(c) APPLICATION.—

(1) IN GENERAL.—A multi-entity group applying for a multi-entity grant under subsection (a) shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(2) MULTI-ENTITY PROJECT PLAN.—An application for a grant under this subchapter of a multi-entity group under paragraph (1) shall include a plan describing—

(A) the division of responsibilities among the eligible entities that comprise the multi-entity group;

(B) the distribution of funding from the grant among the eligible entities that comprise the multi-entity group; and

(C) how the eligible entities that comprise the multi-entity group will work together to implement the Cybersecurity Plan of each of those eligible entities.

§ 12737. Planning committees

(a) IN GENERAL.—An eligible entity that receives a grant under this subchapter shall establish a cybersecurity planning committee to—

(1) assist with the development, implementation, and revision of the Cybersecurity Plan of the eligible entity;

(2) approve the Cybersecurity Plan of the eligible entity; and

(3) assist with the determination of effective funding priorities for a grant under this section in accordance with sections 12734 and 12740 of this title.

(b) COMPOSITION.—A committee of an eligible entity established under subsection (a) shall—

(1) be comprised of representatives from—

(A) the eligible entity;

(B) if the eligible entity is a State, counties, cities, and towns within the jurisdiction of the eligible entity; and

(C) institutions of public education and health within the jurisdiction of the eligible entity; and

(2) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

(c) CYBERSECURITY EXPERTISE.—Not less than 1/2 of the representatives of a committee established under subsection (a) shall have professional experience relating to cybersecurity or information technology.

(d) RULE OF CONSTRUCTION REGARDING EXISTING PLANNING COMMITTEES.—Nothing in this section shall be construed to require an eligible entity to establish a cybersecurity planning committee if the eligible entity has established and uses a multijurisdictional planning committee or commission that—

(1) meets the requirements of this section; and

(2) may be expanded or leveraged to meet the requirements of this section, including through the formation of a cybersecurity planning subcommittee.

(e) RULE OF CONSTRUCTION REGARDING CONTROL OF INFORMATION SYSTEMS IF ELIGIBLE ENTITIES.—Nothing in this section shall be construed to permit a cybersecurity planning committee of an eligible entity that meets the requirements of this section to make decisions relating to information systems owned or operated by, or on behalf of, the eligible entity.

§ 12738. Special rule for Tribal governments

With respect to any requirement under section 12735 or 12737 of this title, the Secretary, in consultation with the Secretary of the Interior and Tribal governments, may prescribe an alternative substantively similar re-

quirement for Tribal governments if the Secretary finds that the alternative requirement is necessary for the effective delivery and administration of grants to Tribal governments under this subchapter.

§ 12739. Review of plans

(a) REVIEW AS CONDITION OF GRANT.—

(1) IN GENERAL.—Subject to subsection (c), before an eligible entity may receive a grant under this subchapter, the Secretary, acting through the Director, shall—

(A) review the Cybersecurity Plan of the eligible entity, including any revised Cybersecurity Plans of the eligible entity; and

(B) determine that the Cybersecurity Plan reviewed under subparagraph (A) satisfies the requirements under subsection (b).

(2) DURATION OF DETERMINATION.—In the case of a determination under paragraph (1)(B) that a Cybersecurity Plan satisfies the requirements under subsection (b), the determination shall be effective for the 2-year period beginning on the date of the determination.

(3) ANNUAL RENEWAL.—Not later than 2 years after the date on which the Secretary determines under paragraph (1)(B) that a Cybersecurity Plan satisfies the requirements under subsection (b), and annually thereafter, the Secretary, acting through the Director, shall—

(A) determine whether the Cybersecurity Plan and any revisions continue to meet the criteria described in subsection (b); and

(B) renew the determination if the Secretary, acting through the Director, makes a positive determination under subparagraph (A).

(b) PLAN REQUIREMENTS.—In reviewing a Cybersecurity Plan of an eligible entity under this section, the Secretary, acting through the Director, shall ensure that the Cybersecurity Plan—

(1) satisfies the requirements of section 12735(b) of this title; and

(2) has been approved by—

(A) the cybersecurity planning committee of the eligible entity established under section 12737 of this title; and

(B) the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity.

(c) EXCEPTION.—Notwithstanding subsection (a) and section 12735 of this title, the Secretary may award a grant under this section to an eligible entity that does not submit a Cybersecurity Plan to the Secretary for review before September 30, 2023, if the eligible entity certifies to the Secretary that—

(1 the activities that will be supported by the grant are—

(A) integral to the development of the Cybersecurity Plan of the eligible entity; or

(B) necessary to assist with activities described in section 12734(4) of this title, as confirmed by the Director; and

(2) the eligible entity will submit to the Secretary a Cybersecurity Plan for review under this section by September 30, 2023.

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide authority to the Secretary to—

(1) regulate the manner by which an eligible entity or local government improves the cybersecurity of the information systems owned or operated by, or on behalf of, the eligible entity or local government; or

(2) condition the receipt of grants under this subchapter on—

(A) participation in a particular Federal program; or

(B) the use of a specific product or technology.

§ 12740. Limitation of use of funds

(a) IN GENERAL.—An entity that receives funds from a grant under this subchapter may not use the grant—

(1) to supplant State or local funds;

(2) for a recipient cost-sharing contribution;

(3) to pay a ransom;

(4) for recreational or social purposes; or

(5) for a purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity.

(b) COMPLIANCE OVERSIGHT.—In addition to any other remedy available, the Secretary may take such actions as are necessary to ensure that a recipient of a grant under this subchapter uses the grant for the purposes for which the grant is awarded.

(c) RULE OF CONSTRUCTION.—Nothing in subsection (a)(1) shall be construed to prohibit the use of funds from a grant under this subchapter awarded to a State, local, or Tribal government for otherwise permissible uses under this subchapter on the basis that the State, local, or Tribal government has previously used State, local, or Tribal funds to support the same or similar uses.

§ 12741. Opportunity to amend applications

In considering applications for grants under this subchapter, the Secretary shall provide applicants with a reasonable opportunity to correct any defects in those applications before making final awards, including by allowing applicants to revise a submitted Cybersecurity Plan.

§ 12742. Apportionment

For each fiscal year, the Secretary shall apportion amounts appropriated to carry out this subchapter among eligible entities as follows:

(1) BASELINE AMOUNT.—The Secretary shall first apportion—

(A) 0.25 percent of the amounts to each of Guam, American Samoa, the Virgin Islands, and the Northern Mariana Islands;

(B) 1 percent of the amounts to each of the remaining States; and

(C) 3 percent of the amounts to Tribal Governments.

(2) REMAINDER.—The Secretary shall apportion the remainder of the amounts to States as follows:

(A) 50 percent of the remainder in the ratio that the population of each State bears to the population of all States; and

(B) 50 percent of the remainder in the ratio that the population of each State that resides in rural areas bears to the population of all States that resides in rural areas.

(3) AMONG TRIBAL GOVERNMENTS.—In determining how to apportion amounts to Trial governments under paragraph (1)(C), the Secretary shall consult with the Secretary of the Interior and Trial governments.

(4) MULTI-ENTITY GRANTS.—An amount received from a multi-entity grant awarded under section 12736(a) of this title by a State or Tribal government that is a member of a multi-entity group shall qualify as an apportionment for the purposes of this section.

§ 12743. Federal share

(a) IN GENERAL.—The Federal share of the cost of an activity carried out using funds made available with a grant under this subchapter may not exceed—

(1) in the case of a grant to a Federal entity—

(A) for fiscal year 2023, 80 percent;

(B) for fiscal year 2024, 70 percent; and

(C) for fiscal year 2025, 60 percent; and

(2) in the case of a grant to a multi-entity group—

(A) for fiscal year 2023, 90 percent;

(B) for fiscal year 2024, 80 percent; and

(C) for fiscal year 2025, 70 percent.

(b) WAIVER.—

(1) IN GENERAL.—The Secretary may waive or modify the requirements of subsection (a) if an eligible entity or multi-entity group demonstrates economic hardship.

(2) GUIDELINES.—The Secretary shall establish and publish guidelines for determining what constitutes economic hardship for the purposes of this section.

(3) CONSIDERATIONS.—In developing guidelines under paragraph (2), the Secretary shall consider, with respect to the jurisdiction of an eligible entity—

(A) changes in rates of unemployment in the jurisdiction from previous years;

(B) changes in the percentage of individuals who are eligible to receive benefits under the supplemental nutrition assistance program established under the Food and Nutrition Act of 2008 (7 U.S.C. 2011 et seq.) from previous years; and

(C) any other factors the Secretary considers appropriate.

(c) WAIVER FOR TRIBAL GOVERNMENTS.—Notwithstanding subsection (b), the Secretary, in consultation with the Secretary of the Interior and Tribal governments, may waive or modify the requirements of subsection (a) for 1 or more Tribal governments if the Secretary determines that the waiver is in the public interest.

§ 12744. Responsibilities of grantees

(a) CERTIFICATION.—Each eligible entity or multi-entity group that receives a grant under this subchapter shall certify to the Secretary that the grant will be used—

(1) for the purpose for which the grant is awarded; and

(2) in compliance with sections 12734 and 12740 of this title.

(b) AVAILABILITY OF FUNDS TO LOCAL GOVERNMENTS AND RURAL AREAS.—

(1) IN GENERAL.—Subject to paragraph (3), not later than 45 days after the date on which an eligible entity or multi-entity group receives a grant under this subchapter, the eligible entity or multi-entity group shall, without imposing unreasonable or unduly burdensome requirements as a condition of receipt, obligate or otherwise make available to local governments within the jurisdiction of the eligible entity or the eligible entities that comprise the multi-entity group—

(A) not less than 80 percent of funds available under the grant;

(B) with the consent of the local governments, items, services, capabilities, or activities having a value of not less than 80 percent of the amount of the grant; or

(C) with the consent of the local governments, grant funds combined with other items, services, capabilities, or activities having a total value of not less than 80 percent of the amount of the grant.

(2) AVAILABILITY TO RURAL AREAS.—In obligating funds, items, services, capabilities, or activities to local governments under paragraph (1), the eligible entity or eligible entities that comprise the multi-entity group shall ensure that rural areas within the jurisdiction of the eligible entity or the eligible entities that comprise the multi-entity group receive—

(A) not less than 25 percent of the amount of the grant awarded to the eligible entity;

(B) items, services, capabilities, or activities having a value of not less than 25 percent of the amount of the grant awarded to the eligible entity; or

(C) grant funds combined with other items, services, capabilities, or activities having a total value of not less than 25 percent of the grant awarded to the eligible entity.

(3) EXCEPTIONS.—This subsection shall not apply to—

(A) a grant awarded under this subchapter that solely supports activities that are integral to the development or revision of the Cybersecurity Plan of the eligible entity; or

(B) the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, the Northern Mariana Islands, or a Tribal government.

(c) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO LOCAL GOVERNMENTS.—An eligible entity or multi-entity group shall certify to the Secretary that the eligible entity or multi-entity group has made the distribution to local governments required under subsection (b).

(d) EXTENSION OF PERIOD.—

(1) IN GENERAL.—An eligible entity or multi-entity group may request in writing that the Secretary extend the period of time specified in subsection (b) for an additional period of time.

(2) APPROVAL.—The Secretary may approve a request for an extension under paragraph (1) if the Secretary determines the extension is necessary to ensure that the obligation and expenditure of grant funds align with the purpose of the State and Local Cybersecurity Grant Program.

(e) DIRECT FUNDING.—If an eligible entity does not make a distribution to a local government required under subsection (b) in a timely fashion, the local government may petition the Secretary to request the Secretary to provide funds directly to the local government.

(f) LIMITATION ON CONSTRUCTION.—A grant awarded under this subchapter may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities.

(g) CONSULTATION IN ALLOCATING FUNDS.—An eligible entity applying for a grant under this subchapter shall agree to consult the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity in allocating funds from a grant awarded under this subchapter.

(h) PENALTIES.—In addition to other remedies available to the Secretary, if an eligible entity violates a requirement of this section, the Secretary may—

(1) terminate or reduce the amount of a grant awarded under this subchapter to the eligible entity; or

(2) distribute grant funds previously awarded to the eligible entity—

(A) in the case of an eligible entity that is a State, directly to the appropriate local government as a replacement grant in an amount determined by the Secretary; or

(B) in the case of an eligible entity that is a Tribal government, to another Tribal government or Tribal governments as a replacement grant in an amount determined by the Secretary.

§ 12745. Consultation with State, local, and Tribal representatives

In carrying out this subchapter, the Secretary shall consult with State, local, and Tribal representatives with professional experience relating to cybersecurity, including representatives of associations representing State, local, and Tribal governments, to inform—

(1) guidance for applicants for grants under this subchapter, including guidance for Cybersecurity Plans;

(2) the study of risk-based formulas required under section 12747(d) of this title;

(3) the development of guidelines required under section 12743(b)(2) of this title; and

(4) any modifications described in section 12747(b)(4) of this title.

§ 12746. Notification to Congress

Not later than 3 business days before the date on which the Department announces the award of a grant to an eligible entity under this subchapter, including an announcement to the eligible entity, the Secretary shall provide to the appropriate congressional committees notice of the announcement.

§ 12747. Reports, study, and review

(a) ANNUAL REPORTS BY GRANT RECIPIENTS.—

(1) IN GENERAL.—Not later than 1 year after the date on which an eligible entity receives a grant under this subchapter for the purpose of implementing the Cybersecurity Plan of the eligible entity, including an eligible entity that comprises a multi-entity group that receives a

grant for that purpose, and annually thereafter until 1 year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report that, using the metrics described in the Cybersecurity Plan of the eligible entity, describes the progress of the eligible entity in—

(A) implementing the Cybersecurity Plan of the eligible entity; and

(B) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.

(2) ABSENCE OF PLAN.—Not later than 1 year after the date on which an eligible entity that does not have a Cybersecurity Plan receives funds under this subchapter, and annually thereafter until 1 year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds to—

(A) develop or revise a Cybersecurity Plan; or

(B) assist with the activities described in section 12734(4).

(b) ANNUAL REPORTS TO CONGRESS.—Not less frequently than annually, the Secretary, acting through the Director, shall submit to Congress a report on—

(1) the use of grants awarded under this subchapter;

(2) the proportion of grants used to support cybersecurity in rural areas;

(3) the effectiveness of the State and Local Cybersecurity Grant Program;

(4) any necessary modifications to the State and Local Cybersecurity Grant Program; and

(5) any progress made toward—

(A) developing, implementing, or revising Cybersecurity Plans; and

(B) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, State, local, or Tribal governments as a result of the award of grants under this subchapter.

(c) PUBLIC AVAILABILITY.—

(1) IN GENERAL.—The Secretary, acting through the Director, shall make each report submitted under subsection (b) publicly available, in-

cluding by making each report available on the website of the Cybersecurity and Infrastructure Security Agency.

(2) REDACTIONS.—In making each report publicly available under paragraph (1), the Director may make redactions that the Director, in consultation with each eligible entity, determines necessary to protect classified or other information exempt from disclosure under section 552 of title 5 (known as the Freedom of Information Act).

(d) STUDY OF RISK-BASED FORMULAS.—

(1) IN GENERAL.—Not later than September 30, 2024, the Secretary, acting through the Director, shall submit to the appropriate congressional committees a study and legislative recommendations on the potential use of a risk-based formula for apportioning funds under this subchapter, including—

(A) potential components that could be included in a risk-based formula, including the potential impact of those components on support for rural areas under this subchapter;

(B) potential sources of data and information necessary for the implementation of a risk-based formula;

(C) any obstacles to implementing a risk-based formula, including obstacles that require a legislative solution;

(D) if a risk-based formula were to be implemented for fiscal year 2026, a recommended risk-based formula for the State and Local Cybersecurity Grant Program; and

(E) any other information that the Secretary, acting through the Director, determines necessary to help Congress understand the progress towards, and obstacles to, implementing a risk-based formula.

(2) INAPPLICABILITY OF PAPERWORK REDUCTION ACT.—The requirements of chapter 35 of title 44 (known as the Paperwork Reduction Act) shall not apply to any action taken to carry out this subsection.

(e) TRIBAL CYBERSECURITY NEEDS REPORT.—Not later than 2 years after November 15, 2021, the Secretary, acting through the Director, shall submit to Congress a report that—

(1) describes the cybersecurity needs of Tribal governments, which shall be determined in consultation with the Secretary of the Interior and Tribal governments; and

(2) includes recommendations for addressing the cybersecurity needs of Tribal governments, including necessary modifications to the State and Local Cybersecurity Grant Program to better serve Tribal governments.

(f) COMPTROLLER GENERAL REVIEW.—Not later than 3 years after November 15, 2021, the Comptroller General shall conduct a review of the State and Local Cybersecurity Grant program, including—

(1) the grant selection process of the Secretary; and

(2) a sample of grants awarded under this subchapter.

§ 12748. Authorization of appropriations

(a) IN GENERAL.—There is authorized to be appropriated for activities under this subchapter—

(1) for fiscal year 2023, $400,000,000;

(2) for fiscal year 2024, $300,000,000; and

(3) for fiscal year 2025, $100,000,000.

(b) TRANSFERS AUTHORIZED.—

(1) IN GENERAL.—During a fiscal year, the Secretary or the head of any component of the Department that administers the State and Local Cybersecurity Grant Program may transfer not more than 5 percent of the amounts appropriated pursuant to subsection (a) or other amounts appropriated to carry out the State and Local Cybersecurity Grant Program for that fiscal year to an account of the Department for salaries, expenses, and other administrative costs incurred for the management, administration, or evaluation of this subchapter.

(2) ADDITIONAL AMOUNTS.—Funds transferred under paragraph (1) shall be in addition to funds appropriated to the Department or the components described in paragraph (1) for salaries, expenses, and other administrative costs.

§ 12749. Termination

(a) IN GENERAL.—Subject to subsection (b), the requirements of this section shall terminate on September 30, 2025.

(b) EXCEPTION.—The reporting requirements under section 12747 of this title shall terminate on the date that is 1 year after the date on which the final funds from a grant under this subchapter are expended or returned.

Chapter 129—Anti-Trafficking Training for Department Personnel

Sec.
12901. Definition of human trafficking.
12902. Training to identify human trafficking.
12903. Reports.
12904. Assistance to non-Federal entities.
12905. Victim protection training.

§ 12901. Definition of human trafficking

In this chapter, the term ''human trafficking'' means an act or practice described in paragraph (11) or (12) of section 103 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7102(11), (12)).

§ 12902. Training to identify human trafficking

(a) IN GENERAL.—The Secretary shall implement a program to—

(1) train and periodically retrain relevant Transportation Security Administration, U. S. Customs and Border Protection, and other Department personnel that the Secretary considers appropriate, with respect to how to effectively deter, detect, and disrupt human trafficking, and, where appropriate, interdict a suspected perpetrator of human trafficking, during the course of their primary roles and responsibilities; and

(2) ensure that the personnel referred to in paragraph (1) regularly receive current information on matters relating to the detection of human trafficking, including information that becomes available outside of the Department's initial or periodic retraining schedule, to the extent relevant to their official duties and consistent with applicable information and privacy laws.

(b) TRAINING.—The training referred to in subsection (a) may be conducted through in-class or virtual learning capabilities, and shall include—

(1) methods for identifying suspected victims of human trafficking and, where appropriate, perpetrators of human trafficking;

(2) for appropriate personnel, methods to approach a suspected victim of human trafficking, where appropriate, in a manner that is sensitive to the suspected victim and is not likely to alert a suspected perpetrator of human trafficking;

(3) training that is most appropriate for the particular location or environment in which the personnel receiving the training perform their official duties;

(4) other topics determined by the Secretary to be appropriate; and

(5) a post-training evaluation for personnel receiving the training.

(c) TRAINING CURRICULUM REVIEW.—The Secretary shall annually reassess the training program established under subsection (a) to ensure it is consistent with current techniques, patterns, and trends associated with human trafficking.

§ 12903. Reports

(a) EFFECTIVENESS OF PROGRAM.—Not later than 1 year after May 29, 2015, and annually thereafter, the Secretary shall report to Congress with respect to the overall effectiveness of the program required by this chapter, the number of cases reported by Department personnel in which human trafficking was suspected, and, of those cases, the number of cases that were confirmed cases of human trafficking.

(b) HUMAN TRAFFICKING INVESTIGATIONS.—Not later than 1 year after December 21, 2018, and annually thereafter, the Executive Associate Direc-

tor of Homeland Security Investigations shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate and the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives a report on human trafficking investigations undertaken by Homeland Security Investigations that includes—

(1) the number of confirmed human trafficking investigations by category, including labor trafficking, sex trafficking, and transnational and domestic human trafficking;

(2) the number of victims by category, including—

(A) whether the victim is a victim of sex trafficking or a victim of labor trafficking; and

(B) whether the victim is a minor or an adult; and

(3) an analysis of the date described in paragraphs (1) and (2) and other data available to Homeland Security Investigations that indicates any general human trafficking or investigatory trends.

§ 12904. Assistance to non-Federal entities

The Secretary may provide training curricula to any State, local, or tribal government, or private organization, to assist the government or organization in establishing a program of training to identify human trafficking, on request from the government or organization.

§ 12905. Victim protection training

(a) DIRECTIVE TO DEPARTMENT LAW ENFORCEMENT OFFICIALS AND TASK FORCES.—

(1) IN GENERAL.—Not later than 180 days after December 21, 2018, the Secretary shall issue a directive to—

(A) all Federal law enforcement officers and relevant personnel employed by the Department who may be involved in the investigation of human trafficking offenses; and

(B) members of all task forces led by the Department that participate in the investigation of human trafficking offenses.

(2) REQUIRED INSTRUCTIONS.—The directive required to be issued under paragraph (1) shall include instructions on—

(A) the investigation of individuals who patronize or solicit human trafficking victims as being engaged in severe trafficking in individuals and how individuals who patronize or solicit human trafficking victims should be investigated for their role in severe trafficking in individuals; and

(B) how victims of sex or labor trafficking often engage in criminal acts as a direct result of severe trafficking in individuals and how the individuals are victims of a crime, and affirmative

measures that should be taken to avoid arresting, charging, or prosecuting those individuals who are victims of a crime for an offense that is the direct result of their victimization.

(b) VICTIM SCREENING PROTOCOL.—

(1) IN GENERAL.—Not later than 180 days after December 21, 2018, the Secretary shall issue a screening protocol for use during all anti-trafficking law enforcement operations in which the Department is involved.

(2) REQUIREMENTS.—The directive required to be issued under paragraph (1) shall—

(A) require the individual screening of all adults and children who are suspected of engaging in commercial sex acts, child labor that is a violation of law, or work in violation of labor standards to determine whether each individual screened is a victim of human trafficking;

(B) require affirmative measures to avoid arresting, charging, or prosecuting human trafficking victims for an offense that is the direct result of their victimization;

(C) be developed in consultation with relevant inter-agency partners and nongovernmental organizations that specialize in the prevention of human trafficking or in the identification and support of victims of human trafficking and survivors of human trafficking; and

(D) include—

(i) procedures and practices to ensure that the screening process minimizes trauma or revictimization of the individual being screened; and

(ii) guidelines on assisting victims of human trafficking in identifying and receiving restorative services.

(c) MANDATORY TRAINING.—The training described in sections 12902 and 12904 of this title shall include training necessary to implement—

(1) the directive required under subsection (a); and

(2) the protocol required under subsection (b).

Subtitle II—National Emergency Management

Chapter 201—General

§ 20101. Definitions

In this subtitle:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Agency.

(2) AGENCY.—The term ''Agency'' means the Federal Emergency Management Agency.

(3) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

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

(B) those committees of the House of Representatives that the Speaker of the House of Representatives determines appropriate.

(4) CATASTROPHIC INCIDENT.—The term ''catastrophic incident'' means any natural disaster, act of terrorism, or other man-made disaster that results in extraordinary levels of casualties or damage or disruption severely affecting the population (including mass evacuations), infrastructure, environment, economy, national morale, or government functions in an area.

(5) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(6) EMERGENCY; MAJOR DISASTER.—The terms ''emergency'' and ''major disaster'' have the meanings given the terms in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(7) EMERGENCY MANAGEMENT.—The term ''emergency management'' means the governmental function that coordinates and integrates all activities necessary to build, sustain, and improve the capability to prepare for, protect against, respond to, recover from, or mitigate against threatened or actual natural disasters, acts of terrorism, or other man-made disasters.

(8) EMERGENCY RESPONSE PROVIDERS.—The term ''emergency response providers'' has the meaning given the term in section 10101 of this title.

(9) FEDERAL COORDINATING OFFICER.—The term ''Federal coordinating officer'' means a Federal coordinating officer as described in section 302 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5143).

(10) INDIVIDUAL WITH A DISABILITY.—The term ''individual with a disability'' has the meaning given the term in section 3 of the Americans with Disabilities Act of 1990 (42 U.S.C. 12102).

(11) LOCAL GOVERNMENT.—The term ''local government'' has the meaning given the term in section 10101 of this title.

(12) NATIONAL INCIDENT MANAGEMENT SYSTEM.—The term ''National Incident Management System'' means a system to enable effective, efficient, and collaborative incident management.

(13) NATIONAL RESPONSE PLAN.—The term ''National Response Plan'' means the National Response Plan or any successor plan prepared under section 11303(a)(6) of this title.

(14) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(15) STATE.—The term ''State'' has the meaning given the term in section 10101 of this title.

(16) SURGE CAPACITY.—The term ''surge capacity'' means the ability to rapidly and substantially increase the provision of search and rescue capabilities, food, water, medicine, shelter and housing, medical care, evacuation capacity, staffing (including disaster assistance employees), and other resources necessary to save lives and protect property during a catastrophic incident.

(17) TRIBAL GOVERNMENT.—The term ''tribal government'' means the government of an Indian tribe or authorized tribal organization, or, in Alaska, a Native village or Alaska Regional Native Corporation.

Chapter 203—Emergency Management Capabilities

Sec.

§ 20301. Surge Capacity Force

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Administrator shall prepare and submit to the appropriate committees of Congress a plan to establish and implement a Surge Capacity Force for deployment of individuals to respond to natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents.

(2) AUTHORITY.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the plan shall provide for individuals in the Surge Capacity Force to be trained and deployed under the authorities set forth in the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

(B) EXCEPTION.—If the Administrator determines that the existing authorities are inadequate for the training and deployment of individuals in the Surge Capacity Force, the Administrator shall report to Congress as to the additional statutory authorities that the Administrator determines necessary.

(b) EMPLOYEES DESIGNATED TO SERVE.—The plan shall include procedures under which the Secretary shall designate employees of the Department who are not employees of the Agency and shall, in conjunction with the heads of other Executive agencies, designate employees of those other Executive agencies, as appropriate, to serve on the Surge Capacity Force.

(c) CAPABILITIES.—The plan shall ensure that the Surge Capacity Force—

(1) includes a sufficient number of individuals credentialed under section 11310 of this title that are capable of deploying rapidly and efficiently after activation to prepare for, respond to, and recover from natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents; and

(2) includes a sufficient number of full-time, highly trained individuals credentialed under section 11310 of this title to lead and manage the Surge Capacity Force.

(d) TRAINING.—The plan shall ensure that the Administrator provides appropriate and continuous training to members of the Surge Capacity Force to ensure the personnel are adequately trained on the Agency's programs and policies for natural disasters, acts of terrorism, and other man-made disasters.

(e) NO IMPACT ON AGENCY PERSONNEL CEILING.—Surge Capacity Force members shall not be counted against any personnel ceiling applicable to the Agency.

(f) EXPENSES.—The Administrator may provide members of the Surge Capacity Force with travel expenses, including per diem in lieu of subsistence, at rates authorized for employees of agencies under subchapter I of chapter 57 of title 5, for the purpose of participating in any training that relates to service as a member of the Surge Capacity Force.

(g) IMMEDIATE IMPLEMENTATION OF SURGE CAPACITY FORCE INVOLVING FEDERAL EMPLOYEES.—The Administrator shall develop and implement—

(1) the procedures under subsection (b); and

(2) other elements of the plan needed to establish the portion of the Surge Capacity Force consisting of individuals designated under those procedures.

§ 20302. Evacuation preparedness technical assistance

(a) IN GENERAL.—The Administrator, in coordination with the heads of other appropriate Federal agencies, shall provide evacuation preparedness technical assistance to State, local, and tribal governments, including the preparation of hurricane evacuation studies and technical assistance in developing evacuation plans, assessing storm surge estimates, evacuation zones, evacuation clearance times, transportation capacity, and shelter capacity.

(b) GUIDANCE ON EVACUATION ROUTES.—

(1) DEFINITION OF STATE.—In this subsection, the term ''State'' has the meaning given the term in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(2) ADMINISTRATOR.—The Administrator, in coordination with the Administrator of the Federal Highway Administration, shall develop and issue guidance for State, local, and Indian tribal governments regarding the identification of evacuation routes. In developing the guidance, the Administrator shall consider—

(A) whether evacuation routes have resisted impacts and recovered quickly from disasters, regardless of cause;

(B) the need to evacuate special needs populations, including—

(i) individuals with a physical or mental disability;

(ii) individuals in schools, daycare centers, mobile home parks, prisons, nursing homes and other long-term care facilities, and detention centers;

(iii) individuals with limited English proficiency;

(iv) the elderly; and

(v) individuals who are tourists, seasonal workers, or homeless;

(C) the sharing of information and other public communications with evacuees during evacuations;

(D) the sheltering of evacuees, including the care, protection, and sheltering of animals;

(E) the return of evacuees to their homes; and

(F) other items the Administrator considers appropriate.

(3) ADMINISTRATOR OF FEDERAL HIGHWAY ADMINISTRATION.—The Administrator of the Federal Highway Administration, in coordination with the Administrator, shall revise existing guidance or issue new guidance as appropriate for State, local, and Indian tribal governments regarding the design, construction, maintenance, and repair of evacuation routes. In revising or issuing the guidance, the Administrator of the Federal Highway Administration shall consider—

(A) methods that assist evacuation routes to—

(i) withstand likely risks to viability, including flammability and hydrostatic forces;

(ii) improve durability, strength (including the ability to withstand tensile stresses and compressive stresses), and sustainability; and

(iii) provide for long-term cost savings;

(B) the ability of evacuation routes to effectively manage contraflow operations;

(C) for evacuation routes on public lands, the viewpoints of the applicable Federal land management agency regarding emergency operations, sustainability, and resource protection; and

(D) other items the Administrator of the Federal Highway Administration considers appropriate.

(4) STUDY.—The Administrator, in coordination with the Administrator of the Federal Highway Administration and State, local, and Indian tribal governments, may—

(A) conduct a study of the adequacy of available evacuation routes to accommodate the flow of evacuees; and

(B) submit recommendations on how to help with anticipated evacuation route flow, based on the study, to—

(i) the Federal Highway Administration;

(ii) the Agency;

(iii) State, local, and Indian tribal governments; and

(iv) Congress.

§ 20303. Urban Search and Rescue Response System

There is in the Agency the Urban Search and Rescue Response System.

§ 20304. Metropolitan Medical Response System Program

(a) IN GENERAL.—There is in the Agency the Metropolitan Medical Response System Program.

(b) PURPOSES.—The Metropolitan Medical Response System Program shall include each purpose of the Program as it existed on June 1, 2006.

§ 20305. Logistics

The Administrator shall develop an efficient, transparent, and flexible logistics system for procurement and delivery of goods and services necessary for an effective and timely response to natural disasters, acts of terrorism, and other man-made disasters and for real-time visibility of items at each point throughout the logistics system.

§ 20306. Pre-positioned equipment program

(a) IN GENERAL.—The Administrator shall establish a pre-positioned equipment program to pre-position standardized emergency equipment in at

least 11 locations to sustain and replenish critical assets used by State, local, and tribal governments in response to (or rendered inoperable by the effects of) natural disasters, acts of terrorism, and other man-made disasters.

(b) NOTICE.—Not later than 60 days before the date of closure, the Administrator shall notify State, local, and tribal officials in an area in which a location for the pre-positioned equipment program will be closed.

§ 20307. Basic life supporting first aid and education

The Administrator shall enter into agreements with organizations to provide funds to emergency response providers to provide education and training in life supporting first aid to children.

§ 20308. Improvements to information technology systems

The Administrator, in coordination with the Chief Information Officer of the Department, shall take appropriate measures to update and improve the information technology systems of the Agency, including measures to—

(1) ensure that the multiple information technology systems of the Agency (including the National Emergency Management Information System, the Logistics Information Management System III, and the Automated Deployment Database) are, to the extent practicable, fully compatible and can share and access information, as appropriate, from each other;

(2) ensure technology enhancements reach the headquarters and regional offices of the Agency in a timely fashion, to allow seamless integration;

(3) develop and maintain a testing environment that ensures that all system components are properly and thoroughly tested before their release;

(4) ensure that the information technology systems of the Agency have the capacity to track disaster response personnel, mission assignment task orders, commodities, and supplies used in response to a natural disaster, act of terrorism, or other man-made disaster;

(5) make appropriate improvements to the National Emergency Management Information System to address shortcomings in the system on October 4, 2006; and

(6) provide training, manuals, and guidance on information technology systems to personnel, including disaster response personnel, to help ensure employees can properly use information technology systems.

§ 20309. Disclosure of certain information to law enforcement agencies

If circumstances require an evacuation, sheltering, or mass relocation, the Administrator may disclose information in any individual assistance database of the Agency under section 552a(b) of title 5 to any law enforcement agency of the Federal Government or a State, local, or tribal government in order to identify illegal conduct or address public safety or security issues, including compliance with sex offender notification laws.

Chapter 205—Comprehensive Preparedness System

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) CREDENTIALED; CREDENTIALING.—The terms ''credentialed'' and ''credentialing'' have the meanings given the terms in section 11301 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.

(5) NATIONAL PREPAREDNESS GOAL.—The term ''national preparedness goal'' means the national preparedness goal established under section 20503 of this title.

(6) NATIONAL PREPAREDNESS SYSTEM.—The term ''national preparedness system'' means the national preparedness system established under section 20504 of this title.

(7) NATIONAL TRAINING PROGRAM.—The term ''national training program'' means the national training program established under section 20508(a) of this title.

(8) OPERATIONAL READINESS.—The term ''operational readiness'' means the capability of an organization, an asset, a system, or equipment to perform the missions or functions for which it is organized or designed.

(9) PERFORMANCE MEASURE.—The term ''performance measure'' means a quantitative or qualitative characteristic used to gauge the results of an outcome compared to its intended purpose.

(10) PERFORMANCE METRIC.—The term ''performance metric'' means a particular value or characteristic used to measure the outcome that is generally expressed in terms of a baseline and a target.

(11) PREVENTION.—The term ''prevention'' means any activity undertaken to avoid, prevent, or stop a threatened or actual act of terrorism.

(12) RESOURCES.—The term ''resources'' has the meaning given the term in section 11301 of this title.

(13) TYPE.—The term ''type'' means a classification of resources that refers to the capability of a resource.

(14) TYPED; TYPING.—The terms ''typed'' and ''typing'' have the meanings given the terms in section 11301 of this title.

§ 20502. Development of national preparedness goal and national preparedness system

To prepare the Nation for all hazards, including natural disasters, acts of terrorism, and other man-made disasters, the President, consistent with the declaration of policy under section 601 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5195) and chapter 113 of this title, shall develop a national preparedness goal and a national preparedness system.

§ 20503. National preparedness goal

(a) ESTABLISHMENT.—The President, acting through the Administrator, shall complete, revise, and update, as necessary, a national preparedness goal that defines the target level of preparedness to ensure the Nation's ability to prevent, respond to, recover from, and mitigate against natural disasters, acts of terrorism, and other man-made disasters.

(b) CONSISTENT WITH NATIONAL INCIDENT MANAGEMENT SYSTEM AND NATIONAL RESPONSE PLAN.—The national preparedness goal, to the greatest extent practicable, shall be consistent with the National Incident Management System and the National Response Plan.

§ 20504. National preparedness system

(a) ESTABLISHMENT.—The President, acting through the Administrator, shall develop a national preparedness system to enable the Nation to meet the national preparedness goal.

(b) COMPONENTS.—The national preparedness system shall include the following components:

(1) Target capabilities and preparedness priorities.

(2) Equipment and training standards.

(3) Training and exercises.

(4) A comprehensive assessment system.

(5) A remedial action management program.

(6) A Federal response capability inventory.

(7) Reporting requirements.

(8) Federal preparedness.

(c) NATIONAL PLANNING SCENARIOS.—The national preparedness system may include national planning scenarios.

§ 20505. National planning scenarios

(a) IN GENERAL.—The Administrator, in coordination with the heads of appropriate Federal agencies and the National Advisory Council, may develop planning scenarios to reflect the relative risk requirements presented by all hazards, including natural disasters, acts of terrorism, and other man-made disasters, to provide the foundation for the flexible and adaptive

development of target capabilities and the identification of target capability levels to meet the national preparedness goal.

(b) DEVELOPMENT.—In developing, revising, and replacing national planning scenarios, the Administrator shall ensure that the scenarios—

(1) reflect the relative risk of all hazards and illustrate the potential scope, magnitude, and complexity of a broad range of representative hazards; and

(2) provide the minimum number of representative scenarios necessary to identify and define the tasks and target capabilities required to respond to all hazards.

§ 20506. Target capabilities and preparedness priorities

(a) ESTABLISHMENT OF GUIDELINES ON TARGET CAPABILITIES.—The Administrator, in coordination with the heads of appropriate Federal agencies, the National Council on Disability, and the National Advisory Council, shall complete, revise, and update, as necessary, guidelines to define risk-based target capabilities for Federal, State, local, and tribal government preparedness that will enable the Nation to prevent, respond to, recover from, and mitigate against all hazards, including natural disasters, acts of terrorism, and other man-made disasters.

(b) DISTRIBUTION OF GUIDELINES.—The Administrator shall ensure that the guidelines are provided promptly to the appropriate committees of Congress and the States.

(c) OBJECTIVES.—The Administrator shall ensure that the guidelines are specific, flexible, and measurable.

(d) TERRORISM RISK ASSESSMENT.—With respect to analyzing and assessing the risk of acts of terrorism, the Administrator shall consider—

(1) the variables of threat, vulnerability, and consequences related to population (including transient commuting and tourist populations), areas of high population density, critical infrastructure, coastline, and international borders; and

(2) the most current risk assessment available from the Chief Intelligence Officer of the Department of the threats of terrorism against the United States.

(e) PREPAREDNESS PRIORITIES.—In establishing the guidelines under subsection (a), the Administrator shall establish preparedness priorities that appropriately balance the risk of all hazards, including natural disasters, acts of terrorism, and other man-made disasters, with the resources required to prevent, respond to, recover from, and mitigate against the hazards.

(f) MUTUAL AID AGREEMENTS.—The Administrator may provide support for the development of mutual aid agreements in States.

§ 20507. Equipment and training standards

(a) EQUIPMENT STANDARDS.—

(1) IN GENERAL.—The Administrator, in coordination with the heads of appropriate Federal agencies and the National Advisory Council, shall support the development, promulgation, and updating, as necessary, of national voluntary consensus standards for the performance, use, and validation of equipment used by Federal, State, local, and tribal governments and nongovernmental emergency response providers.

(2) REQUIREMENTS.—The national voluntary consensus standards shall—

(A) be designed to achieve equipment and other capabilities consistent with the national preparedness goal, including the safety and health of emergency response providers;

(B) to the maximum extent practicable, be consistent with existing national voluntary consensus standards;

(C) take into account, as appropriate, threats that may not have been contemplated when the existing standards were developed; and

(D) focus on maximizing operability, interoperability, interchangeability, durability, flexibility, efficiency, efficacy, portability, sustainability, and safety.

(b) TRAINING STANDARDS.—The Administrator shall—

(1) support the development, promulgation, and regular updating, as necessary, of national voluntary consensus standards for training; and

(2) ensure that the training provided under the national training program is consistent with the standards.

(c) CONSULTATION WITH STANDARDS ORGANIZATIONS.—In carrying out this section, the Administrator shall consult with representatives of relevant public- and private-sector national voluntary consensus standards development organizations.

§ 20508. Training and exercises

(a) NATIONAL TRAINING PROGRAM.—

(1) IN GENERAL.—The Administrator, in coordination with the heads of appropriate Federal agencies, the National Council on Disability, and the National Advisory Council, shall carry out a national training program to implement the national preparedness goal, National Incident Management System, National Response Plan, and other related plans and strategies.

(2) TRAINING PARTNERS.—In developing and implementing the national training program, the Administrator shall—

(A) work with government training facilities, academic institutions, private organizations, and other entities that provide specialized, state-of-the-art training for emergency managers or emergency response providers; and

(B) utilize, as appropriate, training courses provided by community colleges, State and local public safety academies, State and private universities, and other facilities.

(b) NATIONAL EXERCISE PROGRAM.—

(1) IN GENERAL.—The Administrator, in coordination with the heads of appropriate Federal agencies, the National Council on Disability, and the National Advisory Council, shall carry out a national exercise program to test and evaluate the national preparedness goal, National Incident Management System, National Response Plan, and other related plans and strategies.

(2) REQUIREMENTS.—The national exercise program—

(A) shall be—

(i) as realistic as practicable, based on current risk assessments, including credible and emerging threats, vulnerabilities, and consequences, and designed to stress the national preparedness system;

(ii) designed, as practicable, to simulate the partial or complete incapacitation of a State, local, or tribal government;

(iii) carried out, as appropriate, with a minimum degree of notice to involved parties regarding the timing and details of the exercises, consistent with safety considerations;

(iv) designed to provide for the systematic evaluation of readiness and enhance operational understanding of the incident command system and relevant mutual aid agreements;

(v) designed to address the unique requirements of populations with special needs, including the elderly; and

(vi) designed to promptly develop after-action reports and plans for quickly incorporating lessons learned into future operations; and

(B) shall include a selection of model exercises that State, local, and tribal governments can readily adapt for use and provide assistance to State, local, and tribal governments with the design, implementation, and evaluation of exercises (whether a model exercise program or an exercise designed locally) that—

(i) conform to the requirements under subparagraph (A);

(ii) are consistent with any applicable State, local, or tribal strategy or plan; and

(iii) provide for systematic evaluation of readiness.

(3) NATIONAL LEVEL EXERCISES.—Periodically but not less than biennially, the Administrator shall perform national exercises to test and evaluate the following:

(A) The capability of Federal, State, local, and tribal governments to detect, disrupt, and prevent threatened or actual catastrophic acts of terrorism, especially those involving weapons of mass destruction.

(B) The readiness of Federal, State, local, and tribal governments to respond and recover in a coordinated and unified manner to catastrophic incidents.

(c) ANNUAL GUIDANCE AND TRAINING.—The Administrator shall provide guidance and training on an annual basis to State, local, and Indian tribal governments, first responders, and utility companies on—

(1) the need to prioritize assistance to hospitals, nursing homes, and other long-term care facilities to ensure that the health care facilities remain functioning or return to functioning as soon as practicable during power outages caused by natural hazards, including severe weather events;

(2) how hospitals, nursing homes, and other long-term care facilities should adequately prepare for power outages during a major disaster or emergency, as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122); and

(3) how State, local, and Indian tribal governments, first responders, utility companies, hospitals, nursing homes, and other long-term care facilities should develop a strategy to coordinate emergency response plans, including the activation of emergency response plans, in anticipation of a major disaster, including severe weather events.

§ 20509. Comprehensive assessment system

(a) ESTABLISHMENT.—The Administrator, in coordination with the National Council on Disability and the National Advisory Council, shall establish a comprehensive system to assess, on an ongoing basis, the Nation's prevention capabilities and overall preparedness, including operational readiness.

(b) PERFORMANCE METRICS AND MEASURES.—The Administrator shall ensure that each component of the national preparedness system, National Incident Management System, National Response Plan, and other related plans and strategies, and the reports required under section 20512 of this title are developed, revised, and updated with clear and quantifiable performance metrics, measures, and outcomes.

(c) CONTENTS.—The assessment system established under subsection (a) shall assess—

(1) compliance with the national preparedness system, National Incident Management System, National Response Plan, and other related plans and strategies;

(2) capability levels at the time of assessment against target capability levels defined pursuant to the guidelines established under section 20506(a) of this title;

(3) resources needed to meet the desired target capability levels defined pursuant to the guidelines established under section 20506(a) of this title; and

(4) performance of training, exercises, and operations.

§ 20510. Remedial action management program

The Administrator, in coordination with the National Council on Disability and the National Advisory Council, shall establish a remedial action management program to—

(1) analyze training, exercises, and real-world events to identify and disseminate lessons learned and best practices;

(2) generate and disseminate, as appropriate, after-action reports to participants in exercises and real-world events; and

(3) conduct remedial action tracking and long-term trend analysis.

§ 20511. Federal response capability inventory

(a) IN GENERAL.—Under section 611(h)(1)(C) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196(h)(1)(C)), the Administrator shall accelerate the completion of the inventory of Federal response capabilities.

(b) CONTENTS.—For each Federal agency with responsibilities under the National Response Plan, the inventory shall include—

(1) for each capability—

(A) the performance parameters of the capability;

(B) the time frame within which the capability can be brought to bear on an incident; and

(C) the readiness of the capability to respond to all hazards, including natural disasters, acts of terrorism, and other man-made disasters;

(2) a list of personnel credentialed under section 11310 of this title;

(3) a list of resources typed under section 11310 of this title; and

(4) emergency communications assets maintained by the Federal Government and, if appropriate, State, local, and tribal governments and the private sector.

(c) DEPARTMENT OF DEFENSE.—The Administrator, in coordination with the Secretary of Defense, shall develop a list of organizations and functions within the Department of Defense that may be used, pursuant to the authority provided under the National Response Plan and sections 402, 403, and 502 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5170a, 5170b, 5192), to provide support to civil authorities during natural disasters, acts of terrorism, and other man-made disasters.

(d) DATABASE.—The Administrator shall establish an inventory database to allow—

(1) real-time exchange of information regarding—

(A) capabilities;

(B) readiness;

(C) the compatibility of equipment;

(D) credentialed personnel; and

(E) typed resources;

(2) easy identification and rapid deployment of capabilities, credentialed personnel, and typed resources during an incident; and

(3) the sharing of the inventory described in subsection (a) with other Federal agencies, as appropriate.

§ 20512. Reporting requirements

(a) FEDERAL PREPAREDNESS REPORT.—

(1) IN GENERAL.—The Administrator, in coordination with the heads of appropriate Federal agencies, shall submit annually to the appropriate committees of Congress a report on the Nation's level of preparedness for all hazards, including natural disasters, acts of terrorism, and other man-made disasters.

(2) CONTENTS.—Each report shall include—

(A) an assessment of how Federal assistance supports the national preparedness system;

(B) the results of the comprehensive assessment carried out under section 20509 of this title;

(C) a review of the inventory described in section 20511 of this title, including the number and type of credentialed personnel in each category of personnel trained and ready to respond to a natural disaster, act of terrorism, or other man-made disaster;

(D) an assessment of resources needed to meet preparedness priorities established under section 20506(e) of this title, including—

(i) an estimate of the amount of Federal, State, local, and tribal expenditures required to attain the preparedness priorities; and

(ii) the extent to which the use of Federal assistance during the preceding fiscal year achieved the preparedness priorities;

(E) an evaluation of the extent to which grants administered by the Department, including grants under chapter 127 of this title—

(i) have contributed to the progress of State, local, and tribal governments in achieving target capabilities; and

(ii) have led to the reduction of risk from natural disasters, acts of terrorism, or other man-made disasters nationally and in State, local, and tribal jurisdictions; and

(F) a discussion of whether the list of credentialed personnel of the Agency described in section 20511(b)(2) of this title—

(i) complies with the strategic human capital plan developed under section 10102 of title 5; and

(ii) is sufficient to respond to a natural disaster, act of terrorism, or other man-made disaster, including a catastrophic incident.

(b) CATASTROPHIC RESOURCE ESTIMATE.—

(1) IN GENERAL.—The Administrator shall develop and submit annually to the appropriate committees of Congress an estimate of the resources of the Agency and other Federal agencies needed for, and devoted specifically to, developing the capabilities of Federal, State, local, and tribal governments necessary to respond to a catastrophic incident.

(2) CONTENTS.—Each estimate shall include the resources necessary for and devoted to—

(A) planning;

(B) training and exercises;

(C) Regional Office enhancements;

(D) staffing, including for surge capacity during a catastrophic incident;

(E) additional logistics capabilities;

(F) other responsibilities under the catastrophic incident annex and the catastrophic incident supplement of the National Response Plan;

(G) State, local, and tribal government catastrophic incident preparedness; and

(H) increases in the fixed costs or expenses of the Agency, including rent or property acquisition costs or expenses, taxes, con-

tributions to the working capital fund of the Department, and security costs for the year after the year in which the estimate is submitted.

(c) STATE PREPAREDNESS REPORT.—

(1) IN GENERAL.—A State receiving Federal preparedness assistance administered by the Department annually shall submit a report to the Administrator on the State's level of preparedness.

(2) CONTENTS.—Each report shall include—

(A) an assessment of State compliance with the national preparedness system, National Incident Management System, National Response Plan, and other related plans and strategies;

(B) an assessment of current capability levels and a description of target capability levels; and

(C) a discussion of the extent to which target capabilities identified in the applicable State homeland security plan and other applicable plans remain unmet and an assessment of resources needed to meet the preparedness priorities established under section 20506(e) of this title, including—

(i) an estimate of the amount of expenditures required to attain the preparedness priorities; and

(ii) the extent to which the use of Federal assistance during the preceding fiscal year achieved the preparedness priorities.

§ 20513. Federal preparedness

(a) AGENCY RESPONSIBILITY.—In support of the national preparedness system, the President shall ensure that each Federal agency with responsibilities under the National Response Plan—

(1) has the operational capability to meet the national preparedness goal, including—

(A) the personnel to make and communicate decisions;

(B) organizational structures that are assigned, trained, and exercised for the missions of the agency;

(C) sufficient physical resources; and

(D) the command, control, and communication channels to make, monitor, and communicate decisions;

(2) complies with the National Incident Management System, including credentialing of personnel and typing of resources likely needed to respond to a natural disaster, act of terrorism, or other man-made disaster under section 11310 of this title;

(3) develops, trains, and exercises rosters of response personnel to be deployed when the agency is called on to support a Federal response;

(4) develops deliberate operational plans and the corresponding capabilities, including crisis planning, to respond effectively to natural disasters, acts of terrorism, and other man-made disasters in support of the National Response Plan to ensure a coordinated Federal response; and

(5) regularly updates, verifies the accuracy of, and provides to the Administrator the information in the inventory required under section 20511 of this title.

(b) OPERATIONAL PLANS.—An operations plan developed under subsection (a)(4) shall meet the following requirements:

(1) The operations plan shall be coordinated under a unified system with a common terminology, approach, and framework.

(2) The operations plan shall be developed, in coordination with State, local, and tribal government officials, to address both regional and national risks.

(3) The operations plan shall contain, as appropriate, the following elements:

(A) Concepts of operations.

(B) Critical tasks and responsibilities.

(C) Detailed resource and personnel requirements, together with sourcing requirements.

(D) Specific provisions for the rapid integration of the resources and personnel of the agency into the overall response.

(4) The operations plan shall address, as appropriate, the following matters:

(A) Support of State, local, and tribal governments in conducting mass evacuations, including—

(i) transportation and relocation;

(ii) short- and long-term sheltering and accommodation;

(iii) provisions for populations with special needs, keeping families together, and expeditious location of missing children; and

(iv) policies and provisions for pets.

(B) The preparedness and deployment of public health and medical resources, including resources to address the needs of evacuees and populations with special needs.

(C) The coordination of interagency search and rescue operations, including land, water, and airborne search and rescue operations.

(D) The roles and responsibilities of the Senior Federal Law Enforcement Official with respect to other law enforcement entities.

(E) The protection of critical infrastructure.

(F) The coordination of maritime salvage efforts among relevant agencies.

(G) The coordination of Department of Defense and National Guard support of civilian authorities.

(H) To the extent practicable, the utilization of Department of Defense, National Air and Space Administration, National Oceanic and Atmospheric Administration, and commercial aircraft and satellite remotely sensed imagery.

(I) The coordination and integration of support from the private sector and nongovernmental organizations.

(J) The safe disposal of debris, including hazardous materials, and, when practicable, the recycling of debris.

(K) The identification of the required surge capacity.

(L) Specific provisions for the recovery of affected geographic areas.

(c) MISSION ASSIGNMENTS.—To expedite the provision of assistance under the National Response Plan, the President shall ensure that the Administrator, in coordination with Federal agencies with responsibilities under the National Response Plan, develops pre-scripted mission assignments, including logistics, communications, mass care, health services, and public safety.

(d) CERTIFICATION.—The President shall certify to 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 of Representatives on an annual basis that each Federal agency with responsibilities under the National Response Plan complies with subsections (a) and (b).

(e) CONSTRUCTION.—Nothing in this section shall be construed to limit the authority of the Secretary of Defense with regard to—

(1) the command, control, training, planning, equipment, exercises, or employment of Department of Defense forces; or

(2) the allocation of Department of Defense resources.

§ 20514. Use of existing resources

In establishing the national preparedness goal and national preparedness system, the Administrator shall use existing preparedness documents, planning tools, and guidelines to the extent practicable and consistent with this subtitle.

Subchapter II—Additional Preparedness

§ 20521. Emergency Management Assistance Compact grants

(a) IN GENERAL.—The Administrator may make grants to administer the Emergency Management Assistance Compact consented to by the Joint Resolution entitled ''Joint Resolution granting the consent of Congress to the Emergency Management Assistance Compact'' (Public Law 104–321, 110 Stat. 3877).

(b) USES.—A grant under this section shall be used—

(1) to carry out recommendations identified in the Emergency Management Assistance Compact after-action reports for the 2004 and 2005 hurricane seasons;

(2) to administer compact operations on behalf of all member States and territories;

(3) to continue coordination with the Agency and appropriate Federal agencies;

(4) to continue coordination with State, local, and tribal government entities and their respective national organizations; and

(5) to assist State and local governments, emergency response providers, and organizations representing the providers with credentialing emergency response providers and the typing of emergency response resources.

(c) COORDINATION.—The Administrator shall consult with the Administrator of the Emergency Management Assistance Compact to ensure effective coordination of efforts in responding to requests for assistance.

(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $4,000,000 for fiscal year 2022, to remain available until expended.

§ 20522. Emergency Management Performance Grants Program

(a) DEFINITIONS.—In this section:

(1) PROGRAM.—The term ''program'' means the emergency management performance grants program described in subsection (b).

(2) STATE.—The term ''State'' has the meaning given that term in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(b) IN GENERAL.—The Administrator shall continue implementation of an emergency management performance grants program to make grants to States to assist State, local, and tribal governments in preparing for all hazards, as authorized by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

(c) FEDERAL SHARE.—Except as otherwise specifically provided by title VI of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5195 et seq.), the Federal share of the cost of an activity carried out using funds made available under the program shall not exceed 50 percent.

(d) APPORTIONMENT.—The Administrator shall apportion the amounts appropriated each fiscal year to carry out the program among the States as follows:

(1) The Administrator shall first apportion 0.25 percent of the amounts to each of American Samoa, the Northern Mariana Islands, Guam, and the Virgin Islands and 0.75 percent of the amounts to each of the remaining States.

(2) The Administrator shall apportion the remainder of the amounts in the ratio that the population of each State bears to the population of all States.

(e) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out the program $950,000,000 for fiscal year 2022.

§ 20523. Training for emergency response providers from Federal Government, foreign governments, or private entities

(a) IN GENERAL.—The Center for Domestic Preparedness may provide training to emergency response providers from the Federal Government, foreign governments, or private entities if the Center for Domestic Preparedness is reimbursed for the cost of the training. Any reimbursement under this subsection shall be credited to the account from which the expenditure being reimbursed was made and is available, without fiscal year limitation, for the purposes for which amounts in the account may be expended.

(b) TRAINING NOT TO INTERFERE WITH PRIMARY MISSION.—The head of the Center for Domestic Preparedness shall ensure that any training provided under subsection (a) does not interfere with the primary mission of the Center for Domestic Preparedness to train State and local emergency response providers.

(c) TRAINING FEDERAL EMERGENCY MANAGEMENT AGENCY EMPLOYEES.—Subject to subsection (b), subsection (a) does not prohibit the Center for Domestic Preparedness from providing training to employees of the Agency in existing chemical, biological, radiological, nuclear, explosives,

mass casualty, and medical surge courses pursuant to 5 U.S.C. 4103 without reimbursement for the cost of the training.

§ 20524. National exercise simulation center

The President shall establish a national exercise simulation center that—

(1) uses a mix of live, virtual, and constructive simulations to—

(A) prepare elected officials, emergency managers, emergency response providers, and emergency support providers at all levels of government to operate cohesively;

(B) provide a learning environment for the homeland security personnel of all Federal agencies;

(C) assist in the development of operational procedures and exercises, particularly those based on catastrophic incidents; and

(D) allow incident commanders to exercise decision-making in a simulated environment; and

(2) uses modeling and simulation for training, exercises, and command and control functions at the operational level.

§ 20525. Real property transactions

(a) APPLICATION.—This section applies only to real property in the States, the District of Columbia, and Puerto Rico. It does not apply to real property for river and harbor projects or flood control projects, or to leases of Government-owned real property for agricultural or grazing purposes.

(b) REPORTS TO ARMED SERVICES COMMITTEES BEFORE TRANSACTION MAY BE ENTERED INTO.—

(1) TRANSACTIONS THAT MAY NOT BE ENTERED INTO BEFORE EXPIRATION OF PERIOD AFTER REPORT IS SUBMITTED.—The Director of the Office of Civil and Defense Mobilization, or the designee of the Director, may not enter into any of the following listed transactions by or for the use of the Office until after the expiration of 30 days from the date on which a report of the facts concerning the proposed transaction is submitted to the Committees on Armed Services of the Senate and House of Representatives:

(A) An acquisition of fee title to any real property, if the estimated price is more than $50,000.

(B) A lease of real property to the United States, if the estimated annual rental is more than $50,000.

(C) A lease of real property owned by the United States, if the estimated annual rental is more than $50,000.

(D) A transfer of real property owned by the United States to another Federal agency or to a State, if the estimated value is more than $50,000.

(E) A transfer of excess real property owned by the United States to a disposal agency, if the estimated value is more than $50,000.

(2) SUMMARY OF GENERAL PLAN REQUIRED FOR CERTAIN TRANSACTIONS.—If a transaction covered by clause (A) or (B) of paragraph (1) is part of a project, the report must include a summarization of the general plan for that project, including an estimate of the total cost of the lands to be acquired or leases to be made.

(c) ANNUAL REPORTS TO ARMED SERVICES COMMITTEES.—The Director of the Office of Civil and Defense Mobilization shall report annually to the Committees on Armed Services of the Senate and the House of Representatives on transactions described in subsection (a) that involve an estimated value of more than $5,000 but not more than $50,000.

(d) STATEMENT OF COMPLIANCE IS CONCLUSIVE.—A statement in an instrument of conveyance, including a lease, that the requirements of this section have been met, or that the conveyance is not subject to this section, is conclusive.

Subchapter III—Miscellaneous Authorities

§ 20531. National Disaster Recovery Strategy

(a) IN GENERAL.—The Administrator, in coordination with the Secretary of Housing and Urban Development, the Administrator of the Environmental Protection Agency, the Secretary of Agriculture, the Secretary of Commerce, the Secretary of the Treasury, the Secretary of Transportation, the Administrator of the Small Business Administration, the Assistant Secretary for Indian Affairs of the Department of the Interior, and the heads of other appropriate Federal agencies, State, local, and tribal government officials (including through the National Advisory Council), and representatives of appropriate nongovernmental organizations, shall develop, coordinate, and maintain a National Disaster Recovery Strategy to serve as a guide to recovery efforts after major disasters and emergencies.

(b) CONTENTS.—The National Disaster Recovery Strategy shall—

(1) outline the most efficient and cost-effective Federal programs that will meet the recovery needs of States, local and tribal governments, and individuals and households affected by a major disaster;

(2) clearly define the role, programs, authorities, and responsibilities of each Federal agency that may be of assistance in providing assistance in the recovery from a major disaster;

(3) promote the use of the most appropriate and cost-effective building materials (based on the hazards present in an area) in an area affected by a major disaster, with the goal of encouraging the construction of disaster-resistant buildings; and

(4) describe in detail the programs that may be offered by the agencies described in paragraph (2), including—

(A) discussing funding issues;

(B) detailing how responsibilities under the National Disaster Recovery Strategy will be shared; and

(C) addressing other matters concerning the cooperative effort to provide recovery assistance.

(c) REPORT.—

(1) IN GENERAL.—The Administrator shall submit to the appropriate committees of Congress a report describing in detail the National Disaster Recovery Strategy and any additional authorities necessary to implement any portion of the National Disaster Recovery Strategy.

(2) UPDATE.—The Administrator shall submit to the appropriate committees of Congress a report updating the report submitted under paragraph (1)—

(A) on the same date that any change is made to the National Disaster Recovery Strategy; and

(B) on a periodic basis after the submission of the report under paragraph (1), but not less than once every 5 years after the date of the submission.

§ 20532. National Disaster Housing Strategy

(a) IN GENERAL.—The Administrator, in coordination with representatives of the Federal agencies, governments, and organizations listed in subsection (b)(2), the National Advisory Council, the National Council on Disability, and other entities at the Administrator's discretion, shall develop, coordinate, and maintain a National Disaster Housing Strategy.

(b) CONTENTS.—The National Disaster Housing Strategy shall—

(1) outline the most efficient and cost-effective Federal programs that will best meet the short-term and long-term housing needs of individuals and households affected by a major disaster;

(2) clearly define the role, programs, authorities, and responsibilities of each entity in providing housing assistance in the event of a major disaster, including—

(A) the Agency;

(B) the Department of Housing and Urban Development;

(C) the Department of Agriculture;

(D) the Department of Veterans Affairs;

(E) the Department of Health and Human Services;

(F) the Bureau of Indian Affairs;

(G) any other Federal agency that may provide housing assistance in the event of a major disaster;

(H) the American Red Cross; and

(I) State, local, and tribal governments;

(3) describe in detail the programs that may be offered by the entities described in paragraph (2), including—

(A) outlining any funding issues;

(B) detailing how responsibilities under the National Disaster Housing Strategy will be shared; and

(C) addressing other matters concerning the cooperative effort to provide housing assistance during a major disaster;

(4) consider methods through which housing assistance can be provided to individuals and households where employment and other resources for living are available;

(5) describe programs directed to meet the needs of special-needs and low-income populations and ensure that a sufficient number of housing units are provided for individuals with disabilities;

(6) describe plans for the operation of clusters of housing provided to individuals and households, including access to public services, site management, security, and site density;

(7) describe plans for promoting the repair or rehabilitation of existing rental housing, including through lease agreements or other means, in order to improve the provision of housing to individuals and households under section 408 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5174); and

(8) describe any additional authorities necessary to carry out any portion of the strategy.

(c) GUIDANCE.—The Administrator should develop and make publicly available guidance on—

(1) types of housing assistance available under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) to individuals and households affected by an emergency or major disaster;

(2) eligibility for assistance (including, where appropriate, the continuation of assistance); and

(3) application procedures for assistance.

(d) REPORT.—

(1) IN GENERAL.—The Administrator shall submit to the appropriate committees of Congress a report describing in detail the National Disaster Housing Strategy, including programs directed to meeting the needs of populations with special needs.

(2) UPDATE.—The Administrator shall submit to the appropriate committees of Congress a report updating the report submitted under paragraph (1)—

(A) on the same date that any change is made to the National Disaster Housing Strategy; and

(B) on a periodic basis after the submission of the report under paragraph (1), but not less than once every 5 years after the date of the submission.

§ 20533. Individuals with disabilities guidelines

The Administrator, in coordination with the National Advisory Council, the National Council on Disability, the Interagency Coordinating Council on Emergency Preparedness and Individuals With Disabilities established under Executive Order No. 13347 (69 Fed. Reg. 44573), and the Disability Coordinator (established under section 11313 of this title), shall develop guidelines to accommodate individuals with disabilities, which shall include guidelines for—

(1) the accessibility of, and communications and programs in, shelters, recovery centers, and other facilities; and

(2) devices used in connection with disaster operations, including first aid stations, mass feeding areas, portable payphone stations, portable toilets, and temporary housing.

§ 20534. Reunification

(a) DEFINITIONS.—In this section:

(1) CHILD LOCATOR CENTER.—The term ''Child Locator Center'' means the National Emergency Child Locator Center established under subsection (b).

(2) DECLARED EVENT.—The term ''declared event'' means a major disaster or emergency.

(3) DISPLACED ADULT.—The term ''displaced adult'' means an individual 21 years of age or older who is displaced from the habitual residence of that individual as a result of a declared event.

(4) DISPLACED CHILD.—The term ''displaced child'' means an individual under 21 years of age who is displaced from the habitual residence of that individual as a result of a declared event.

(b) NATIONAL EMERGENCY CHILD LOCATOR CENTER.—

(1) IN GENERAL.—The Administrator, in coordination with the Attorney General of the United States, shall establish in the National Center for Missing and Exploited Children the National Emergency Child Locator Center. In establishing the Child Locator Center, the Administrator shall establish procedures to make all relevant information available to the Child Locator Center in a timely manner to facili-

tate the expeditious identification and reunification of children with their families.

(2) PURPOSES.—The purposes of the Child Locator Center are to—

(A) enable individuals to provide to the Child Locator Center the name of, and other identifying information about, a displaced child or a displaced adult who may have information about the location of a displaced child;

(B) enable individuals to receive information about other sources of information about displaced children and displaced adults; and

(C) assist law enforcement in locating displaced children.

(3) RESPONSIBILITIES AND DUTIES.—The responsibilities and duties of the Child Locator Center are to—

(A) establish a toll-free telephone number to receive reports of displaced children and information about displaced adults that may assist in locating displaced children;

(B) create a website to provide information about displaced children;

(C) deploy its staff to the location of a declared event to gather information about displaced children;

(D) assist in the reunification of displaced children with their families;

(E) provide information to the public about additional resources for disaster assistance;

(F) work in partnership with Federal, State, and local law enforcement agencies;

(G) provide technical assistance in locating displaced children;

(H) share information on displaced children and displaced adults with governmental agencies and nongovernmental organizations providing disaster assistance;

(I) use its resources to gather information about displaced children;

(J) refer reports of displaced adults to—

(i) an entity designated by the Attorney General to provide technical assistance in locating displaced adults; and

(ii) the National Emergency Family Registry and Locator System established under section 20535(b) of this title;

(K) enter into cooperative agreements with Federal and State agencies and other organizations such as the American Red Cross as necessary to implement the mission of the Child Locator Center; and

(L) develop an emergency response plan to prepare for the activation of the Child Locator Center.

§ 20535. National Emergency Family Registry and Locator System

(a) DEFINITION OF DISPLACED INDIVIDUAL.—In this section, the term ''displaced individual'' means an individual displaced by an emergency or major disaster.

(b) ESTABLISHMENT.—The Administrator shall establish a National Emergency Family Registry and Locator System to help reunify families separated after an emergency or major disaster.

(c) OPERATION.—The National Emergency Family Registry and Locator System shall—

(1) allow a displaced adult (including a medical patient) to voluntarily register (and allow an adult who is the parent or guardian of a displaced child to register the child), by submitting personal information to be entered into a database (such as the name, current location of residence, and any other relevant information that could be used by others seeking to locate that individual);

(2) ensure that information submitted under paragraph (1) is accessible to those individuals named by a displaced individual and to law enforcement officials;

(3) be accessible through the Internet and through a toll-free number, to receive reports of displaced individuals; and

(4) include a means of referring displaced children to the National Emergency Child Locator Center established under section 20534(b) of this title.

(d) INFORMING THE PUBLIC.—The Administrator shall establish a mechanism to inform the public about the National Emergency Family Registry and Locator System and its potential to assist in reunifying displaced individuals with their families.

(e) COORDINATION.—The Administrator shall enter into a memorandum of understanding with the Department of Justice, the National Center for Missing and Exploited Children, the Department of Health and Human Services, and the American Red Cross and other relevant private organizations that will enhance the sharing of information to facilitate reunifying displaced individuals (including medical patients) with their families.

Chapter 207—Prevention of Fraud, Waste, and Abuse

Sec.

§ 20701. Advance contracting

(a) ENTERING INTO CONTRACTS.—

(1) IN GENERAL.—The Administrator shall enter into 1 or more contracts for recurring disaster response requirements, including specific goods and services, for which the Agency is capable of contracting in advance of a natural disaster or act of terrorism or other man-made disaster in a cost-effective manner, using a contracting strategy that maximizes the use of advance contracts to the extent practical and cost-effective. A previously awarded contract for goods or services may be maintained in fulfilling this requirement.

(2) CONSIDERED FACTORS.—Before entering into any contract under this subsection, the Administrator shall consider section 307 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5150).

(3) PRE-NEGOTIATED FEDERAL CONTRACTS FOR GOODS AND SERVICES.—The Administrator, in coordination with State and local governments and other Federal agencies, shall establish a process to ensure that Federal pre-negotiated contracts for goods and services are coordinated with State and local governments, as appropriate.

(4) PRE-NEGOTIATED STATE AND LOCAL CONTRACTS FOR GOODS AND SERVICES.—The Administrator shall encourage State and local governments to establish pre-negotiated contracts with vendors for goods and services in advance of natural disasters and acts of terrorism or other man-made disasters.

(b) MAINTENANCE OF CONTRACTS.—The Administrator is responsible for maintaining contracts for appropriate levels of goods and services in accordance with a contracting strategy that maximizes the use of advance contracts to the extent practical and cost-effective.

(c) REPORT ON CONTRACTS NOT USING COMPETITIVE PROCEDURES.—At the end of each fiscal quarter, the Administrator shall submit a report on each disaster assistance contract entered into by the Agency by other than competitive procedures to the appropriate committees of Congress.

(d) UPDATED REPORT.—Not later than 180 days after December 31, 2020, the Administrator shall submit to the appropriate committees of Congress an updated report that contains—

(1) the information required in the initial report under subparagraphs (A) and (B) of subsection (a)(1) of section 691 of the Post-

Katrina Emergency Reform Act of 2006 (Public Law 109–295, 120 Stat. 1457); and

(2) an updated strategy described in section 691(a)(1)(C) of the Act that clearly defines—

(A) the objectives of advance contracts;

(B) how advance contracts contribute to disaster response operations of the Agency;

(C) how to maximize the award of advance contracts to small business concerns, as defined in section 3 of the Small Business Act (15 U.S.C. 632); and

(D) whether and how advance contracts should be prioritized in relation to new post-disaster contract awards.

(e) ADDITIONAL DUTIES OF ADMINISTRATOR.—

(1) ENSURE THAT HEAD OF CONTRACTING ACTIVITY CARRIES OUT CERTAIN DUTIES.—The Administrator shall ensure that the head of contracting activity of the Agency—

(A) not later than 270 days after December 31, 2020, updates the Disaster Contracting Desk Guide of the Agency to provide specific guidance—

(i) on whether and under what circumstances contracting officers should consider using existing advance contracts entered into in accordance with this section prior to making new post-disaster contract awards, and include this guidance in existing semi-annual training given to contracting officers; and

(ii) for contracting officers to perform outreach to State and local governments on the potential benefits of establishing their own pre-negotiated advance contracts;

(B) adheres to hard copy contract file management requirements in effect to ensure that the files relating to advance contracts entered into in accordance with this section are complete and up to date, whether the files will be transferred into the Electronic Contract Filing System of the Agency or remain in hard copy format;

(C) notifies contracting officers of the 3-day time frame requirement for entering completed award documentation into the contract writing system of the Agency when executing notice-to-proceed documentation;

(D) not later than 180 days after December 31, 2020, revises the reporting methodology of the Agency to ensure that all disaster contracts are included in each quarterly report submitted to

the appropriate congressional committees under this section on disaster contract actions;

(E) identifies a single centralized resource listing advance contracts entered into under this section and ensures that source is current and up to date and includes all available advance contracts; and

(F) communicates complete and up-to-date information on available advance contracts to State and local governments to inform their advance contracting efforts.

(2) UPDATE AND IMPLEMENT GUIDANCE.—Not later than 180 days after December 31, 2020, the Administrator shall update and implement guidance for program office and acquisition personnel of the Agency to—

(A) identify acquisition planning time frames and considerations across the entire acquisition planning process of the Agency; and

(B) clearly communicate the purpose and use of a master acquisition planning schedule.

§ 20702. Oversight and accountability of Federal disaster expenditures

(a) DEFINITION OF OVERSIGHT FUNDS.—In this section, the term ''oversight funds'' means funds referred to in subsection (b) that are designated for use in performing oversight activities.

(b) AUTHORITY OF ADMINISTRATOR TO DESIGNATE FUNDS FOR OVERSIGHT ACTIVITIES.—The Administrator may designate up to 1 percent of the total amount provided to a Federal agency for a mission assignment as oversight funds to be used by the recipient agency for performing oversight of activities carried out under the Agency reimbursable mission assignment process. The funds are available until expended.

(c) USE OF FUNDS.—

(1) TYPES OF OVERSIGHT ACTIVITIES.—Oversight funds may be used for the following types of oversight activities related to Agency mission assignments:

(A) Monitoring, tracking, and auditing expenditures of funds.

(B) Ensuring that sufficient management and internal control mechanisms are available so that Agency funds are spent appropriately and in accordance with all applicable laws and regulations.

(C) Reviewing selected contracts and other activities.

(D) Investigating allegations of fraud involving Agency funds.

(E) Conducting and participating in fraud prevention activities with other Federal, State, and local government personnel and contractors.

(2) PLANS AND REPORTS.—Oversight funds may be used to issue the plans required under subsection (f) and the reports required under subsection (g).

(d) RESTRICTION ON USE OF FUNDS.—Oversight funds may not be used to finance existing agency oversight responsibilities related to direct agency appropriations used for disaster response, relief, and recovery activities.

(e) METHODS OF OVERSIGHT ACTIVITIES.—

(1) IN GENERAL.—Oversight activities may be carried out by an agency under this section either directly or by contract. The activities may include evaluations and financial and performance audits.

(2) COORDINATION OF OVERSIGHT ACTIVITIES.—To the extent practicable, evaluations and audits under this section shall be performed by the inspector general of the agency.

(f) DEVELOPMENT OF OVERSIGHT PLANS.—

(1) IN GENERAL.—If an agency receives oversight funds for a fiscal year, the head of the agency shall prepare a plan describing the oversight activities for disaster response, relief, and recovery anticipated to be undertaken during the subsequent fiscal year.

(2) SELECTION OF OVERSIGHT ACTIVITIES.—In preparing the plan, the head of the agency shall select oversight activities based upon a risk assessment of those areas that present the greatest risk of fraud, waste, and abuse.

(3) SCHEDULE.—The plan shall include a schedule for conducting oversight activities, including anticipated dates of completion.

(g) FEDERAL DISASTER ASSISTANCE ACCOUNTABILITY REPORTS.—An agency receiving oversight funds under this section shall submit annually to the Administrator and the appropriate committees of Congress a consolidated report regarding the use of the funds, including information summarizing oversight activities and the results achieved.

§ 20703. Limitation on length of certain noncompetitive contracts

(a) COVERED CONTRACTS.—This section applies to any contract in an amount greater than the simplified acquisition threshold (as defined by section 134 of title 41) entered into by the Department to facilitate response to or recovery from a natural disaster, act of terrorism, or other man-made disaster.

(b) REGULATIONS.—The Secretary shall promulgate regulations applicable to contracts described in subsection (a) to restrict the contract period of a contract entered into using procedures other than competitive procedures pursuant to the exception provided in section 3304(a)(2) of title 41 to the minimum contract period necessary—

(1) to meet the urgent and compelling requirements of the work to be performed under the contract; and

(2) to enter into another contract for the required goods or services through the use of competitive procedures.

(c) SPECIFIC CONTRACT PERIOD.—The regulations promulgated under subsection (b) shall require the contract period to not exceed 150 days, unless the Secretary determines that exceptional circumstances apply.

§ 20704. Fraud, waste, and abuse controls

(a) IN GENERAL.—The Administrator shall ensure that—

(1) all programs in the Agency administering Federal disaster relief assistance develop and maintain proper internal management controls to prevent and detect fraud, waste, and abuse;

(2) application databases used by the Agency to collect information on eligible recipients must record disbursements;

(3) tracking to prevent and detect fraud, waste, and abuse is designed to highlight and identify ineligible applications; and

(4) the databases used to collect information from applications for assistance are integrated with disbursements and payment records.

(b) AUDITS AND REVIEWS REQUIRED.—The Administrator shall ensure that any database or similar application processing system for Federal disaster relief assistance programs administered by the Agency undergoes a review by the Inspector General of the Department to determine the existence and implementation of internal controls required under this section and section 408(i) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5174(i)).

§ 20705. Registry of disaster response contractors

(a) DEFINITIONS.—In this section, the terms ''small business concern'', ''small business concern owned and controlled by service-disabled veterans'', ''small business concern owned and controlled by socially and economically disadvantaged individuals'', and ''small business concern owned and controlled by women'' have the meanings given the terms under the Small Business Act (15 U.S.C. 631 et seq.).

(b) REGISTRY.—

(1) IN GENERAL.—The Administrator shall establish and maintain a registry of contractors who are willing to perform debris removal, distribution of supplies, reconstruction, and other disaster or emergency relief activities.

(2) CONTENTS.—The registry shall include, for each business concern—

(A) the name of the business concern;

(B) the location of the business concern;

(C) the area served by the business concern;

(D) the type of good or service provided by the business concern;

(E) the bonding level of the business concern; and

(F) whether the business concern is—

(i) a small business concern;

(ii) a small business concern owned and controlled by socially and economically disadvantaged individuals;

(iii) a small business concern owned and controlled by women; or

(iv) a small business concern owned and controlled by service-disabled veterans.

(3) SOURCE OF INFORMATION.—

(A) SUBMISSION.—Information maintained in the registry shall be submitted on a voluntary basis and be kept current by the submitting business concerns.

(B) ATTESTATION.—Each business concern submitting information to the registry shall submit—

(i) an attestation that the information is true; and

(ii) documentation supporting the attestation.

(C) VERIFICATION.—The Administrator shall verify that the documentation submitted by each business concern supports the information submitted by that business concern.

(4) AVAILABILITY.—The registry shall be made generally available on the website of the Agency.

(5) CONSULTATION OF REGISTRY AS PART OF ACQUISITION PLANNING.—A Federal agency shall consult the registry as part of the acquisition planning for contracting for debris removal, distribution of supplies in a disaster, reconstruction, and other disaster or emergency relief activities.

§ 20706. Fraud prevention training program

The Administrator shall develop and implement a program to provide training on the prevention of waste, fraud, and abuse of Federal disaster relief assistance relating to the response to or recovery from natural disasters and acts of terrorism or other man-made disasters and ways to identify potential waste, fraud, and abuse.

Subtitle III—Port Security and Accountability

Chapter 301—General

§ 30101. Definitions

In this subtitle:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—Except as otherwise provided, the term ''appropriate congressional committees'' means—

(A) the Committee on Appropriations of the Senate;

(B) the Committee on Commerce, Science, and Transportation of the Senate;

(C) the Committee on Finance of the Senate;

(D) the Committee on Homeland Security and Governmental Affairs of the Senate;

(E) the Committee on Appropriations of the House of Representatives;

(F) the Committee on Homeland Security of the House of Representatives;

(G) the Committee on Transportation and Infrastructure of the House of Representatives;

(H) the Committee on Ways and Means of the House of Representatives; and

(I) other congressional committees, as appropriate.

(2) COMMERCIAL CUSTOMS OPERATIONS ADVISORY COMMITTEE.—The term ''Commercial Customs Operations Advisory Committee'' means the Advisory Committee established under section 109 of the Trade Facilitation and Trade Enforcement Act of 2015 (19 U.S.C. 4316) or any successor committee.

(3) COMMERCIAL SEAPORT PERSONNEL.—The term ''commercial seaport personnel'' includes any person engaged in an activity relating to the loading or unloading of cargo or passengers, the movement or tracking of cargo, the maintenance and repair of intermodal equipment, the operation of cargo-related equipment (whether or not integral to the vessel), and the handling of mooring lines on the dock when a vessel is made fast or let go in the United States.

(4) COMMISSIONER.—The term ''Commissioner'' means the Commissioner responsible for U.S. Customs and Border Protection.

(5) CONTAINER.—The term ''container'' has the meaning given the term in the International Convention for Safe Containers, with annexes, done at Geneva, December 2, 1972 (29 UST 3707).

(6) CONTAINER SECURITY DEVICE.—The term ''container security device'' means a device, or system—

(A) designed, at a minimum—

(i) to identify positively a container;

(ii) to detect and record unauthorized intrusion into a container; and

(iii) to secure a container against tampering throughout the supply chain; and

(B) that has a low false alarm rate, as determined by the Secretary.

(7) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(8) EXAMINATION.—The term ''examination'' means an inspection of cargo to detect the presence of mis-declared, restricted, or prohibited items that utilizes nonintrusive imaging and detection technology.

(9) INSPECTION.—The term ''inspection'' means the comprehensive process used by U.S. Customs and Border Protection—

(A) 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; and

(B) that may include screening, conducting an examination, or conducting a search.

(10) 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.

(11) RADIATION DETECTION EQUIPMENT.—The term ''radiation detection equipment'' means any technology that is capable of detecting or identifying nuclear and radiological material or nuclear and radiological explosive devices.

(12) SCAN.—The term ''scan'' means utilizing nonintrusive imaging equipment, radiation detection equipment, or both, to capture data, including images of a container.

(13) SCREENING.—The term ''screening'' means a visual or automated review of information about goods, including manifest or entry documentation accompanying a shipment being imported into the United States, to determine the presence of mis-declared, restricted, or prohibited items and assess the level of threat posed by the affected cargo.

(14) SEARCH.—The term ''search'' means an intrusive examination in which a container is opened and its contents are devanned and visually inspected for the presence of mis-declared, restricted, or prohibited items.

(15) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(16) TRANSPORTATION DISRUPTION.—The term ''transportation disruption'' means any significant delay, interruption, or stoppage in the flow of trade caused by a natural disaster, heightened threat level, act of terrorism, or transportation security incident.

(17) TRANSPORTATION SECURITY INCIDENT.—The term ''transportation security incident'' has the meaning given the term in section 70101(6) of title 46.

Chapter 303—Security of United States Seaports

§ 30301. Port Security Exercise Program

(a) IN GENERAL.—The Secretary, acting through the Administrator of the Federal Emergency Management Agency and in coordination with the Commandant of the Coast Guard, shall establish a Port Security Exercise Program (in this section referred to as the ''Exercise Program'') to test and evaluate the capabilities of Federal, State, local, and foreign governments, commercial seaport personnel and management, governmental and nongovernmental emergency response providers, the private sector, or any other organization or entity, as the Secretary determines to be appropriate, to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at facilities required to submit a plan under section 70103(c) of title 46.

(b) REQUIREMENTS.—The Secretary shall ensure that the Exercise Program—

(1) conducts, on a periodic basis, port security exercises at the facilities that are—

(A) scaled and tailored to the needs of each facility;

(B) live, in the case of the most at-risk facilities;

(C) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(D) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Pre-

paredness Goal, the National Maritime Transportation Security Plan, and other national initiatives;

(E) evaluated against clear and consistent performance measures;

(F) assessed to learn best practices, which shall be shared with appropriate Federal, State, and local officials, commercial seaport personnel and management, governmental and nongovernmental emergency response providers, and the private sector; and

(G) followed by remedial action in response to lessons learned; and

(2) assists State and local governments and facilities in designing, implementing, and evaluating exercises that—

(A) conform to the requirements of paragraph (1); and

(B) are consistent with any applicable Area Maritime Transportation Security Plan and State or Urban Area Homeland Security Plan.

(c) IMPROVEMENT PLAN.—The Secretary shall establish a port security exercise improvement plan process to—

(1) identify and analyze each port security exercise for lessons learned and best practices;

(2) disseminate lessons learned and best practices to participants in the Exercise Program;

(3) monitor the implementation of lessons learned and best practices by participants in the Exercise Program; and

(4) conduct remedial action tracking and long-term trend analysis.

§ 30302. Facility exercise requirements

The Secretary of the Department in which the Coast Guard is operating shall require each high-risk facility to conduct live or full-scale exercises described in section 105.220(c) of title 33, Code of Federal Regulations, not less frequently than once every 2 years, in accordance with the facility security plan required under section 70103(c) of title 46.

§ 30303. Domestic radiation detection and imaging

(a) SCANNING CONTAINERS.—Subject to section 318 of the Tariff Act of 1930 (19 U.S.C. 1318), all containers entering the United States through the 22 ports through which the greatest volume of containers enter the United States by vessel shall be scanned for radiation. To the extent practicable, the Secretary shall deploy next-generation radiation detection technology.

(b) STRATEGY.—The Secretary shall develop and implement a strategy for the deployment of radiation detection capabilities that includes—

(1) a risk-based prioritization of ports of entry at which radiation detection equipment will be deployed;

(2) a proposed timeline of when radiation detection equipment will be deployed at each port of entry identified under paragraph (1);

(3) the type of equipment to be used at each port of entry identified under paragraph (1), including the joint deployment and utilization of radiation detection equipment and nonintrusive imaging equipment;

(4) standard operating procedures for examining containers with the equipment, including sensor alarming, networking, and communications and response protocols;

(5) operator training plans;

(6) an evaluation of the environmental health and safety impacts of nonintrusive imaging technology and a radiation risk reduction plan, in consultation with the Nuclear Regulatory Commission, the Occupational Safety and Health Administration, and the National Institute for Occupational Safety and Health, that seeks to minimize radiation exposure of workers and the public to levels as low as reasonably achievable;

(7) the policy of the Department for using nonintrusive imaging equipment in tandem with radiation detection equipment; and

(8) a classified annex that—

(A) details plans for covert testing; and

(B) outlines the risk-based prioritization of ports of entry identified under paragraph (1).

(c) EXPANSION TO OTHER UNITED STATES PORTS OF ENTRY.—

(1) IN GENERAL.—The Secretary shall expand the strategy developed under subsection (b), in a manner consistent with the requirements of subsection (b), to provide for the deployment of radiation detection capabilities at all other United States ports of entry not covered by the strategy developed under subsection (b).

(2) RISK ASSESSMENT.—In expanding the strategy under paragraph (1), the Secretary shall identify and assess the risks to those other ports of entry in order to determine what equipment and practices will best mitigate the risks.

(d) STANDARDS.—The Secretary, acting through the Assistant Secretary for the Countering Weapons of Mass Destruction Office and in collaboration with the National Institute of Standards and Technology, shall publish technical capability standards and recommended standard operating procedures for the use of nonintrusive imaging and radiation detection equipment in the United States. The standards and procedures—

(1) should take into account relevant standards and procedures utilized by other Federal departments or agencies as well as those developed by international bodies; and

(2) shall not be designed so as to endorse specific companies or create sovereignty conflicts with participating countries.

(e) INTERMODAL RAIL RADIATION DETECTION TEST CENTER.—

(1) ESTABLISHMENT.—In accordance with subsection (b), and to comply with this section, the Secretary shall establish an Intermodal Rail Radiation Detection Test Center (in this subsection referred to as the ''Test Center'').

(2) PROJECTS.—The Secretary shall conduct multiple, concurrent projects at the Test Center to rapidly identify and test concepts specific to the challenges posed by on-dock rail.

(3) LOCATION.—The Test Center shall be located in a public port facility at which a majority of the containerized cargo is directly laden from (or unladen to) on-dock, intermodal rail.

§ 30304. Integration of detection equipment and technologies

The Secretary is responsible for ensuring that domestic chemical, biological, radiological, and nuclear detection equipment and technologies are integrated, as appropriate, with other border security systems and detection technologies.

§ 30305. Random searches of containers

The Secretary, acting through the Commissioner, shall develop and implement a plan, utilizing best practices for empirical scientific research design and random sampling, to conduct random searches of containers in addition to any targeted or pre-shipment inspection of the containers required by law or regulation or conducted under any other program conducted by the Secretary. Nothing in this section shall be construed to mean that implementation of the random sampling plan precludes additional searches of containers not inspected pursuant to the plan.

§ 30306. Threat assessment screening of port truck drivers

The Secretary shall implement a threat assessment screening, including name-based checks against terrorist watch lists and immigration status checks, for all port truck drivers with access to secure areas of a port who have a commercial driver's license but do not have a current and valid hazardous materials endorsement issued under part 1572 of title 49, Code of Federal Regulations, that is the same as the threat assessment screening required for facility employees and longshoremen by the Commandant of the Coast Guard under Coast Guard Notice USCG-2006-24189 (71 Fed. Reg. 25066).

§ 30307. Center of Excellence for Maritime Domain Awareness

(a) ESTABLISHMENT.—The Secretary shall establish a university-based Center for Excellence for Maritime Domain Awareness following the merit-review processes and procedures that have been established by the Secretary for selecting university program centers of excellence.

(b) DUTIES.—The Center established under subsection (a) shall—

(1) prioritize its activities based on the ''National Plan To Improve Maritime Domain Awareness'' published by the Department in October 2005;

(2) recognize the extensive previous and ongoing work and existing competence in the field of maritime domain awareness at numerous academic and research institutions, such as the Naval Postgraduate School;

(3) leverage existing knowledge and continue development of a broad base of expertise in academia and industry in maritime domain awareness; and

(4) provide educational, technical, and analytical assistance to Federal agencies with responsibilities for maritime domain awareness, including the Coast Guard, to focus on the need for interoperability, information sharing, and common information technology standards and architecture.

Chapter 305—Security of the International Supply Chain

Subchapter I—General

§ 30501. Strategic plan to enhance the security of the international supply chain

(a) STRATEGIC PLAN.—The Secretary, in consultation with appropriate Federal, State, local, and tribal government agencies and private-sector stakeholders responsible for security matters that affect or relate to the movement of containers through the international supply chain, shall develop, implement, and update, triennially, a strategic plan to enhance the security of the international supply chain.

(b) REQUIREMENTS.—The strategic plan required under subsection (a) shall—

(1) describe the roles, responsibilities, and authorities of Federal, State, local, and tribal government agencies and private-sector stakeholders that relate to the security of the movement of containers through the international supply chain;

(2) identify and address gaps and unnecessary overlaps in the roles, responsibilities, or authorities described in paragraph (1);

(3) identify and make recommendations regarding legislative, regulatory, and organizational changes necessary to improve coordination among the entities or to enhance the security of the international supply chain;

(4) provide measurable goals, including objectives, mechanisms, and a schedule, for furthering the security of commercial operations from point of origin to point of destination;

(5) build on available resources and consider costs and benefits;

(6) provide incentives for additional voluntary measures to enhance cargo security, as recommended by the Commissioner;

(7) consider the impact of supply chain security requirements on small- and medium-sized companies;

(8) include a process for sharing intelligence and information with private-sector stakeholders to assist in their security efforts;

(9) identify a framework for prudent and measured response in the event of a transportation security incident involving the international supply chain;

(10) provide protocols for the expeditious resumption of the flow of trade under section 30502 of this title;

(11) consider the linkages between supply chain security and security programs in other systems of movement, including travel security and terrorism finance programs; and

(12) expand on and relate to existing strategies and plans, including the National Response Plan, the National Maritime Transportation Security Plan, the National Strategy for Maritime Security, and the 8 supporting plans of the Strategy, as required by Homeland Security Presidential Directive–13.

(c) CONSULTATION.—In developing protocols under subsection (b)(10), the Secretary shall consult with Federal, State, local, and private-sector stakeholders, including the National Maritime Security Advisory Committee and the Commercial Operations Advisory Committee.

(d) COMMUNICATION.—To the extent practicable, the strategic plan developed under subsection (a) shall provide for coordination with, and lines of communication among, appropriate Federal, State, local, and private-sector stakeholders on law enforcement actions, intermodal rerouting plans, and other strategic infrastructure issues resulting from a transportation security incident or transportation disruption.

(e) UTILIZATION OF ADVISORY COMMITTEES.—As part of the consultations described in subsection (a), the Secretary shall, to the extent practicable, utilize the Homeland Security Advisory Committee, the National Maritime Security Advisory Committee, and the Commercial Operations Advisory Committee to review, as necessary, the strategic plan and any subsequent updates to the strategic plan.

(f) INTERNATIONAL STANDARDS AND PRACTICES.—In furtherance of the strategic plan required under subsection (a), the Secretary is encouraged to consider proposed or established standards and practices of foreign governments and international organizations, including the International Maritime Organization, the World Customs Organization, the International Labor Organization, and the International Organization for Standardization, as appropriate, to establish standards and best practices for the security of containers moving through the international supply chain.

(g) UPDATE REPORTS.—Not later than 270 days after October 5, 2018, and triennially thereafter, the Secretary shall submit to the appropriate congressional committees a report that contains updates to the strategic plan submitted under subsection (a) since the prior report.

§ 30502. Post-incident resumption of trade

(a) IN GENERAL.—The Secretary shall develop and update, as necessary, protocols for the resumption of trade under section 30501(b)(10) of this title in the event of a transportation disruption or a transportation security incident. The protocols shall include—

(1) the identification of the appropriate initial incident commander, if the Commandant of the Coast Guard is not the appropriate indi-

vidual, and lead departments, agencies, or offices to execute the protocols;

(2) a plan to redeploy resources and personnel, as necessary, to reestablish the flow of trade;

(3) a plan to provide training for the periodic instruction of personnel of U.S. Customs and Border Protection, the Coast Guard, and the Transportation Security Administration in trade resumption functions and responsibilities; and

(4) appropriate factors for establishing prioritization of vessels and cargo determined by the President to be critical for response and recovery, including factors relating to public health, national security, and economic need.

(b) VESSELS.—In determining the prioritization of vessels accessing facilities (as defined under section 70101 of title 46), the Commandant of the Coast Guard may, to the extent practicable and consistent with the protocols and plans required under this section to ensure the safe and secure transit of vessels to ports in the United States after a transportation security incident, give priority to a vessel—

(1) that has an approved security plan under section 70103(c) of title 46, or a valid international ship security certificate, as provided under part 104 of title 33, Code of Federal Regulations;

(2) that is manned by individuals who are described in section 70105(b)(2)(B) of title 46; and

(3) that is operated by validated participants in the Customs–Trade Partnership Against Terrorism (in this chapter referred to as ''C–TPAT'') program.

(c) CARGO.—In determining the prioritization of the resumption of the flow of cargo and consistent with the protocols established under this section, the Commissioner may give preference to cargo—

(1) entering a port of entry directly from a foreign seaport designated under the Container Security Initiative;

(2) from the supply chain of a validated C–TPAT participant and other private-sector entities, as appropriate; or

(3) that has undergone—

(A) a nuclear or radiological detection scan;

(B) an x-ray, density, or other imaging scan; and

(C) a system to positively identify the container at the last port of departure prior to arrival in the United States, which data has been evaluated and analyzed by personnel of U.S. Customs and Border Protection.

(d) COORDINATION.—The Secretary shall ensure that there is appropriate coordination among the Commandant of the Coast Guard, the Commissioner, and other Federal officials following a maritime disruption or maritime transportation security incident in order to provide for the resumption of trade.

(e) COMMUNICATION.—Consistent with section 30501 of this title, the Commandant of the Coast Guard, the Commissioner, and other appropriate Federal officials shall promptly communicate any revised procedures or instructions intended for the private sector following a maritime disruption or maritime transportation security incident.

§ 30503. Automated targeting system

(a) IN GENERAL.—The Secretary, acting through the Commissioner, shall—

(1) identify and seek the submission of data related to the movement of a shipment of cargo through the international supply chain; and

(2) analyze the data described in paragraph (1) to identify high-risk cargo for inspection.

(b) REQUIREMENT.—The Secretary, acting through the Commissioner, shall require the electronic transmission to the Department of additional data elements for improved high-risk targeting, including appropriate security elements of entry data, as determined by the Secretary, to be provided as advanced information with respect to cargo destined for importation into the United States prior to loading of the cargo on vessels at foreign seaports.

(c) CONSIDERATION.—The Secretary, acting through the Commissioner, shall—

(1) consider the cost, benefit, and feasibility of—

(A) requiring additional non-manifest documentation;

(B) reducing the time period allowed by law for revisions to a container cargo manifest;

(C) reducing the time period allowed by law for submission of certain elements of entry data, for vessel or cargo; and

(D) taking other actions the Secretary considers beneficial for improving the information relied on for the Automated Targeting System and any successor targeting system in furthering the security and integrity of the international supply chain; and

(2) consult with stakeholders, including the Commercial Operations Advisory Committee, and identify to them the need for the information referred to in paragraph (1)(D), and the appropriate timing of its submission.

(d) REGULATIONS.—The Secretary shall promulgate regulations to carry out this section. In promulgating regulations, the Secretary shall adhere to the parameters applicable to the development of regulations under section 343(a) of the Customs Border Security Act of 2002 (19 U.S.C. 1415(a)), including provisions relating to consultation, technology, analysis, use of information, confidentiality, and timing requirements.

(e) SYSTEM IMPROVEMENTS.—The Secretary, acting through the Commissioner, shall—

(1) conduct, through an independent panel, a review of the effectiveness and capabilities of the Automated Targeting System;

(2) consider future iterations of the Automated Targeting System, which would incorporate smart features, such as more complex algorithms and real-time intelligence, instead of relying solely on rule sets that are periodically updated;

(3) ensure that the Automated Targeting System has the capability to electronically compare manifest and other available data for cargo entered into or bound for the United States to detect any significant anomalies between the data and facilitate the resolution of the anomalies;

(4) ensure that the Automated Targeting System has the capability to electronically identify, compile, and compare select data elements for cargo entered into or bound for the United States following a maritime transportation security incident, in order to efficiently identify cargo for increased inspection or expeditious release; and

(5) develop a schedule to address the recommendations of the Comptroller General, the Inspector General of the Department of the Treasury, and the Inspector General of the Department with respect to the operation of the Automated Targeting System.

(f) SECURE TRANSMISSION OF CERTAIN INFORMATION.—All information required by the Department from supply chain partners shall be transmitted in a secure fashion, as determined by the Secretary, so as to protect the information from unauthorized access.

§ 30504. Container security standards and procedures

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Secretary shall initiate a rulemaking proceeding to establish minimum standards and procedures for securing containers in transit to the United States.

(2) DEADLINE FOR ENFORCEMENT.—

(A) ENFORCEMENT OF RULE.—Not later than 2 years after the date on which the standards and procedures are established under

paragraph (1), all containers bound for ports of entry in the United States shall meet the standards and procedures.

(B) INTERIM REQUIREMENT.—If an interim final rule issued pursuant to the proceeding described in paragraph (1) was not issued by April 1, 2008—

(i) all containers in transit to the United States are required to meet the requirements of the International Organization for Standardization Publicly Available Specification 17712 standard for sealing containers; and

(ii) the requirements of this subparagraph cease to be effective on the effective date of the interim final rule issued under this subsection.

(b) REVIEW AND ENHANCEMENT.—The Secretary shall regularly review and enhance the standards and procedures established under subsection (a), as appropriate, based on tests of technologies as they become commercially available to detect container intrusion and the highest consequence threats, particularly weapons of mass destruction.

(c) INTERNATIONAL CARGO SECURITY STANDARDS.—The Secretary, in consultation with the Secretary of State, the Secretary of Energy, and other Federal Government officials, as appropriate, and with the Commercial Operations Advisory Committee, the Homeland Security Advisory Committee, and the National Maritime Security Advisory Committee, is encouraged to promote and establish international standards for the security of containers moving through the international supply chain with foreign governments and international organizations, including the International Maritime Organization, the International Organization for Standardization, the International Labor Organization, and the World Customs Organization.

(d) INTERNATIONAL TRADE AND OTHER OBLIGATIONS.—In carrying out this section, the Secretary shall consult with appropriate Federal departments and agencies and private-sector stakeholders and ensure that actions under this section do not violate international trade obligations or other international obligations of the United States.

§ 30505. Container Security Initiative

(a) ESTABLISHMENT.—The Secretary, acting through the Commissioner, shall establish and implement a program (in this section referred to as the ''Container Security Initiative'') to identify and examine or search maritime containers that pose a security risk before loading the containers in a foreign port for shipment to the United States, either directly or through a foreign port.

(b) ASSESSMENT.—The Secretary, acting through the Commissioner, may designate foreign seaports to participate in the Container Security Initiative

after the Secretary has assessed the costs, benefits, and other factors associated with the designation, including—

(1) the level of risk for the potential compromise of containers by terrorists, or other threats as determined by the Secretary;

(2) the volume of cargo being imported to the United States directly from, or being trans-shipped through, the foreign seaport;

(3) the results of the Coast Guard assessments conducted under section 70108 of title 46;

(4) the commitment of the government of the country in which the foreign seaport is located to cooperate with the Department in sharing critical data and risk management information and to maintain programs to ensure employee integrity; and

(5) the potential for validation of security practices at the foreign seaport by the Department.

(c) NOTIFICATION.—The Secretary shall notify the appropriate congressional committees of the designation of a foreign port under the Container Security Initiative or the revocation of a designation before notifying the public of the designation or revocation.

(d) NEGOTIATIONS.—The Secretary, in cooperation with the Secretary of State and in consultation with the United States Trade Representative, may enter into negotiations with the government of each foreign nation in which a seaport is designated under the Container Security Initiative to ensure full compliance with the requirements under the Container Security Initiative.

(e) OVERSEAS INSPECTIONS.—

(1) REQUIREMENTS AND PROCEDURES.—The Secretary shall—

(A) establish minimum technical capability criteria and standard operating procedures for the use of nonintrusive inspection and nuclear and radiological detection systems in conjunction with the Container Security Initiative;

(B) require each port designated under the Container Security Initiative to operate nonintrusive inspection and nuclear and radiological detection systems in accordance with the technical capability criteria and standard operating procedures established under subparagraph (A);

(C) continually monitor the technologies, processes, and techniques used to inspect cargo at ports designated under the Container Security Initiative to ensure adherence to the criteria and the use of the procedures; and

(D) consult with the Secretary of Energy in establishing the minimum technical capability criteria and standard operating procedures established under subparagraph (A) pertaining to radi-

ation detection technologies to promote consistency in detection systems at foreign ports designated under the Container Security Initiative.

(2) CONSTRAINTS.—The criteria and procedures established under paragraph (1)(A)—

(A) shall be consistent, as practicable, with relevant standards and procedures utilized by other Federal departments or agencies, or developed by international bodies if the United States consents to the standards and procedures;

(B) shall not apply to activities conducted under the Megaports Initiative of the Department of Energy; and

(C) shall not be designed to endorse the product or technology of any specific company or to conflict with the sovereignty of a country in which a foreign seaport designated under the Container Security Initiative is located.

(f) SAVINGS PROVISION.—The authority of the Secretary under this section shall not affect any authority or duplicate any efforts or responsibilities of the Federal Government with respect to the deployment of radiation detection equipment outside of the United States.

(g) COORDINATION.—The Secretary shall—

(1) coordinate with the Secretary of Energy, as necessary, to provide radiation detection equipment required to support the Container Security Initiative through the Department of Energy's Second Line of Defense Program and Megaports Initiative; or

(2) work with the private sector or host governments, when possible, to obtain radiation detection equipment that meets the Department's and the Department of Energy's technical specifications for the equipment.

(h) STAFFING.—The Secretary shall develop a human capital management plan to determine adequate staffing levels in the United States and in foreign seaports including, as appropriate, the remote location of personnel in countries in which foreign seaports are designated under the Container Security Initiative.

(i) ANNUAL DISCUSSIONS.—The Secretary, in coordination with the appropriate Federal officials, shall hold annual discussions with foreign governments of countries in which foreign seaports designated under the Container Security Initiative are located regarding best practices, technical assistance, training needs, and technological developments that will assist in ensuring the efficient and secure movement of international cargo.

(j) LESSER RISK PORT.—The Secretary, acting through the Commissioner, may treat cargo loaded in a foreign seaport designated under the

Container Security Initiative as presenting a lesser risk than similar cargo loaded in a foreign seaport that is not designated under the Container Security Initiative, for the purpose of clearing the cargo into the United States.

(k) PROHIBITION.—

(1) IN GENERAL.—The Secretary shall issue a ''do not load'' order, using existing authorities, to prevent the onload of any cargo loaded at a port designated under the Container Security Initiative that has been identified as high risk, including by the Automated Targeting System, unless the cargo is determined to no longer be high risk through—

(A) a scan of the cargo with nonintrusive imaging equipment and radiation detection equipment;

(B) a search of the cargo; or

(C) additional information received by the Department.

(2) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to interfere with the ability of the Secretary to deny entry of any cargo into the United States.

(l) REPORT.—Not later than 270 days after October 5, 2018, the Secretary, acting through the Commissioner, shall, in consultation with other appropriate government officials and the Commercial Operations Advisory Committee, submit a report to the appropriate congressional committees on the effectiveness of, and the need for any improvements to, the Container Security Initiative. The report shall include—

(1) a description of the technical assistance delivered to, as well as needed at, each designated seaport;

(2) a description of the human capital management plan at each designated seaport;

(3) a summary of the requests made by the United States to foreign governments to conduct physical or nonintrusive inspections of cargo at designated seaports, and whether each request was granted or denied by the foreign government;

(4) an assessment of the effectiveness of screening, scanning, and inspection protocols and technologies utilized at designated seaports and the effect on the flow of commerce at the seaports, as well as any recommendations for improving the effectiveness of screening, scanning, and inspection protocols and technologies utilized at designated seaports;

(5) a description and assessment of the outcome of any security incident involving a foreign seaport designated under the Container Security Initiative;

(6) the rationale for the continuance of each port designated under the Consumer Security Initiative;

(7) a description of the potential for remote targeting to decrease the number of personnel who are deployed at foreign ports under the Consumer Security Initiative; and

(8) a summary and assessment of the aggregate number and extent of trade compliance lapses at each seaport designated under the Container Security Initiative.

(m) COORDINATION OF ASSESSMENTS.—

(1) IN GENERAL.—The Secretary shall, to the extent practicable, conduct the assessments required by the following provisions of law concurrently, or develop a process by which the assessments are coordinated between the Coast Guard and U.S. Customs and Border Protection:

(A) This section.

(B) Section 30523 of this title.

(C) Section 70108 of title 46.

(2) LIMITATION.—Nothing in paragraph (1) shall be construed to affect or diminish the Secretary's authority or discretion—

(A) to conduct an assessment of a foreign port at any time;

(B) to compel the Secretary to conduct an assessment of a foreign port so as to ensure that 2 or more assessments are conducted concurrently; or

(C) to cancel an assessment of a foreign port if the Secretary is unable to conduct 2 or more assessments concurrently.

(3) MULTIPLE ASSESSMENT REPORT.—The Secretary shall provide written notice to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives when the Secretary conducts 2 or more assessments of the same port within a 3-year period.

§ 30506. Avoiding duplication of effort and identifying security gaps

The Secretary shall—

(1) provide the Administrator with updates to vulnerability assessments required under section 70102(b)(3) of title 46 to avoid duplication of effort between the Coast Guard and the Transportation Security Administration; and

(2) identify security gaps between authorities of operating entities in the Department that a threat could exploit to cause a transportation security incident (as defined in section 70101 of title 46).

Subchapter II—Customs–Trade Partnership Against Terrorism

§ 30521. Establishment

(a) IN GENERAL.—The Secretary, acting through the Commissioner, may establish a voluntary government-private-sector program (to be known as the ''Customs-Trade Partnership Against Terrorism'' or ''C–TPAT'') to strengthen and improve the overall security of the international supply chain and United States border security, and to facilitate the movement of secure cargo through the international supply chain, by providing benefits to participants meeting or exceeding the program requirements. Participants in C–TPAT shall include Tier 1 participants, Tier 2 participants, and Tier 3 participants.

(b) REVIEW OF MINIMUM SECURITY REQUIREMENTS.—The Secretary, acting through the Commissioner, shall review the minimum security requirements of C–TPAT at least once every year and update requirements as necessary.

§ 30522. Eligible entities

Importers, customs brokers, forwarders, air, sea, and land carriers, contract logistics providers, and other entities in the international supply chain and intermodal transportation system are eligible to apply to voluntarily enter into partnerships with the Department under C–TPAT.

§ 30523. Minimum requirements

An applicant seeking to participate in C–TPAT shall—

(1) demonstrate a history of moving cargo in the international supply chain;

(2) conduct an assessment of its supply chain based upon security criteria established by the Secretary, acting through the Commissioner, including—

(A) business partner requirements;

(B) container security;

(C) physical security and access controls;

(D) personnel security;

(E) procedural security;

(F) security training and threat awareness; and

(G) information technology security;

(3) implement and maintain security measures and supply chain security practices meeting security criteria established by the Commissioner; and

(4) meet all other requirements established by the Commissioner, in consultation with the Commercial Operations Advisory Committee.

§ 30524. Tier 1 participants

(a) BENEFITS.—The Secretary, acting through the Commissioner, shall offer limited benefits to a Tier 1 participant who has been certified in accordance with the guidelines referred to in subsection (b). Benefits may include a reduction in the score assigned pursuant to the Automated Targeting System of not greater than 20 percent of the high-risk threshold established by the Secretary.

(b) GUIDELINES.—The Secretary, acting through the Commissioner, shall update the guidelines for certifying a C–TPAT participant's security measures and supply chain security practices under this section. The guidelines shall include a background investigation and extensive documentation review.

(c) TIME FRAME.—To the extent practicable, the Secretary, acting through the Commissioner, shall complete the Tier 1 certification process within 90 days of receipt of an application for participation in C–TPAT.

§ 30525. Tier 2 participants

(a) VALIDATION.—The Secretary, acting through the Commissioner, shall validate the security measures and supply chain security practices of a Tier 1 participant in accordance with the guidelines referred to in subsection (c). The validation shall include on-site assessments at appropriate foreign locations utilized by the Tier 1 participant in its supply chain and shall, to the extent practicable, be completed not later than 1 year after certification as a Tier 1 participant.

(b) BENEFITS.—The Secretary, acting through the Commissioner, shall extend benefits to each C–TPAT participant that has been validated as a Tier 2 participant under this section, which may include—

(1) reduced scores in the Automated Targeting System;

(2) reduced examinations of cargo; and

(3) priority searches of cargo.

(c) GUIDELINES.—The Secretary, acting through the Commissioner, shall develop a schedule and update the guidelines for validating a participant's security measures and supply chain security practices under this section.

§ 30526. Tier 3 participants

(a) IN GENERAL.—The Secretary, acting through the Commissioner, shall establish a third tier of C–TPAT participation that offers additional benefits to participants who demonstrate a sustained commitment to maintaining security measures and supply chain security practices that exceed the guidelines established for validation as a Tier 2 participant in C–TPAT under section 30525 of this title.

(b) CRITERIA.—The Secretary, acting through the Commissioner, shall designate criteria for validating a C–TPAT participant as a Tier 3 participant under this section. Criteria may include—

(1) compliance with any additional guidelines established by the Secretary that exceed the guidelines established under section 30525 of this title for validating a C–TPAT participant as a Tier 2 participant, particularly with respect to controls over access to cargo throughout the supply chain;

(2) submission of additional information regarding cargo prior to loading, as determined by the Secretary;

(3) utilization of container security devices, technologies, policies, or practices that meet standards and criteria established by the Secretary; and

(4) compliance with any other cargo requirements established by the Secretary.

(c) BENEFITS.—The Secretary, acting through the Commissioner, in consultation with the Commercial Operations Advisory Committee and the National Maritime Security Advisory Committee, shall extend benefits to each C–TPAT participant that has been validated as a Tier 3 participant under this section, which may include—

(1) the expedited release of a Tier 3 participant's cargo in destination ports within the United States during all threat levels designated by the Secretary;

(2) further reduction in examinations of cargo;

(3) priority for examinations of cargo; and

(4) further reduction in the risk score assigned pursuant to the Automated Targeting System; and

(5) inclusion in joint incident management exercises, as appropriate.

§ 30527. Consequences for lack of compliance

(a) IN GENERAL.—If at any time a C–TPAT participant's security measures and supply chain security practices fail to meet any of the requirements under this subchapter, the Commissioner may deny the participant benefits otherwise available under this subchapter in whole or in part. The Commissioner shall develop procedures that provide appropriate protections to C–TPAT participants before benefits are revoked. The procedures may not limit the ability of the Commissioner to take actions to protect the national security of the United States.

(b) FALSE OR MISLEADING INFORMATION.—If a C–TPAT participant knowingly provides false or misleading information to the Commissioner during the validation process provided for under this subchapter, the Commissioner shall suspend or expel the participant from C–TPAT for an ap-

propriate period of time. The Commissioner, after the completion of the process under subsection (c), may publish in the Federal Register a list of participants who have been suspended or expelled from C–TPAT under this subsection, and may make the list available to C–TPAT participants.

(c) RIGHT OF APPEAL.—

(1) APPEAL OF DENIAL OF BENEFITS.—A C–TPAT participant may appeal a decision of the Commissioner under subsection (a). The appeal shall be filed with the Secretary not later than 90 days after the date of the decision, and the Secretary shall issue a determination not later than 180 days after the appeal is filed.

(2) APPEAL 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.

§ 30528. 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.

§ 30529. 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.

§ 30530. 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 through the Commissioner, shall develop and implement procedures to ensure the protection of confidential data collected, stored, or shared with government agencies or as part of the application, certification, validation, and revalidation processes.

(d) RESOURCE MANAGEMENT STAFFING PLAN.—The Secretary, acting through the Commissioner, shall—

(1) develop a staffing plan to recruit and train staff (including a formalized training program) to meet the objectives identified in the strategic plan of the C–TPAT program; and

(2) provide cross-training in post-incident trade resumption for personnel who administer the C–TPAT program.

(e) REPORT TO CONGRESS.—In connection with the President's annual budget submission for the Department, the Secretary shall report to the appropriate congressional committees on the progress made by the Commissioner to certify, validate, and revalidate C–TPAT participants. The report shall be due on the same date that the President's budget is submitted to the Congress.

Subchapter III—Miscellaneous Provisions

§ 30541. Screening and scanning of cargo containers

(a) ONE HUNDRED PERCENT SCREENING OF CARGO CONTAINERS AND 100 PERCENT SCANNING OF HIGH-RISK CONTAINERS.—

(1) SCREENING OF CARGO CONTAINERS.—The Secretary shall ensure that 100 percent of the cargo containers originating outside the United States and unloaded at a United States seaport undergo a screening to identify high-risk containers

(2) SCANNING OF HIGH-RISK CONTAINERS.—The Secretary shall ensure that 100 percent of the containers that have been identified as high-risk under paragraph (1), or through other means, are scanned or searched before the containers leave a United States seaport facility.

(b) FULL-SCALE IMPLEMENTATION.—

(1) IN GENERAL.—A container that was loaded on a vessel in a foreign port shall not enter the United States (either directly or via a foreign port) unless the container was scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel.

(2) APPLICATION.—Paragraph (1) shall apply with respect to containers loaded on a vessel in a foreign country on or after the earlier of—

(A) July 1, 2012; or

(B) another date established by the Secretary under paragraph (3).

(3) ESTABLISHMENT OF EARLIER DEADLINE.—The Secretary shall establish a date under paragraph (2)(B) pursuant to the lessons learned through the pilot integrated scanning systems established under section 231 of the Security and Accountability For Every Port Act of 2006 (or SAFE Port Act) (Public Law 109–347, 120 Stat. 1915).

(4) EXTENSIONS.—The Secretary may extend the date specified in subparagraph (A) or (B) of paragraph (2) for 2 years, and may renew the extension in additional 2-year increments, for containers loaded in a port or ports, if the Secretary certifies to Congress that at least 2 of the following conditions exist:

(A) Systems to scan containers under paragraph (1) are not available for purchase and installation.

(B) Systems to scan containers under paragraph (1) do not have a sufficiently low false alarm rate for use in the supply chain.

(C) Systems to scan containers under paragraph (1) cannot be purchased, deployed, or operated at ports overseas, including, if applicable, because a port does not have the physical characteristics to install a system.

(D) Systems to scan containers under paragraph (1) cannot be integrated, as necessary, with existing systems.

(E) Use of systems that are available to scan containers under paragraph (1) will significantly impact trade capacity and the flow of cargo.

(F) Systems to scan containers under paragraph (1) do not adequately provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.

(5) EXEMPTION FOR MILITARY CARGO.—Notwithstanding this section, supplies bought by the Secretary of Defense and transported in

compliance with section 2631 of title 10 and military cargo of foreign countries are exempt from the requirements of this section.

(6) REPORT ON EXTENSIONS.—An extension under paragraph (4) for a port takes effect on the expiration of the 60-day period beginning on the date the Secretary provides a report to Congress that—

(A) states what container traffic will be affected by the extension;

(B) provides supporting evidence to support the Secretary's certification of the basis for the extension; and

(C) explains what measures the Secretary is taking to ensure that scanning can be implemented as early as possible at the port or ports that are the subject of the report.

(7) REPORT ON RENEWAL OF EXTENSION.—If an extension under paragraph (4) takes effect, the Secretary shall, after 1 year, submit a report to Congress on whether the Secretary expects to seek to renew the extension.

(8) SCANNING TECHNOLOGY STANDARDS.—In implementing paragraph (1), the Secretary shall—

(A) establish technological and operational standards for systems to scan containers;

(B) ensure that the standards are consistent with the global nuclear detection architecture developed under the Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2135); and

(C) coordinate with other Federal agencies that administer scanning or detection programs at foreign ports.

(9) INTERNATIONAL TRADE AND OTHER OBLIGATIONS.—In carrying out this subsection, the Secretary shall consult with appropriate Federal departments and agencies and private-sector stakeholders, and ensure that actions under this section do not violate international trade obligations, and are consistent with the World Customs Organization framework or other international obligations of the United States.

(c) REPORT.—Not later than 6 months after the submission of a report under section 231(d) of the Security and Accountability For Every Port Act of 2006 (or SAFE Port Act) (Public Law 109–347, 120 Stat. 1916), and every 6 months thereafter, the Secretary shall submit a report to the appropriate congressional committees describing the status of full-scale deployment under subsection (b) and the cost of deploying the system at each foreign port at which the integrated scanning systems are deployed.

(d) SCANNING TECHNOLOGY REVIEW.—

(1) SOLICITATION OF PROPOSALS.—Not later than 1 year after October 5, 2018, and not less frequently than once every 5 years there-

after until the date of full-scale implementation of 100 percent screening of cargo containers and 100 percent scanning of high-risk containers required under this section, the Secretary shall solicit proposals for scanning technologies, consistent with the standards under subsection (b)(8), to improve scanning of cargo at domestic ports. In soliciting the proposals, the Secretary shall establish measures to assess the performance of the proposed scanning technologies, including—

(A) the rate of false positives;

(B) the delays in processing time; and

(C) the impact on the supply chain.

(2) PILOT PROGRAM.—

(A) ESTABLISHMENT.—The Secretary may establish a pilot program to determine the efficacy of a scanning technology referred to in paragraph (1).

(B) APPLICATION PROCESS.—In carrying out the pilot program, the Secretary shall—

(i) solicit applications from domestic ports;

(ii) select up to 4 domestic ports to participate in the pilot program; and

(iii) select ports with unique features and differing levels of trade volume.

(3) REPORT.—Not later than 1 year after initiating a pilot program under paragraph (2)(A), the Secretary shall submit to the Committees on Commerce, Science, and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives a report on the pilot program, including—

(A) an evaluation of the scanning technologies proposed to improve security at domestic ports and to meet the full-scale implementation requirement;

(B) the costs to implement a pilot program;

(C) the benefits of the proposed scanning technologies;

(D) the impact of the pilot program on the supply chain; and

(E) recommendations for implementation of advanced cargo scanning technologies at domestic ports.

(4) SHARING PILOT PROGRAM TESTING RESULTS.—The results of the pilot testing of advanced cargo scanning technologies shall be shared, as appropriate, with government agencies and private stakeholders whose responsibilities encompass the secure transport of cargo.

§ 30542. Provision of assistance, equipment, and training

(a) INSPECTION TECHNOLOGY AND TRAINING.—The Secretary, in coordination with the Secretary of State, the Secretary of Energy, and appropriate representatives of other Federal agencies, may provide technical assistance, equipment, and training to facilitate the implementation of supply chain security measures at ports designated under the Container Security Initiative.

(b) ACQUISITION AND TRAINING.—Unless otherwise prohibited by law, the Secretary may—

(1) lease, lend, provide, or otherwise assist in the deployment of nonintrusive inspection and radiation detection equipment at foreign land and sea ports under terms and conditions the Secretary prescribes, including 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.

§ 30543. 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 appropriate risk information relating to the supply chain from, and to share that information 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

(a) IN GENERAL.—The Secretary of State shall designate a liaison office in the Department of State to assist the Secretary, as appropriate, in negotiating cargo security-related international agreements.

(b) RELATIONSHIP WITH COAST GUARD.—Nothing in this section shall be construed to affect—

(1) the authorities, functions, or capabilities of the Coast Guard to perform its missions; or

(2) the requirement under section 10312 of this title that those authorities, functions, and capabilities be maintained intact.

§ 30702. Homeland Security Science and Technology Advisory Committee

The Under Secretary for Science and Technology shall utilize the Homeland Security Science and Technology Advisory Committee, as appropriate, to provide outside expertise in advancing cargo security technology.

§ 30703. Research, development, test, and evaluation efforts in furtherance of maritime and cargo security

(a) IN GENERAL.—The Secretary shall—

(1) direct research, development, testing, and evaluation efforts in furtherance of maritime and cargo security;

(2) coordinate with public- and private-sector entities to develop and test technologies, and process innovations in furtherance of these objectives; and

(3) evaluate the technologies.

(b) COORDINATION.—The Secretary, in coordination with the Under Secretary for Science and Technology, the Assistant Secretary for Policy, the

Commandant of the Coast Guard, the Assistant Secretary for the Countering Weapons of Mass Destruction Office, the Chief Financial Officer, and the heads of other appropriate offices or entities of the Department, shall ensure that—

(1) research, development, testing, and evaluation efforts funded by the Department in furtherance of maritime and cargo security are coordinated within the Department and with other appropriate Federal agencies to avoid duplication of efforts; and

(2) the results of the efforts are shared throughout the Department and with other Federal, State, and local agencies, as appropriate.

§ 30704. Maritime cybersecurity risk assessment model and information sharing

(a) RISK ASSESSMENT MODEL.—The Secretary, through the Commandant of the Coast Guard and the Under Secretary responsible for overseeing the critical infrastructure protection, cybersecurity, and other related programs of the Department, shall—

(1) not later than 1 year after October 5, 2018, coordinate with the National Maritime Security Advisory Committee, the Area Maritime Security Advisory Committee, and other maritime stakeholders, as necessary, to develop and implement a maritime cybersecurity risk assessment model, consistent with the activities described in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)), to evaluate current and future cybersecurity risks that have the potential to affect the maritime transportation system or that would cause a transportation security incident (as defined in 46 U.S.C. 70101) in ports; and

(2) not less than biennially thereafter, evaluate the effectiveness of the cybersecurity risk assessment model established under paragraph (1).

(b) INFORMATION SHARING.—The Commandant of the Coast Guard and the Under Secretary responsible for overseeing the critical infrastructure protection, cybersecurity, and other related programs of the Department shall—

(1) ensure there is a process for each Area Maritime Security Advisory Committee established under section 70112 of title 46—

(A) to facilitate the sharing of information related to cybersecurity risks that may cause transportation security incidents;

(B) to timely report transportation security incidents to the national level; and

(C) to disseminate the reports across the entire maritime transportation system via the National Cybersecurity and Communications Integration Center; and

(2) issue voluntary guidance for the management of those cybersecurity risks in each Area Maritime Transportation Security Plan and facility security plan required under section 70103 of title 46 approved after the date that the cybersecurity risk assessment model is developed under subsection (a).

§ 30705. Updates of maritime operations coordination plan

(a) IN GENERAL.—Not later than 180 days after October 5, 2018, and biennially thereafter, the Secretary shall—

(1) update the Maritime Operations Security Plan, published by the Department on July 7, 2011, to strengthen coordination, planning, information sharing, and intelligence integration for maritime operations of components and offices of the Department with responsibility for maritime security missions; and

(2) submit each update to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives.

(b) CONTENTS.—Each update shall address the following:

(1) Coordinating the planning, integration of maritime operations, and development of joint maritime domain awareness efforts of any component or office of the Department with responsibility for maritime security missions;

(2) Maintaining effective information sharing and, as appropriate, intelligence integration with Federal, State, and local officials and the private sector regarding threats to maritime security;

(3) Cooperating and coordinating with Federal departments and agencies, and State and local agencies, in the maritime environment in support of maritime security missions.

(4) Highlighting the work completed in the context of other national and Department maritime security strategic guidance and how the work fits with the Maritime Operations Coordination Plan.

§ 30706. Maritime security capabilities assessments

Not later than 180 days after October 5, 2018, and annually thereafter, the Secretary shall submit to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Rep-

resentatives an assessment of the number and type of maritime assets and the number of personnel required to increase the Department's maritime response rate pursuant to section 11115 of this title.

§ 30707. Operational data sharing capability

(a) IN GENERAL.—Not later than June 23, 2024, the Secretary shall, consistent with the ongoing Integrated Multi-Domain Enterprise joint effort by the Department and the Department of Defense, establish a secure centralized capability to allow real-time or near real-time data and information sharing between Customs and Border Protection and the Coast Guard for purposes of maritime boundary domain awareness and enforcement activities along the maritime boundaries of the United States including the maritime boundaries in the northern and southern continental United States and Alaska.

(b) PRIORITY.—In establishing the capability under subsection (a), the Secretary shall prioritize enforcement areas experiencing the highest levels of enforcement activity.

(c) REQUIREMENTS.—The capability established under subsection (a) shall be sufficient for the secure sharing of data, information, and surveillance necessary for operational missions, including data from governmental assets, irrespective of whether an asset located in or around mission operations areas belongs to the Coast Guard, Customs and Border Protection, or any other partner agency.

(d) ELEMENTS.—The Commissioner and the Commandant of the Coast Guard shall jointly—

(1) assess and delineate the types of data and quality of data sharing needed to meet the respective operational missions of Customs and Border Protection and the Coast Guard, including video surveillance, seismic sensors, infrared detection, space-based remote sensing, and any other necessary data or information;

(2) develop appropriate requirements and processes for the credentialing of personnel of Customs and Border Protection and personnel of the Coast Guard to access and use the capability established under subsection(a); and

(3) establish a cost-sharing agreement for the long-term operation and maintenance of the capability and the assets that provide data to the capability.

(e) REPORTS.—Not later than December 23, 2024, the Secretary shall submit to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Transportation and Infrastructure and the Com-

mittee on Homeland Security of the House of Representatives a report on the establishment of the capability under this section.

(f) RULE OF CONSTRUCTION.—Nothing in this section may be construed to authorize the Coast Guard, Customs and Border Protection, or any other partner agency to acquire, share, or transfer personal information relating to an individual in violation of any Federal or State law or regulation.

Subtitle IV—Transportation Security

Chapter 401—General

Sec.
40101. Definitions.

§ 40101. Definitions

(a) DEPARTMENT.—In chapters 403 through 407 of this title, the term ''Department'' means the Department of Homeland Security.

(b) SECRETARY.—In this subtitle, the term ''Secretary'' means the Secretary of Homeland Security.

Chapter 403—Transportation Security Planning, Information Sharing, and Enhancements

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. Third party domestic canines.
40318. Voluntary use of credentialing.
40319. Biometrics expansion.
40320. Roles of the Department and the Department of Transportation.
40321. Integrated and unified operations centers.
40322. Security awareness program.

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.

(b) DESIGNATION.—The Secretary shall select one of the institutions identified in subsection (c) as the lead institution responsible for coordinating the National Transportation Security Center of Excellence.

(c) MEMBER INSTITUTIONS.—

(1) CONSORTIUM.—The institution of higher education selected under subsection (b) shall execute agreements with the other institutions of higher education identified in this subsection and other institutions designated by the Secretary to develop a consortium to assist in accomplishing the goals of the Center.

(2) MEMBERS.—The National Transportation Security Center of Excellence consists of—

(A) Texas Southern University in Houston, Texas;

(B) the National Transit Institute at Rutgers, The State University of New Jersey;

(C) Tougaloo College;

(D) the Connecticut Transportation Institute at the University of Connecticut;

(E) the Homeland Security Management Institute, Long Island University;

(F) the Mack-Blackwell National Rural Transportation Study Center at the University of Arkansas; and

(G) any additional institutions or facilities designated by the Secretary.

(3) CERTAIN INCLUSIONS.—To the extent practicable, the Secretary shall ensure that an appropriate number of additional consortium colleges or universities designated by the Secretary under this subsection are Historically Black Colleges and Universities, Hispanic-serving institutions, and Indian tribally controlled colleges and universities.

§ 40303. Immunity for reports of suspected terrorist activity or suspicious behavior and response

(a) DEFINITIONS.—In this section:

(1) AUTHORIZED OFFICIAL.—The term ''authorized official'' means—

(A) an employee or agent of a passenger transportation system or other person with responsibilities relating to the security of the system;

(B) an officer, employee, or agent of the Department, the Department of Transportation, or the Department of Justice with responsibilities relating to the security of passenger transportation systems; or

(C) a Federal, State, or local law enforcement officer.

(2) COVERED ACTIVITY.—The term ''covered activity'' means a suspicious transaction, activity, or occurrence that involves, or is directed against, a passenger transportation system or vehicle or its passengers indicating that an individual may be engaging, or preparing to engage, in a violation of law relating to—

(A) a threat to a passenger transportation system or passenger safety or security; or

(B) an act of terrorism (as that term is defined in section 3077 of title 18).

(3) PASSENGER TRANSPORTATION.—The term ''passenger transportation'' means—

(A) public transportation, as defined in section 5302 of title 49;

(B) transportation by an over-the-road bus, as defined in section 40701 of this title, and school bus transportation;

(C) intercity rail passenger transportation, as defined in section 24102 of title 49;

(D) the transportation of passengers onboard a passenger vessel, as defined in section 2101 of title 46;

(E) other regularly scheduled waterborne transportation service of passengers by a vessel of at least 20 gross tons; and

(F) air transportation, as defined in section 40102 of title 49, of passengers.

(4) PASSENGER TRANSPORTATION SYSTEM.—The term ''passenger transportation system'' means an entity or entities organized to provide passenger transportation using vehicles, including the infrastructure used to provide the transportation.

(5) VEHICLE.—The term ''vehicle'' has the meaning given the term in section 1992(d)(16) of title 18.

(b) IMMUNITY FOR REPORTS OF SUSPECTED TERRORIST ACTIVITY OR SUSPICIOUS BEHAVIOR.—

(1) IN GENERAL.—A person who, in good faith and based on objectively reasonable suspicion, makes, or causes to be made, a voluntary report of covered activity to an authorized official shall be immune from civil liability under Federal, State, and local law for the report.

(2) FALSE REPORTS.—Paragraph (1) shall not apply to any report that the person knew to be false or was made with reckless disregard for the truth at the time that person made that report.

(c) IMMUNITY FOR RESPONSE.—

(1) IN GENERAL.—An authorized official who observes, or receives a report of, covered activity and takes reasonable action in good faith to respond to the activity has qualified immunity from civil liability for the action, consistent with applicable law in the relevant jurisdiction. An authorized official (as defined by subsection (a)(1)(A)) not entitled to assert the defense of qualified immunity is immune from civil liability under Federal, State, and local law if the authorized official takes reasonable action, in good faith, to respond to the reported activity.

(2) SAVINGS CLAUSE.—Nothing in this subsection affects the ability of an authorized official to assert any defense, privilege, or immunity that would otherwise be available, and this subsection shall not be construed as affecting the defense, privilege, or immunity.

(d) ATTORNEY FEES AND COSTS.—A person or authorized official found to be immune from civil liability under this section is entitled to recover from the plaintiff all reasonable costs and attorney fees.

Subchapter II—Security Enhancements

§ 40311. Definitions

In this subchapter:

(1) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term ''appropriate congressional committee'' means the Committee on Commerce, Science, and Transportation, the Committee on Banking, Housing, and

Urban Affairs, 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.

(2) STATE.—The term ''State'' means a State, the District of Columbia, Puerto Rico, the Northern Mariana Islands, the Virgin Islands, Guam, American Samoa, and any other territory (including a possession) of the United States.

(3) TERRORISM.—The term ''terrorism'' has the meaning given the term in section 10101 of this title.

(4) UNITED STATES.—The term ''United States'' means the States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, the Virgin Islands, Guam, American Samoa, and any other territory (including a possession) of the United States.

§ 40312. Authorization of Visible Intermodal Prevention and Response teams

(a) IN GENERAL.—The Secretary, acting through the Administrator of the Transportation Security Administration, may develop Visible Intermodal Prevention and Response (in this section referred to as ''VIPR'') teams to augment the security of any mode of transportation at any location within the United States. In forming a VIPR team, the Secretary—

(1) may use any asset of the Department, including Federal air marshals, surface transportation security inspectors, canine detection teams, and advanced screening technology;

(2) may determine when a VIPR team shall be deployed, as well as the duration of the deployment;

(3) shall, prior to and during the deployment, consult with local security and law enforcement officials in the jurisdiction where the VIPR team is or will be deployed, to develop and agree upon the appropriate operational protocols and provide relevant information about the mission of the VIPR team, as appropriate;

(4) shall, prior to and during the deployment, consult with all transportation entities directly affected by the deployment of a VIPR team as to specific locations and times in the facilities of the entities at which VIPR teams are to be deployed to maximize the effectiveness of the deployment, as appropriate, including railroad carriers, air carriers, airport owners, over-the-road bus operators and terminal owners and operators, motor carriers, public transportation agencies, owners or operators of highways, port operators and facility owners, vessel owners and operators, and pipeline operators; and

(5) shall require, as appropriate based on risk, in the case of a VIPR team deployed to an airport, that the VIPR team conduct operations—

(A) in the sterile area and any other areas to which only individuals issued security credentials have unrestricted access; and

(B) in nonsterile areas.

(b) PERFORMANCE MEASURES.—Not later than 1 year after October 5, 2018, the Administrator shall develop and implement a system of qualitative performance measures and objectives to assess the roles, activities, and effectiveness of VIPR team operations on an ongoing basis, including a mechanism through which the transportation entities referred to in subsection (a)(4) may submit feedback on VIPR team operations involving their systems or facilities.

(c) PLAN FOR ENSURING INTEROPERABILITY OF COMMUNICATIONS.—Not later than 1 year after October 5, 2018, the Administrator shall develop and implement a plan for ensuring the interoperability of communications among VIPR team participants and between VIPR teams and transportation entities with systems or facilities that are involved in VIPR team operations. The plan shall include an analysis of the costs and resources required to carry out the plan.

(d) NOTIFICATIONS TO CONGRESS.—

(1) NUMBER OF VIPR TEAMS AVAILABLE FOR DEPLOYMENT.—

(A) IN GENERAL.—Not later than 90 days after October 5, 2018, and annually thereafter, the Administrator shall notify the Committees on Commerce, Science, and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives of the number of VIPR teams available for deployment at transportation facilities, including—

(i) the number of VIPR team operations that include explosive detection canine teams; and

(ii) the distribution of VIPR team operations deployed across different modes of transportation.

(B) ANNEX.—The notification under subparagraph (A) may contain a classified annex.

(2) DEPLOYMENT OF PERSONNEL OR RESOURCES.—

(A)IN GENERAL.—If the Administrator deploys any counterterrorism personnel or resource, such as explosive detection sweeps, random bag inspections, or patrols by VIPR teams, to enhance security at a transportation system or transportation facility for a period of not less than 180 consecutive days, the Administrator shall provide sufficient notification to the system or facility operator, as applicable, not less than 14 days prior to terminating the deployment.

(B)EXCEPTION.—This paragraph shall not apply if the Administrator—

(i) determines there is an urgent security need for the personnel or resource described in subparagraph (A); and

(ii) notifies the Committees on Commerce, Science, and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives of the determination under subparagraph (A).

§ 40313. Surface transportation security inspectors

(a) IN GENERAL.—The Secretary, acting through the Administrator of the Transportation Security Administration, may train, employ, and utilize surface transportation security inspectors.

(b) MISSION.—The Secretary shall use surface transportation security inspectors to assist surface transportation carriers, operators, owners, entities, and facilities to enhance their security against terrorist attack and other security threats and to assist the Secretary in enforcing applicable surface transportation security regulations and directives.

(c) AUTHORITIES.—Surface transportation security inspectors employed under this section shall be authorized powers and delegated responsibilities that the Secretary determines appropriate, subject to subsection (e).

(d) REQUIREMENTS.—The Secretary shall require that surface transportation security inspectors have relevant transportation experience and other security and inspection qualifications, as determined appropriate.

(e) LIMITATIONS.—

(1) INSPECTORS.—Surface transportation inspectors shall be prohibited from issuing fines to public transportation agencies (as defined in section 40501 of this title) for violations of the Department's regulations or orders except through the process described in paragraph (2).

(2) CIVIL PENALTIES.—The Secretary shall be prohibited from assessing civil penalties against public transportation agencies (as defined in section 40501 of this title) for violations of the Department's regulations or orders, except in accordance with the following:

(A) In the case of a public transportation agency that is found to be in violation of a regulation or order issued by the Secretary, the Secretary shall seek correction of the violation through a written notice to the public transportation agency and shall give the public transportation agency reasonable opportunity to correct the violation or propose an alternative means of compliance acceptable to the Secretary.

(B) If the public transportation agency does not correct the violation or propose an alternative means of compliance acceptable to the Secretary within a reasonable time period that is specified in the written notice, the Secretary may take any action authorized in sections 11501 through 11505(b), 11506 through 11514, 11516(a) through (h), and 11519 of this title.

(3) LIMITATION ON SECRETARY.—The Secretary shall not initiate civil enforcement actions for violations of administrative and procedural requirements pertaining to the application for, and expenditure of, funds awarded under transportation security grant programs under the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 266).

(f) COORDINATION.—The Secretary shall ensure that the mission of the surface transportation security inspectors is consistent with any relevant risk assessments required by the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 266) or completed by the Department, the modal plans required under section 11514 of this title, the Memorandum of Understanding between the Department and the Department of Transportation on Roles and Responsibilities, dated September 28, 2004, and all subsequent annexes to this Memorandum of Understanding, and other relevant documents setting forth the Department's transportation security strategy, as appropriate.

(g) CONSULTATION.—The Secretary shall periodically consult with the surface transportation entities that are or may be inspected by the surface transportation security inspectors, including, as appropriate, railroad carriers, over-the-road bus operators and terminal owners and operators, motor carriers, public transportation agencies, owners or operators of highways, and pipeline operators on—

(1) the inspectors' duties, responsibilities, authorities, and mission; and

(2) strategies to improve transportation security and to ensure compliance with transportation security requirements.

§ 40314. Surface transportation security technology information sharing

(a) IN GENERAL.—

(1) INFORMATION SHARING.—The Secretary, in consultation with the Secretary of Transportation, shall establish a program to provide appropriate information that the Department has gathered or developed on the performance, use, and testing of technologies that may be used to enhance railroad, public transportation, and surface transportation security to surface transportation entities, including railroad car-

riers, over-the-road bus operators and terminal owners and operators, motor carriers, public transportation agencies, owners or operators of highways, pipeline operators, and State, local, and tribal governments that provide security assistance to the entities.

(2) DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES.—The Secretary shall include in the information provided in paragraph (1) whether the technology is designated as a qualified anti-terrorism technology under subchapter II of chapter 109 of this title, as appropriate.

(b) PURPOSE.—The purpose of the program is to assist eligible grant recipients under this subtitle and others, as appropriate, to purchase and use the best technology and equipment available to meet the security needs of the Nation's surface transportation system.

(c) COORDINATION.—The Secretary shall ensure that the program established under this section makes use of and is consistent with other Department technology testing, information sharing, evaluation, and standards-setting programs, as appropriate.

§ 40315. Transportation Security Administration personnel limitations

Any statutory limitation on the number of employees in the Transportation Security Administration does not apply to employees carrying out this chapter, chapters 401, 405, and 407 of this title, and titles XII through XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 381).

§ 40316. National explosives detection canine team training program

(a) DEFINITION OF EXPLOSIVES DETECTION CANINE TEAM.—In this section, the term ''explosives detection canine team'' means a canine and a canine handler that are trained to detect explosives, radiological materials, chemical, nuclear or biological weapons, or other threats as defined by the Secretary.

(b) IN GENERAL.—

(1) INCREASED CAPACITY.—The Secretary shall—

(A) begin to increase the number of explosives detection canine teams certified by the Transportation Security Administration for the purposes of transportation-related security by up to 200 canine teams annually by the end of 2010; and

(B) encourage State, local, and tribal governments and private owners of high-risk transportation facilities to strengthen security through the use of highly trained explosives detection canine teams.

(2) WAYS TO INCREASE NUMBER OF EXPLOSIVES DETECTION CANINE TEAMS.—The Secretary shall increase the number of explosives detection canine teams by—

(A) using the Transportation Security Administration's National Explosives Detection Canine Team Training Center, including expanding and upgrading existing facilities, procuring and breeding additional canines, and increasing staffing and oversight commensurate with the increased training and deployment capabilities;

(B) partnering with other Federal, State, or local agencies, nonprofit organizations, universities, or the private sector to increase the training capacity for canine detection teams;

(C) procuring explosives detection canines trained by nonprofit organizations, universities, or the private sector, provided they are trained in a manner consistent with the standards and requirements developed under subsection (c) or other criteria developed by the Secretary; or

(D) employing a combination of subparagraphs (A), (B), and (C), as appropriate.

(c) STANDARDS FOR EXPLOSIVES DETECTION CANINE TEAMS.—

(1) IN GENERAL.—Based on the feasibility of meeting the ongoing demand for quality explosives detection canine teams, the Secretary shall establish criteria, including canine training curricula, performance standards, and other requirements approved by the Transportation Security Administration necessary to ensure that explosives detection canine teams trained by nonprofit organizations, universities, and private-sector entities are adequately trained and maintained.

(2) EXPANSION.—In developing and implementing the curricula, performance standards, and other requirements, the Secretary shall—

(A) coordinate with key stakeholders, including international, Federal, State, and local officials, and private-sector and academic entities to develop best practice guidelines for a standardized program, as appropriate;

(B) require that explosives detection canine teams trained by nonprofit organizations, universities, or private-sector entities that are used or made available by the Secretary be trained consistent with specific training criteria developed by the Secretary; and

(C) review the status of the private-sector programs on at least an annual basis to ensure compliance with training curricula, performance standards, and other requirements.

(d) DEPLOYMENT.—The Secretary shall—

(1) use the additional explosives detection canine teams as part of the Department's efforts to strengthen security across the Nation's transportation network, and may use the canine teams on a more limited basis to support other homeland security missions, as determined appropriate by the Secretary;

(2) make available explosives detection canine teams to all modes of transportation, for high-risk areas or to address specific threats, on an as-needed basis and as otherwise determined appropriate by the Secretary;

(3) encourage, but not require, any transportation facility or system to deploy TSA-certified explosives detection canine teams developed under this section; and

(4) consider specific needs and training requirements for explosives detection canine teams to be deployed across the Nation's transportation network, including in venues of multiple modes of transportation, as appropriate.

(e) CANINE PROCUREMENT.—The Secretary, acting through the Administrator of the Transportation Security Administration, shall work to ensure that explosives detection canine teams are procured as efficiently as possible and at the best price, while maintaining the needed level of quality, including, if appropriate, through increased domestic breeding.

(f) REVIEW OF PROGRAM.—

(1) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the Committee on Commerce, Science, and Transportation of the Senate;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Homeland Security of the House of Representatives.

(2) IN GENERAL.—Not later than 90 days after the date on which the Inspector General of the Department receives the report under section 11353(c) of this title, the Inspector General of the Department shall—

(A) review the explosives detection canine team program, including—

(i) the development by the Transportation Security Administration of a deployment strategy for explosives detection canine teams;

(ii) the national explosives detection canine team training program, including canine training, handler training, refresher training, and updates to the training;

(iii) the use of the canine assets during an urgent security need, including the reallocation of the program resources outside the transportation systems sector during an urgent security need; and

(iv) the monitoring and tracking of canine assets; and

(B) submit to the appropriate committees of Congress a report on the review, including any recommendations.

(3) CONSIDERATIONS.—In conducting the review of the deployment strategy under paragraph (2)(A)(i), the Inspector General shall consider whether the Transportation Security Administration's method to analyze the risk to transportation facilities and transportation systems is appropriate.

(g) EXPANSION OF PROGRAM.—

(1) DEFINITION OF EXPLOSIVES DETECTION CANINE TEAMS.—In this subsection, the term ''explosives detection canine teams'' means a canine and a canine handler that are trained to detect explosives and other threats as defined by the Secretary.

(2) ENCOURAGEMENT OF USE OF EXPLOSIVE DETECTION CANINE TEAMS.—The Secretary, where appropriate, shall encourage State, local, and tribal governments and private owners of high-risk transportation facilities to strengthen security through the use of explosives detection canine teams.

(3) INCREASED CAPACITY.—

(A) BEFORE REPORT SUBMITTED.—Before the date on which the Inspector General of the Department submits the report under subsection (f), the Administrator may increase the number of State and local surface and maritime transportation canines by not more than 70 explosives detection canine teams.

(B) BEGINNING ON DATE REPORT SUBMITTED.—Beginning on the date on which the Inspector General of the Department submits the report under subsection (f), the Secretary may increase the State and local surface and maritime transportation canines by up to 200 explosives detection canine teams unless more are identified in the risk-based surface transportation security strategy under section 40723 of this title, consistent with section 40724 of this title or with the President's most recent budget submitted under section 1105 of title 31.

(C) RECOMMENDATIONS.—Before initiating an increase in the number of explosives detection teams under subparagraph (B), the Secretary shall consider any recommendations in the report under subsection (f) on the efficacy and management of the explosives detection canine program.

(4) DEPLOYMENT.—The Secretary shall—

(A) use the additional explosives detection canine teams, as described in paragraph (3)(A), as part of the Department's efforts to strengthen security across the Nation's surface and maritime transportation networks;

(B) make available explosives detection canine teams to all modes of transportation, subject to the requirements under section 40312(a) through (c) of this title, to address specific vulnerabilities or risks, on an as-needed basis and as otherwise determined appropriate by the Secretary; and

(C) consider specific needs and training requirements for explosives detection canine teams to be deployed across the Nation's surface and maritime transportation networks, including in venues of multiple modes of transportation, as the Secretary considers appropriate.

(h) USE OF DIGITAL MONITORING SYSTEM TO FACILITATE IMPROVED REVIEW, DATA ANALYSIS, AND RECORD KEEPING OF CANINE TESTING PERFORMANCE AND PROGRAM ADMINISTRATION.—Not later than 180 days after October 5, 2018, the Administrator shall use, to the extent practicable, a digital monitoring system for all training, testing, and validation or certification of public and private canine assets utilized or funded by the Transportation Security Administration to facilitate improved review, data analysis, and record keeping of canine testing performance and program administration.

§ 40317. Third party domestic canines

(a) DEFINITIONS.—In this section:

(1) BEHAVIORAL STANDARDS.—The term ''behavioral standards'' means standards for the evaluation of explosives detection working canines for certain factors, including canine temperament, work drive, suitability for training, environmental factors used in evaluations, and canine familiarity with natural or man-made surfaces or working conditions relevant to the canine's expected work area.

(2) MEDICAL STANDARDS.—The term ''medical standards'' means standards for the evaluation of explosives detection working canines for certain factors, including canine health, management of heredity health

conditions, breeding practices, genetics, pedigree, and long-term health tracking.

(3) TECHNICAL STANDARDS.—The term ''technical standards'' means standards for the evaluation of explosives detection working canines for certain factors, including canine search techniques, handler-canine communication, detection testing conditions and logistics, and learned explosive odor libraries.

(b) WORKING GROUP.—

(1) ESTABLISHMENT.—Not later than 90 days after October 5, 2018, the Administrator shall establish a working group to determine ways to support decentralized, non-Federal domestic canine breeding capacity to produce high quality explosives detection canines and modernize canine training standards.

(2) COMPOSITION.—The working group established under paragraph (1) shall be comprised of representatives from the following:

(A) The Transportation Security Administration.

(B) The Science and Technology Directorate of the Department.

(C) National domestic canine associations with expertise in breeding and pedigree.

(D) Universities with expertise related to explosives detection canines and canine breeding.

(E) Domestic canine breeders and vendors.

(3) CHAIRPERSONS.—The Administrator shall approve of 2 individuals from among the representatives of the working group specified in paragraph (2) to serve as the Chairpersons of the working group as follows:

(A) One Chairperson shall be from an entity specified in subparagraph (A) or (B) of paragraph (2).

(B) One Chairperson shall be from an entity specified in subparagraph (C), (D), or (E) of paragraph (2).

(4) PROPOSED STANDARDS AND RECOMMENDATIONS.—Not later than 180 days after the date on which the working group is established under paragraph (1), the working group shall submit to the Administrator—

(A) proposed behavioral standards, medical standards, and technical standards for domestic canine breeding and canine training described in paragraph (1); and

(B) recommendations on how the Transportation Security Administration can engage stakeholders to further the development of the domestic non-Federal canine breeding capacity and training described in paragraph (1).

(5) STRATEGY.—Not later than 180 days after the date the recommendations are submitted under paragraph (4), the Administrator shall develop and submit to the appropriate committees of Congress a strategy for working with non-Federal stakeholders to facilitate the expanded domestic canine breeding capacity described in paragraph (1), based on the recommendations.

(6) CONSULTATION.—In developing the strategy under paragraph (5), the Administrator shall consult with the Under Secretary for Science and Technology of the Department, the Commissioner for U.S. Customs and Border Protection, the Director of the United States Secret Service, and the heads of such other Federal departments or agencies as the Administrator considers appropriate to incorporate, to the extent practicable, mission needs across the Department for an expanded non-Federal domestic explosives detection canine breeding capacity that can be leveraged to help meet the Department's operational needs.

(7) TERMINATION.—The working group established under paragraph (1) shall terminate on the date on which the strategy is submitted under paragraph (5), unless the Administrator extends the termination date for the purposes of subsection (c).

(8) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5T.—Chapter 10 of title 5 shall not apply to the working group established under this subsection.

(c) DEVELOPMENT AND ISSUANCE OF STANDARDS AND GUIDANCE.—

(1) IN GENERAL.—Not later than 1 year after October 5, 2018, to enhance the efficiency and efficacy of transportation security by increasing the supply of canine teams for use by the Transportation Security Administration and transportation stakeholders, the Administrator shall develop and issue behavioral standards, medical standards, and technical standards, based on the recommendations of the working group under subsection (b), that a third party explosives detection canine must satisfy to be certified for the screening of individuals and property, including detection of explosive vapors among individuals and articles of property, in public areas of an airport under section 44901 of title 49.

(2) AUGMENTING PUBLIC AREA SECURITY.—

(A) IN GENERAL.—The Administrator shall develop guidance on the coordination of development and deployment of explosives detection canine teams for use by transportation stakeholders to enhance public area security at transportation hubs, including airports.

(B) CONSULTATION.—In developing the guidance under subparagraph (A), the Administrator shall consult with—

(i) the working group established under subsection (b);

(ii) the officials responsible for carrying out subsection (e); and

(iii) such transportation stakeholders, canine providers, law enforcement, privacy groups, and transportation security providers as the Administrator considers relevant.

(3) AGREEMENT TO TEST AND CERTIFY CAPABILITIES OF CANINES.—Subject to paragraphs (4), (5), and (6), not later than 270 days after the issuance of standards under paragraph (1), the Administrator shall, to the extent possible, enter into an agreement with at least 1 third party to test and certify the capabilities of canines in accordance with the standards under paragraph (1).

(4) EXPEDITED DEPLOYMENT.—In entering into an agreement under paragraph (3), the Administrator shall use—

(A) other transaction authority under section 11508 of this title; or

(B) such other authority of the Administrator as the Administrator considers appropriate to expedite the deployment of additional canine teams.

(5) PROCESS.—Before entering into an agreement under paragraph (3), the Administrator shall—

(A) evaluate and verify the third party's ability to effectively evaluate the capabilities of canines;

(B) designate key elements required for appropriate evaluation venues where third parties may conduct testing; and

(C) periodically assess the program at evaluation centers to ensure the proficiency of the canines beyond the initial testing and certification by the third party.

(6) CONSULTATION.—To determine best practices for the use of third parties to test and certify the capabilities of canines, the Administrator shall consult with the following persons before entering into an agreement under paragraph (3):

(A) The Secretary of State.

(B) The Secretary of Defense.

(C) Non-profit organizations that train, certify, and provide the services of canines for various purposes.

(D) Institutions of higher education with research programs related to use of canines for the screening of individuals and prop-

erty, including detection of explosive vapors among individuals and articles of property.

(7) THIRD PARTY EXPLOSIVES DETECTION CANINE PROVIDER LIST.—

(A) DEVELOPMENT AND MAINTENANCE.—Not later than 90 days after the date on which the Administrator enters into an agreement under paragraph (3), the Administrator shall develop and maintain a list of the names of each third party from which the Transportation Security Administration procures explosive detection canines, including for each third party the relevant contractual period of performance.

(B) DISTRIBUTION.—The Administrator shall make the list under subparagraph (A) available to appropriate transportation stakeholders in such form and manner as the Administrator prescribes.

(8) OVERSIGHT.—The Administrator shall establish a process to ensure appropriate oversight of the certification program and compliance with the standards under paragraph (1), including periodic audits of participating third parties.

(9) DEVELOPMENT AND IMPLEMENTATION OF PROCUREMENT PROCESS.—The Administrator shall develop and implement a process for the Transportation Security Administration to procure third party explosives detection canines certified under this section.

(d) DEPLOYMENT TO AUGMENT PUBLIC AREA AT AIRPORT.—

(1) DEFINITIONS.—In this subsection:

(A) APPLICABLE LARGE HUB AIRPORT.—The term ''applicable large hub airport'' means a large hub airport (as defined in section 40102 of title 49) that has less than 100 percent of the allocated passenger screening canine teams staffed by the Transportation Security Administration.

(B) AVIATION STAKEHOLDER.—The term ''aviation stakeholder'' includes an airport, airport operator, and air carrier.

(2) AUTHORIZATION OF AVIATION STAKEHOLDER.—The Administrator shall authorize an aviation stakeholder, under the oversight of and in coordination with the Federal Security Director at an applicable airport, to contract with, procure or purchase, and deploy one or more third party explosives detection canines certified under this section to augment public area security at that airport.

(3) APPLICABLE LARGE HUB AIRPORTS.—

(A) PROVISION OF CERTIFIED CANINE FOR DEPLOYMENT.—Except as provided under subparagraph (B), notwithstanding any

law to the contrary, and subject to the other provisions of this paragraph and paragraph (2), an applicable large hub airport may provide a certified canine described in paragraph (2) on an in-kind basis to the Transportation Security Administration to be deployed as a passenger screening canine at that airport unless the applicable large hub airport consents to the use of that certified canine elsewhere.

(B) EXCEPTION.—The Administrator may, on a case-by-case basis, deploy a certified canine described in paragraph (2) to a transportation facility other than the applicable large hub airport described in subparagraph (A) for not more than 90 days per year if the Administrator—

(i) determines that the deployment is necessary to meet operational or security needs; and

(ii) notifies the applicable large hub airport described in subparagraph (A).

(C) NONEMPLOYABLE CANINES.—A certified canine provided to the Transportation Security Administration under subparagraph (A) that does not complete training for deployment under subparagraph (A) shall be the responsibility of the large hub airport unless the Transportation Security Administration agrees to a different outcome.

(4) HANDLERS.—Not later than 30 days before a canine begins training to become a certified canine under paragraph (3), the airport shall notify the Transportation Security Administration of the training and the Administrator shall assign a Transportation Security Administration canine handler to participate in the training with that canine, as appropriate.

(5) LIMITATION ON REDUCING STAFFING ALLOCATION MODEL.—The Administrator may not reduce the staffing allocation model for an applicable large hub airport based on that airport's provision of a certified canine under this paragraph or paragraph (2).

(e) THIRD PARTY CANINE TEAMS FOR AIR CARGO SECURITY.—

(1) DEFINITIONS.—In this subsection:

(A) AIR CARRIER.—The term ''air carrier'' has the meaning given the term in section 40102 of title 49.

(B) FOREIGN AIR CARRIER.—The term ''foreign air carrier'' has the meaning given the term in section 40102 of title 49.

(C) THIRD PARTY EXPLOSIVES DETECTION CANINE ASSET.—The term ''third party explosives detection canine asset'' means an

explosives detection canine or handler not owned or employed, respectively, by the Transportation Security Administration.

(2) IN GENERAL.—To enhance the screening of air cargo and ensure that third party explosives detection canine assets are leveraged for that purpose, the Administrator shall, not later than 180 days after October 5, 2018—

(A) develop and issue standards for the use of the third party explosives detection canine assets for the primary screening of air cargo;

(B) develop a process to identify qualified non-Federal entities that will certify canine assets that meet the standards established by the Administrator under subparagraph (A);

(C) ensure that entities qualified to certify canine assets shall be independent from entities that will train and provide canines to end users of the canine assets;

(D) establish a system of Transportation Security Administration audits of the process developed under subparagraph (B); and

(E) provide that canines certified for the primary screening of air cargo can be used by air carriers, foreign air carriers, freight forwarders, and shippers.

(3) IMPLEMENTATION.—Beginning on the date that the development of the process under paragraph (2)(B) is complete, the Administrator shall—

(A) facilitate the deployment of the assets that meet the certification standards of the Administration, as determined by the Administrator;

(B) make the standards available to vendors seeking to train and deploy third party explosives detection canine assets; and

(C) ensure that all costs for the training and certification of canines, and for the use of supplied canines, are borne by private industry and not the Federal Government.

§ 40318. Voluntary use of credentialing

(a) DEFINITIONS.—In this section:

(1) APPLICABLE INDIVIDUAL WHO IS SUBJECT TO CREDENTIALING OR A BACKGROUND INVESTIGATION.—The term ''applicable individual who is subject to credentialing or a background investigation'' means only an individual who—

(A) because of employment is regulated by the Transportation Security Administration, Department of Transportation, or Coast Guard and is required to have a background records check to ob-

tain a hazardous materials endorsement on a commercial driver's license issued by a State under section 5103a of title 49; or

(B) is required to have a credential and background records check under section 10862(d)(2) of this title at a facility with activities that are regulated by the Transportation Security Administration, Department of Transportation, or Coast Guard.

(2) VALID TRANSPORTATION SECURITY CARD.—The term ''valid transportation security card'' means a transportation security card that is—

(A) issued under section 70105 of title 46;

(B) not expired;

(C) shows no signs of tampering; and

(D) bears a photograph of the individual representing the card.

(b) SATISFY REQUIREMENT.—An applicable individual who is subject to credentialing or a background investigation may satisfy that requirement by obtaining a valid transportation security card.

(c) ISSUANCE OF CARDS.—The Secretary—

(1) shall expand the transportation security card program, consistent with section 70105 of title 46, to allow an applicable individual who is subject to credentialing or a background investigation to apply for a transportation security card; and

(2) may charge reasonable fees, in accordance with section 10398(a) of this title, for providing the necessary credentialing and background investigation.

(d) VETTING.—The Administrator shall develop and implement a plan to utilize, in addition to any background check required for initial issue, the Federal Bureau of Investigation's Rap Back Service and other vetting tools as appropriate, including the No-Fly and Selectee lists, to get immediate notification of any criminal activity relating to any person with a valid transportation security card.

§ 40319. Biometrics expansion

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Commerce, Science, and Transportation of the Senate;

(2) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(3) the Committee on Homeland Security of the House of Representatives.

(b) CONSULTATION.—The Administrator and the Commissioner of U.S. Customs and Border Protection shall consult with each other on the deployment of biometric technologies.

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to permit the Commissioner of U.S. Customs and Border Protection to facilitate or expand the deployment of biometric technologies, or otherwise collect, use, or retain biometrics, not authorized by a provision of this chapter or a provision of or amendment made by the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458, 118 Stat. 3638) or the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 266).

(d) REPORT REQUIRED.—Not later than 270 days after October 5, 2018, the Secretary shall submit to the appropriate committees of Congress, and to any Member of Congress on request of that Member, a report that includes specific assessments from the Administrator and the Commissioner of U.S. Customs and Border Protection with respect to the following:

(1) The operational and security impact of using biometric technology to identify travelers.

(2) The potential effects on privacy of the expansion of the use of biometric technology under paragraph (1), including methods proposed or implemented to mitigate any risks to privacy identified by the Administrator or the Commissioner related to the active or passive collection of biometric data.

(3) Methods to analyze and address any matching performance errors related to race, gender, or age identified by the Administrator with respect to the use of biometric technology, including the deployment of facial recognition technology.

(4) With respect to the biometric entry-exit program, the following:

(A) Assessments of—

(i) the error rates, including the rates of false positives and false negatives, and accuracy of biometric technologies;

(ii) the effects of biometric technologies, to ensure that the technologies do not unduly burden categories of travelers, such as a certain race, gender, or nationality;

(iii) the extent to which and how biometric technologies could address instances of travelers to the United States overstaying their visas, including

(I) an estimate of how often biometric matches are contained in an existing database;

(II) an estimate of the rate at which travelers using fraudulent credentials identifications are accurately rejected; and

(III) an assessment of what percentage of the detection of fraudulent identifications could have been accomplished using conventional methods;

(iv) the effects on privacy of the use of biometric technologies, including methods to mitigate any risks to privacy identified by the Administrator or the Commissioner of U.S. Customs and Border Protection related to the active or passive collection of biometric data; and

(v) the number of individuals who stay in the United States after the expiration of their visas each year.

(B) A description of—

(i) all audits performed to assess—

(I) error rates in the use of biometric technologies; or

(II) whether the use of biometric technologies and error rates in the use of the technologies disproportionately affect a certain race, gender, or nationality; and

(ii) the results of the audits described in clause (i).

(C) A description of the process by which domestic travelers are able to opt-out of scanning using biometric technologies.

(D) A description of—

(i) what traveler data is collected through scanning using biometric technologies, what agencies have access to the data, and how long the agencies possess the data;

(ii) specific actions that the Department and other relevant Federal departments and agencies take to safeguard the data; and

(iii) a short-term goal for the prompt deletion of the data of individual United States citizens after the data is used to verify traveler identities.

(e) PUBLICATION OF ASSESSMENT.—The Secretary, the Administrator, and the Commissioner shall, if practicable, publish a public version of the assessment required by subsection (d)(2) on the websites of the Transportation Security Administration and of U.S. Customs and Border Protection.

§ 40320. Roles of the Department and the Department of Transportation

(a) IN GENERAL.—The Secretary is the principal Federal official responsible for transportation security.

(b) EQUIVALENT ROLES AND RESPONSIBILITIES.—In carrying out this chapter, chapters 401, 405, and 407 of this title, and titles XII through XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 381), the roles and responsibilities of the Department and the Department of Transportation are the same as their roles and responsibilities under the following:

(1) The Aviation and Transportation Security Act (Public Law 107–71, 115 Stat. 597).

(2) The Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458, 118 Stat. 3638).

(3) The National Infrastructure Protection Plan required by Homeland Security Presidential Directive–7.

(4) The Homeland Security Act of 2002 (Public Law 107–296, 116 Stat. 2135).

(5) The National Response Plan.

(6) Executive Order No. 13416, 71 Fed. Reg. 71033 (Dec. 5, 2006).

(7) The Memorandum of Understanding between the Department of Homeland Security and the Department of Transportation on Roles and Responsibilities, dated September 28, 2004, and any and all subsequent annexes to this Memorandum of Understanding and other relevant agreements between the two Departments.

§ 40321. Integrated and unified operations centers

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Commerce, Science, and Transportation of the Senate;

(2) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(3) the Committee on Homeland Security of the House of Representatives.

(b) FRAMEWORK FOR ESTABLISHING OPERATIONS CENTERS.—Not later than 120 days after October 5, 2018, the Administrator, in consultation with the heads of other appropriate offices or components of the Department, shall make available to public and private stakeholders a framework for establishing an integrated and unified operations center responsible for overseeing daily operations of a transportation facility that promotes coordination for responses to terrorism, serious incidents, and other purposes, as determined appropriate by the Administrator.

(c) REPORT.—Not later than 1 year after October 5, 2018, the Administrator shall brief the appropriate committees of Congress regarding the establishment and activities of integrated and unified operations centers at

transportation facilities at which the Transportation Security Administration has a presence.

§ 40322. Security awareness program

(a) DEFINITION OF FRONTLINE EMPLOYEE.—In this section, the term ''frontline employee'' includes—

(1) an employee of a public transportation agency who is a transit vehicle driver or operator, dispatcher, maintenance or maintenance support employee, security employee, or transit police employee, or any other employee who has direct contact with riders on a regular basis, and any other employee of a public transportation agency who the Administrator determines should receive security training under this section or who is receiving security training under other law;

(2) over-the-road bus drivers, security personnel, dispatchers, maintenance and maintenance support personnel, ticket agents, other terminal employees, and other employees of an over-the-road bus operator or terminal owner or operator who the Administrator determines should receive security training under this section or who are receiving security training under other law; or

(3) security personnel, dispatchers, locomotive engineers, conductors, trainmen, other onboard employees, maintenance and maintenance support personnel, bridge tenders, and other employees of railroad carriers who the Administrator determines should receive security training under this section or who are receiving security training under other law.

(b) ESTABLISHMENT.—The Administrator shall establish a program to promote surface transportation security through the training of surface transportation operators and frontline employees on each of the skills identified in subsection (d).

(c) APPLICATION.—The program established under subsection (b) shall apply to all modes of surface transportation, including public transportation, rail, highway, motor carrier, and pipeline.

(d) TRAINING.—The program established under subsection (b) shall cover, at a minimum, the skills necessary to recognize, assess, and respond to suspicious items or actions that could indicate a threat to transportation.

(e) ASSESSMENT.—

(1) IN GENERAL.—The Administrator shall conduct an assessment of current training programs for surface transportation operators and frontline employees.

(2) CONTENTS.—The assessment shall identify—

(A) whether other training is being provided, either voluntarily or in response to other Federal requirements; and

(B) whether there are any gaps in existing training.

(f) UPDATES.—The Administrator shall ensure the program established under subsection (b) is updated as necessary to address changes in risk and terrorist methods and to close any gaps identified in the assessment under subsection (e).

(g) SUSPICIOUS ACTIVITY REPORTING.—

(1) NATIONAL TELEPHONE NUMBER.—The Secretary shall maintain a national telephone number for an individual to use to report suspicious activity under this section to the Transportation Security Administration.

(2) PROCEDURES.—The Administrator shall establish procedures for the Transportation Security Administration—

(A) to review and follow-up, as necessary, on each report received under paragraph (1); and

(B) to share, as necessary and in accordance with law, the report with appropriate Federal, State, local, and tribal entities.

(3) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

(A) replace or affect in any way the use of 9–1–1 services in an emergency; or

(B) replace or affect in any way the security training program requirements specified in sections 1408, 1517, and 1534 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1137, 1167, 1184).

Chapter 405—Public Transportation Security

Sec.

§ 40501. Definitions

In this chapter:

(1) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term ''appropriate congressional committee'' means the Committee on Banking, Housing, and Urban Affairs 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.

(2) 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.

(3) FRONTLINE EMPLOYEE.—The term ''frontline employee'' means an employee of a public transportation agency who is a transit vehicle driver or operator, dispatcher, maintenance or maintenance support employee, station attendant, customer service employee, security employee, or transit police employee, or any other employee who has direct contact with riders on a regular basis, or any other employee of a public transportation agency that the Secretary determines should receive security training under section 40506 of this title.

(4) PUBLIC TRANSPORTATION AGENCY.—The term ''public transportation agency'' means a publicly owned operator of public transportation eligible to receive Federal assistance under chapter 53 of title 49.

§ 40502. National Strategy for Public Transportation Security

(a) NATIONAL STRATEGY.—Based on the previous and ongoing security assessments conducted by the Department and the Department of Transportation, the Secretary, consistent with and as required by section 11514 of this title, shall develop and implement the modal plan for public transportation, entitled the ''National Strategy for Public Transportation Security'' (in this section referred to as the ''Strategy'').

(b) PURPOSE.—

(1) GUIDELINES.—In developing the Strategy, the Secretary shall establish guidelines for public transportation security that—

(A) minimize security threats to public transportation systems; and

(B) maximize the abilities of public transportation systems to mitigate damage resulting from a terrorist attack or other major incident.

(2) ASSESSMENTS AND CONSULTATIONS.—In developing the Strategy, the Secretary shall—

(A) use established and ongoing public transportation security assessments as the basis of the Strategy; and

(B) consult with all relevant stakeholders, including public transportation agencies, nonprofit labor organizations representing

public transportation employees, emergency responders, public safety officials, and other relevant parties.

(c) CONTENTS.—In the Strategy, the Secretary shall describe prioritized goals, objectives, policies, actions, and schedules to improve the security of public transportation.

(d) RESPONSIBILITIES.—The Secretary shall include in the Strategy a description of the roles, responsibilities, and authorities of Federal, State, and local agencies, tribal governments, and appropriate stakeholders. The Strategy shall also include—

(1) the identification of, and a plan to address, gaps and unnecessary overlaps in the roles, responsibilities, and authorities of Federal agencies; and

(2) a process for coordinating existing or future security strategies and plans for public transportation, including—

(A) the National Infrastructure Protection Plan required by Homeland Security Presidential Directive–7;

(B) Executive Order No. 13416, 71 Fed. Reg. 71033 (Dec. 5, 2006); and

(C) the Memorandum of Understanding between the Department and the Department of Transportation on Roles and Responsibilities dated September 28, 2004, and subsequent annexes and agreements.

(e) ADEQUACY OF EXISTING PLANS AND STRATEGIES.—In developing the Strategy, the Secretary shall use relevant existing risk assessments and strategies developed by the Department or other Federal agencies, including those developed or implemented under section 11514 of this title or Homeland Security Presidential Directive–7.

§ 40503. Security assessments and plans

(a) PUBLIC TRANSPORTATION SECURITY ASSESSMENTS.—

(1) SUBMISSION.—The Administrator of the Federal Transit Administration shall submit all public transportation security assessments and all other relevant information to the Secretary.

(2) SECRETARIAL REVIEW.—Not later than 60 days after receiving the submission under paragraph (1), the Secretary shall review and augment the security assessments received, and conduct additional security assessments as necessary to ensure that at a minimum, all high-risk public transportation agencies, as determined by the Secretary, will have a completed security assessment.

(3) CONTENT.—The Secretary shall ensure that each completed security assessment includes—

(A) identification of critical assets, infrastructure, and systems, and their vulnerabilities; and

(B) identification of any other security weaknesses, including weaknesses in emergency response planning and employee training.

(b) BUS AND RURAL PUBLIC TRANSPORTATION SYSTEMS.—The Secretary shall—

(1) conduct security assessments, based on a representative sample, to determine the specific needs of—

(A) local bus-only public transportation systems; and

(B) public transportation systems that receive funds under section 5311 of title 49; and

(2) make the representative assessments available for use by similarly situated systems.

(c) SECURITY PLANS.—

(1) REQUIREMENT FOR PLAN.—

(A) HIGH RISK AGENCIES.—The Secretary shall require public transportation agencies determined by the Secretary to be at high risk for terrorism to develop a comprehensive security plan. The Secretary shall provide technical assistance and guidance to public transportation agencies in preparing and implementing security plans under this section.

(B) OTHER AGENCIES.—Subject to subparagraph (C), the Secretary may also establish a security program for public transportation agencies not designated high risk by the Secretary, to assist those public transportation agencies that request assistance, including—

(i) guidance to assist agencies in conducting security assessments and preparing and implementing security plans; and

(ii) a process for the Secretary to review and approve assessments and plans, as appropriate.

(C) PLAN NOT REQUIRED.—A public transportation agency that has not been designated high risk may not be required to develop a security plan.

(2) CONTENT.—The Secretary shall ensure that security plans include, as appropriate—

(A) a prioritized list of all items included in the public transportation agency's security assessment that have not yet been addressed;

(B) a detailed list of any additional capital and operational improvements identified by the Department or the public transportation agency and a certification of the public transportation agency's technical capacity for operating and maintaining security equipment that may be identified in the list;

(C) specific procedures to be implemented or used by the public transportation agency in response to a terrorist attack, including evacuation and passenger communication plans and appropriate evacuation and communication measures for the elderly and individuals with disabilities;

(D) a coordinated response plan that establishes procedures for appropriate interaction with State and local law enforcement agencies, emergency responders, and Federal officials in order to coordinate security measures and plans for response in the event of a terrorist attack or other major incident;

(E) a strategy and timeline for conducting training under section 40506 of this title;

(F) plans for providing redundant and other appropriate backup systems necessary to ensure the continued operation of critical elements of the public transportation system in the event of a terrorist attack or other major incident;

(G) plans for providing service capabilities throughout the system in the event of a terrorist attack or other major incident in the city or region that the public transportation system serves;

(H) methods to mitigate damage within a public transportation system in case of an attack on the system, including a plan for communication and coordination with emergency responders; and

(I) other actions or procedures as the Secretary determines are appropriate to address the security of the public transportation system.

(3) REVIEW.—Not later than 6 months after receiving the plans required under this section, the Secretary shall—

(A) review each security plan submitted;

(B) require the public transportation agency to make any amendments needed to ensure that the plan meets the requirements of this section; and

(C) approve any security plan that meets the requirements of this section.

(4) EXEMPTION.—The Secretary may not require a public transportation agency to develop a security plan under paragraph (1) if the agency does not receive a grant under section 40504 of this title.

(5) WAIVER.—The Secretary may waive the exemption provided in paragraph (4) to require a public transportation agency to develop a security plan under paragraph (1) in the absence of grant funds under section 40504 of this title if not less than 3 days after making the determination the Secretary provides the appropriate congressional committees and the public transportation agency written notification detailing the need for the security plan, the reasons grant funding has not been made available, and the reason the agency has been designated high risk.

(d) CONSISTENCY WITH OTHER PLANS.—The Secretary shall ensure that the security plans developed by public transportation agencies under this section are consistent with the security assessments developed by the Department and the National Strategy for Public Transportation Security developed under section 40502 of this title.

(e) UPDATES.—The Secretary annually shall—

(1) update the security assessments referred to in subsection (a);

(2) update the security improvement priorities required under subsection (f); and

(3) require public transportation agencies to update the security plans required under subsection (c), as appropriate.

(f) SECURITY IMPROVEMENT PRIORITIES.—

(1) IN GENERAL.—Each fiscal year, the Secretary, after consultation with management and nonprofit employee labor organizations representing public transportation employees, as appropriate, and with appropriate State and local officials, shall utilize the information developed or received in this section to establish security improvement priorities unique to each individual public transportation agency that has been assessed.

(2) ALLOCATIONS.—The Secretary shall use the security improvement priorities established in paragraph (1) as the basis for allocating risk-based grant funds under section 40504 of this title, unless the Secretary notifies the appropriate congressional committees that the Secretary has determined an adjustment is necessary to respond to an urgent threat or other significant national security factors.

(g) SHARED FACILITIES.—The Secretary shall encourage the development and implementation of coordinated assessments and security plans to the extent a public transportation agency shares facilities (such as tunnels, bridges, stations, or platforms) with another public transportation agency, a freight or passenger railroad carrier, or over-the-road bus operator that is geographically close or otherwise co-located.

(h) NONDISCLOSURE OF INFORMATION.—

(1) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this section shall be construed as authorizing the withholding of any information from Congress.

(2) DISCLOSURE OF INDEPENDENTLY FURNISHED INFORMATION.—Nothing in this section shall be construed as affecting any authority or obligation of a Federal agency to disclose any record or information that the Federal agency obtains from a public transportation agency under any other Federal law.

(i) DETERMINATION.—In response to a petition by a public transportation agency or at the discretion of the Secretary, the Secretary may recognize existing procedures, protocols, and standards of a public transportation agency that the Secretary determines meet all or part of the requirements of this section regarding security assessments or security plans.

§ 40504. Public transportation security improvement grants

(a) SECURITY ASSISTANCE PROGRAM.—

(1) IN GENERAL.—The Secretary shall establish a program for making grants to eligible public transportation agencies for security improvements described in subsection (b).

(2) ELIGIBILITY.—A public transportation agency is eligible for a grant under this section if the Secretary has performed a security assessment or the agency has developed a security plan under section 40503 of this title. Grant funds shall only be awarded for permissible uses under subsection (b) to—

(A) address items included in a security assessment; or

(B) further a security plan.

(b) USES OF FUNDS.—A recipient of a grant under subsection (a) shall use the grant funds for one or more of the following:

(1) CAPITAL USES OF FUNDS, INCLUDING—

(A) tunnel protection systems;

(B) perimeter protection systems, including access control, installation of improved lighting, fencing, and barricades;

(C) redundant critical operations control systems;

(D) chemical, biological, radiological, or explosive detection systems, including the acquisition of canines used for detection;

(E) surveillance equipment;

(F) communications equipment, including mobile service equipment to provide access to wireless Enhanced 911 (E911) emergency services in an underground fixed guideway system;

(G) emergency response equipment, including personal protective equipment;

(H) fire suppression and decontamination equipment;

(I) global positioning or tracking and recovery equipment, and other automated-vehicle-locator-type system equipment;

(J) evacuation improvements;

(K) purchase and placement of bomb-resistant trash cans throughout public transportation facilities, including subway exits, entrances, and tunnels;

(L) capital costs associated with security awareness, security preparedness, and security response training, including training under section 40506 of this title and exercises under section 40505 of this title;

(M) security improvements for public transportation systems, including extensions thereto, in final design or under construction;

(N) security improvements for stations and other public transportation infrastructure, including stations and other public transportation infrastructure owned by State or local governments; and

(O) other capital security improvements determined appropriate by the Secretary.

(2) OPERATING USES OF FUNDS, INCLUDING—

(A) security training and associated backfill, including training under section 40506 of this title and training developed by institutions of higher education and by nonprofit employee labor organizations, for public transportation employees, including frontline employees;

(B) live or simulated exercises under section 40505 of this title;

(C) public awareness campaigns for enhanced public transportation security;

(D) canine patrols for chemical, radiological, biological, or explosives detection;

(E) development of security plans under section 40503 of this title;

(F) overtime reimbursement including reimbursement of State, local, and tribal governments, for costs for enhanced security personnel during significant national and international public events;

(G) operational costs, including reimbursement of State, local, and tribal governments for costs for personnel assigned to full-time or part-time security or counterterrorism duties related to public transportation, provided that this expense totals no more than 10 percent of the total grant funds received by a public transportation agency in any 1 year; and

(H) other operational security costs determined appropriate by the Secretary, excluding routine, ongoing personnel costs, other than those set forth in this section.

(c) SECRETARY'S RESPONSIBILITIES.—In carrying out the responsibilities under subsection (a), the Secretary shall—

(1) determine the requirements for recipients of grants under this section, including application requirements;

(2) under subsection (a)(2), select the recipients of grants based solely on risk; and

(3) under subsection (b), establish the priorities for which grant funds may be used under this section.

(d) DISTRIBUTION OF GRANTS.—The Secretary and the Secretary of Transportation shall determine the most effective and efficient way to distribute grant funds to the recipients of grants determined by the Secretary under subsection (a). Subject to the determination made by the Secretaries, the Secretary may transfer funds to the Secretary of Transportation for the purposes of disbursing funds to the grant recipient.

(e) GRANT SUBJECT TO CERTAIN TERMS AND CONDITIONS.—Except as otherwise specifically provided in this section, a grant provided under this section is subject to the terms and conditions applicable to a grant made under section 5307 of title 49, as in effect on January 1, 2007, and other terms and conditions determined necessary by the Secretary.

(f) LIMITATION ON USES OF FUNDS.—Grants made under this section may not be used to make any State or local government cost-sharing contribution under any other Federal law.

(g) ANNUAL REPORTS.—Each recipient of a grant under this section shall report annually to the Secretary on the use of the grant funds.

(h) GUIDELINES ON USE OF CONTRACTORS AND SUBCONTRACTORS.—Before the distribution of funds to recipients of grants, the Secretary shall issue guidelines to ensure that, to the extent that recipients of grants under this section use contractors or subcontractors, the recipients shall use small, minority, women-owned, or disadvantaged business concerns as contractors or subcontractors to the extent practicable.

(i) COORDINATION WITH STATE HOMELAND SECURITY PLANS.—In establishing security improvement priorities under section 40503 of this title and in awarding grants for capital security improvements and operational security improvements under subsection (b), the Secretary shall act consistently with relevant State homeland security plans.

(j) MULTISTATE TRANSPORTATION SYSTEMS.—In cases in which a public transportation system operates in more than one State, the Secretary shall give appropriate consideration to the risks of the entire system, including

those portions of the States into which the system crosses, in establishing security improvement priorities under section 40503 of this title and in awarding grants for capital security improvements and operational security improvements under subsection (b).

(k) CONGRESSIONAL NOTIFICATION.—Not later than 3 days before the award of any grant under this section, the Secretary shall notify simultaneously the appropriate congressional committees of the intent to award the grant.

(l) RETURN OF MISSPENT GRANT FUNDS.—The Secretary shall establish a process to require the return of any misspent grant funds received under this section determined to have been spent for a purpose other than those specified in the grant award.

(m) AVAILABILITY OF FUNDS.—

(1) IN GENERAL.—Except as provided in paragraph (2), funds provided pursuant to a grant awarded under this section for a use specified in subsection (b) shall remain available for use by a grant recipient for a period of not fewer than 36 months.

(2) CERTAIN SECURITY IMPROVEMENTS.—Funds provided pursuant to a grant awarded under this section for a use specified in subparagraph (M) or (N) of subsection (b)(1) shall remain available for use by a grant recipient for a period of not fewer than 48 months.

§ 40505. Security exercises

(a) IN GENERAL.—The Secretary shall establish a program for conducting security exercises for public transportation agencies for the purpose of assessing and improving the capabilities of entities described in subsection (b) to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism.

(b) COVERED ENTITIES.—Entities to be assessed under the program include—

(1) Federal, State, and local agencies and tribal governments;

(2) public transportation agencies;

(3) governmental and nongovernmental emergency response providers and law enforcement personnel, including transit police; and

(4) any other organization or entity that the Secretary determines appropriate.

(c) REQUIREMENTS.—The Secretary shall ensure that the program—

(1) requires, for public transportation agencies that the Secretary considers appropriate, exercises to be conducted that are—

(A) scaled and tailored to the needs of specific public transportation systems, and include taking into account the needs of the elderly and individuals with disabilities;

(B) live;

(C) coordinated with appropriate officials;

(D) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(E) inclusive, as appropriate, of frontline employees and managers; and

(F) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, and other national initiatives of this type;

(2) provides that exercises described in paragraph (1) will be—

(A) evaluated by the Secretary against clear and consistent performance measures;

(B) assessed by the Secretary to learn best practices, which shall be shared with appropriate Federal, State, local, and tribal officials, governmental and nongovernmental emergency response providers, law enforcement personnel, including railroad and transit police, and appropriate stakeholders; and

(C) followed by remedial action by covered entities in response to lessons learned;

(3) involves individuals in neighborhoods around the infrastructure of a public transportation system; and

(4) assists State, local, and tribal governments and public transportation agencies in designing, implementing, and evaluating exercises that conform to the requirements of paragraph (2).

(d) NATIONAL EXERCISE PROGRAM.—The Secretary shall ensure that the exercise program developed under subsection (a) is a component of the national exercise program established under section 20508 of this title.

(e) FERRY SYSTEM EXEMPTION.—This section does not apply to a ferry system for which drills are required to be conducted under section 70103 of title 46.

§ 40506. Public transportation security training program

(a) APPLICABILITY.—A public transportation agency that receives a grant award under this chapter shall develop and implement a security training program under this section.

(b) IN GENERAL.—The Secretary shall develop and issue detailed final regulations for a public transportation security training program to prepare public transportation employees, including frontline employees, for potential security threats and conditions.

(c) CONSULTATION.—The Secretary shall develop the final regulations under subsection (b) in consultation with—

(1) appropriate law enforcement, fire service, security, and terrorism experts;

(2) representatives of public transportation agencies; and

(3) nonprofit employee labor organizations representing public transportation employees or emergency response personnel.

(d) PROGRAM ELEMENTS.—The final regulations developed under subsection (b) shall require security training programs to include, at a minimum, elements to address the following:

(1) Determination of the seriousness of any occurrence or threat.

(2) Crew and passenger communication and coordination.

(3) Appropriate responses to defend oneself, including using nonlethal defense devices.

(4) Use of personal protective devices and other protective equipment.

(5) Evacuation procedures for passengers and employees, including individuals with disabilities and the elderly.

(6) Training related to behavioral and psychological understanding of, and responses to, terrorist incidents, including the ability to cope with hijacker behavior, and passenger responses.

(7) Live situational training exercises regarding various threat conditions, including tunnel evacuation procedures.

(8) Recognition and reporting of dangerous substances and suspicious packages, persons, and situations.

(9) Understanding of security incident procedures, including procedures for communicating with governmental and nongovernmental emergency response providers and for on-scene interaction with emergency response providers.

(10) Operation and maintenance of security equipment and systems.

(11) Other security training activities that the Secretary considers appropriate.

(e) REQUIRED PROGRAMS.—

(1) DEVELOPMENT AND SUBMISSION TO SECRETARY.—Not later than 90 days after a public transportation agency meets the requirements under subsection (a), the public transportation agency shall develop a security training program in accordance with the regulations developed under subsection (b) and submit the program to the Secretary for approval.

(2) APPROVAL.—Not later than 60 days after receiving a security training program proposal under this subsection, the Secretary shall

approve the program or require the public transportation agency that developed the program to make any revisions to the program that the Secretary determines necessary for the program to meet the requirements of the regulations. A public transportation agency shall respond to the Secretary's comments within 30 days after receiving them.

(3) TRAINING.—Not later than 1 year after the Secretary approves a security training program proposal under this subsection, the public transportation agency that developed the program shall complete the training of all employees covered under the program.

(4) UPDATES OF REGULATIONS AND PROGRAM REVISIONS.—The Secretary shall periodically review and update, as appropriate, the training regulations issued under subsection (b) to reflect new or changing security threats. Each public transportation agency shall revise its training program accordingly and provide additional training as necessary to its workers within a reasonable time after the regulations are updated.

(f) LONG-TERM TRAINING REQUIREMENT.—A public transportation agency required to develop a security training program under this section shall provide routine and ongoing training for employees covered under the program, regardless of whether the public transportation agency receives subsequent grant awards.

(g) NATIONAL TRAINING PROGRAM.—The Secretary shall ensure that the training program developed under subsection (a) is a component of the national training program established under section 20508 of this title.

(h) FERRY EXEMPTION.—This section shall not apply to a ferry system for which training is required to be conducted under section 70103 of title 46.

§ 40507. Security training program for law enforcement agencies

(a) DEFINITIONS.—In this section:

(1) PUBLIC AND PRIVATE SECTOR STAKEHOLDERS.—The term ''public and private sector stakeholders'' has the meaning given the term in section 11516(a).

(2) SURFACE TRANSPORTATION ASSET.—The term ''surface transportation asset'' includes facilities, equipment, or systems used to provide transportation services by—

(A) a public transportation agency (as the term is defined insection 40501 of this title);

(B) a railroad carrier (as the term is defined insection 20102 of title 49);

(C) an owner or operator of—

(i) an entity offering scheduled, fixed-route transportation services by over-the-road bus (as the term is defined insection 40701 of this title); or

(ii) a bus terminal; or

(D) other transportation facilities, equipment, or systems, as determined by the Secretary.

(3) TARGETED VIOLENCE.—The term ''targeted violence'' means an incident of violence in which an attacker selected a particular target to inflict mass injury or death with no discernable political or ideological motivation beyond mass injury or death.

(4) TERRORISM.—The term ''terrorism'' means—

(A) domestic terrorism (as the term is defined insection 2331 of title 18); and

(B) international terrorism (as the term is defined insection 2331 of title 18).

(b) DEVELOPMENT.—The Secretary, in consultation with public and private sector stakeholders, may in a manner consistent with the protection of privacy rights, civil rights, and civil liberties, develop, through the Federal Law Enforcement Training Centers, a training program to enhance the protection, preparedness, and response capabilities of law enforcement agencies with respect to threats of terrorism and other threats, including targeted violence, at a surface transportation asset.

(c) REQUIREMENTS.—The training program described in subsection (b) that the Secretary may develop shall—

(1) be informed by current information regarding tactics used by terrorists and others engaging in targeted violence;

(2) include tactical instruction tailored to the diverse nature of the surface transportation asset operational environment; and

(3) prioritize training officers from law enforcement agencies that are eligible for or receive grants under sections12703 and12704 of this title and officers employed by railroad carriers that operate passenger service, including interstate passenger service.

(d) REPORT.—If the Secretary develops the training program described in subsection (b), not later than 1 year after the date on which the Secretary first implements the program, and annually thereafter during each year the Secretary carries out the program, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the program. Each report shall include, for the year covered by the report—-

(1) a description of the curriculum for the training and any changes to the curriculum;

(2) an identification of any contracts entered into for the development or provision of training under the program;

(3) information on the law enforcement agencies the personnel of which received the training, and for each agency, the number of participants; and

(4) a description of the measures used to ensure the program was carried out to provide for protections of privacy rights, civil rights, and civil liberties.

§ 40508. Public transportation research and development

(a) ESTABLISHMENT OF RESEARCH AND DEVELOPMENT PROGRAM.—The Secretary shall carry out, through the Homeland Security Advanced Research Projects Agency in the Science and Technology Directorate and in consultation with the Transportation Security Administration and the Federal Transit Administration, a research and development program to improve the security of transportation systems.

(b) AWARDING OF GRANTS AND CONTRACTS.—The Secretary shall award grants or contracts to public or private entities to conduct research and demonstrate technologies and methods to reduce and deter terrorist threats or mitigate damages resulting from terrorist attacks against public transportation systems.

(c) USE OF FUNDS.—Grants or contracts awarded under this section—

(1) shall be coordinated with activities of the Homeland Security Advanced Research Projects Agency; and

(2) may be used to—

(A) research chemical, biological, radiological, or explosive detection systems that do not significantly impede passenger access;

(B) research imaging technologies;

(C) conduct product evaluations and testing;

(D) improve security and redundancy for critical communications, electrical power, and computer and train control systems;

(E) develop technologies for securing tunnels, transit bridges, and aerial structures;

(F) research technologies that mitigate damages in the event of a cyberattack; and

(G) research other technologies or methods for reducing or deterring terrorist attacks against public transportation systems, or mitigating damage from attacks.

(d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES.—

(1) CONSULTATION.—In carrying out research and development projects under this section, the Secretary shall consult with the Chief Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department, as appropriate, and in accordance with section 10520 of this title.

(2) PRIVACY IMPACT ASSESSMENTS.—In accordance with sections 10520 and 11705 of this title, the Chief Privacy Officer shall conduct privacy impact assessments and the Officer for Civil Rights and Civil Liberties shall conduct reviews, as appropriate, for research and development initiatives developed under this section.

(e) REPORTING REQUIREMENT.—Each entity that is awarded a grant or contract under this section shall report annually to the Department on the use of grant or contract funds received under this section to ensure that the awards made are expended in accordance with the purposes of this chapter and the priorities developed by the Secretary.

(f) COORDINATION.—The Secretary shall ensure that the research is consistent with the priorities established in the National Strategy for Public Transportation Security and is coordinated, to the extent practicable, with other Federal, State, local, tribal, and private-sector public transportation, railroad, commuter railroad, and over-the-road bus research initiatives to leverage resources and avoid unnecessary duplicative efforts.

(g) RETURN OF MISSPENT GRANT OR CONTRACT FUNDS.—If the Secretary determines that a grantee or contractor used any portion of the grant or contract funds received under this section for a purpose other than the allowable uses specified under subsection (c), the grantee or contractor shall return that amount to the Treasury.

§ 40509. Information sharing

(a) INTELLIGENCE SHARING.—The Secretary shall ensure that the Department of Transportation receives appropriate and timely notification of all credible terrorist threats against public transportation assets in the United States.

(b) INFORMATION SHARING AND ANALYSIS CENTER.—

(1) AUTHORIZATION.—The Secretary shall provide for the reasonable costs of the Information Sharing and Analysis Center for Public Transportation (in this subsection referred to as the ''ISAC'').

(2) PARTICIPATION.—The Secretary—

(A) shall require public transportation agencies that the Secretary determines to be at high risk of terrorist attack to participate in the ISAC;

(B) shall encourage all other public transportation agencies to participate in the ISAC;

(C) shall encourage the participation of nonprofit employee labor organizations representing public transportation employees, as appropriate; and

(D) shall not charge a fee for participating in the ISAC.

§ 40510. Reporting requirements

(a) ANNUAL REPORT TO CONGRESS.—

(1) IN GENERAL.—Not later than March 31 of each year, the Secretary shall submit a report, containing the information described in paragraph (2), to the appropriate congressional committees.

(2) CONTENTS.—The report submitted under paragraph (1) shall include—

(A) a description of the implementation of this chapter;

(B) the amount of funds appropriated to carry out this chapter that have not been expended or obligated;

(C) the National Strategy for Public Transportation Security required under section 40502 of this title;

(D) an estimate of the cost to implement the National Strategy for Public Transportation Security, which shall break out the aggregated total cost of needed capital and operational security improvements for fiscal years 2008 through 2018; and

(E) the state of public transportation security in the United States, which shall include detailing the status of security assessments, the progress being made around the country in developing prioritized lists of security improvements necessary to make public transportation facilities and passengers more secure, the progress being made by agencies in developing security plans and how those plans differ from the security assessments, and a prioritized list of security improvements being compiled by other agencies, as well as a random sample of an equal number of large- and small-scale projects currently underway.

(3) FORMAT.—The Secretary may submit the report in both classified and redacted formats if the Secretary determines that it is appropriate or necessary.

(b) ANNUAL REPORT TO CHIEF EXECUTIVE OFFICERS.—

(1) IN GENERAL.—Not later than March 31 of each year, the Secretary shall submit a report to the chief executive officer of each State with a public transportation agency that has received a grant under this chapter.

(2) CONTENTS.—The report submitted under paragraph (1) shall specify—

(A) the amount of grant funds distributed to each public transportation agency; and

(B) the use of the grant funds.

§ 40511. Public transportation employee protections

(a) IN GENERAL.—A public transportation agency, a contractor or a subcontractor of the agency, or an officer or employee of the agency, shall not discharge, demote, suspend, reprimand, or in any other way discriminate against an employee if the discrimination is due, in whole or in part, to the employee's lawful, good faith act done, or perceived by the employer to have been done or about to be done—

(1) to provide information, directly cause information to be provided, or otherwise directly assist in any investigation regarding any conduct that the employee reasonably believes constitutes a violation of any Federal law, rule, or regulation relating to public transportation safety or security, or fraud, waste, or abuse of Federal grants or other public funds intended to be used for public transportation safety or security, if the information or assistance is provided to, or an investigation stemming from the provided information is conducted by—

(A) a Federal, State, or local regulatory or law enforcement agency (including an office of the Inspector General under chapter 4 of title 5);

(B) a Member of Congress, a committee of Congress, or the Government Accountability Office; or

(C) an individual with supervisory authority over the employee, or another individual who has the authority to investigate, discover, or terminate the misconduct;

(2) to refuse to violate or assist in the violation of any Federal law, rule, or regulation relating to public transportation safety or security;

(3) to file a complaint or directly cause to be brought a proceeding relating to the enforcement of this section or to testify in that proceeding;

(4) to cooperate with a safety or security investigation by the Secretary of Transportation, the Secretary, or the National Transportation Safety Board; or

(5) to furnish information to the Secretary of Transportation, the Secretary, the National Transportation Safety Board, or another Federal, State, or local regulatory or law enforcement agency as to the facts relating to any accident or incident resulting in injury or death to an individual or damage to property occurring in connection with public transportation.

(b) HAZARDOUS SAFETY OR SECURITY CONDITIONS.—

(1) IN GENERAL.—A public transportation agency, a contractor or a subcontractor of the agency, or an officer or employee of the agency, shall not discharge, demote, suspend, reprimand, or in any other way discriminate against an employee for—

(A) reporting a hazardous safety or security condition;

(B) refusing to work when confronted by a hazardous safety or security condition related to the performance of the employee's duties, if the conditions described in paragraph (2) exist; or

(C) refusing to authorize the use of any safety- or security-related equipment, track, or structures, if the employee is responsible for the inspection or repair of the equipment, track, or structures, when the employee believes that the equipment, track, or structures are in a hazardous safety or security condition, if the conditions described in paragraph (2) exist.

(2) PROTECTED REFUSAL.—A refusal is protected under subparagraphs (B) and (C) of paragraph (1) if—

(A) the refusal is made in good faith and no reasonable alternative to the refusal is available to the employee;

(B) a reasonable individual in the circumstances then confronting the employee would conclude that—

(i) the hazardous condition presents an imminent danger of death or serious injury; and

(ii) the urgency of the situation does not allow sufficient time to eliminate the danger without the refusal; and

(C) the employee, where possible, has notified the public transportation agency of the existence of the hazardous condition and the intention not to perform further work, or not to authorize the use of the hazardous equipment, track, or structures, unless the condition is corrected immediately or the equipment, track, or structures are repaired properly or replaced.

(3) LIMITED APPLICABILITY.—Only paragraph (1)(A) applies to security personnel, including transit police, employed or utilized by a public transportation agency to protect riders, equipment, assets, or facilities.

(c) ENFORCEMENT ACTION.—

(1) FILING AND NOTIFICATION.—An individual who believes that he or she has been discharged or otherwise discriminated against by a person in violation of subsection (a) or (b) may, not later than 180 days after the date on which the violation occurs, file (or have a person file on his or her behalf) a complaint with the Secretary of Labor alleging the discharge or discrimination. On receipt of a complaint filed under

this paragraph, the Secretary of Labor shall notify, in writing, the individual named in the complaint and the individual's employer of the filing of the complaint, the allegations contained in the complaint, the substance of evidence supporting the complaint, and the opportunities that will be afforded to the individual under paragraph (2).

(2) INVESTIGATION; PRELIMINARY ORDER.—

(A) IN GENERAL.—Not later than 60 days after the date of receipt of a complaint filed under paragraph (1) and after affording the individual named in the complaint an opportunity to submit to the Secretary of Labor a written response to the complaint and an opportunity to meet with a representative of the Secretary of Labor to present statements from witnesses, the Secretary of Labor shall conduct an investigation and determine whether there is reasonable cause to believe that the complaint has merit and notify, in writing, the complainant and the person alleged to have committed a violation of subsection (a) or (b) of the Secretary of Labor's findings. If the Secretary of Labor concludes that there is a reasonable cause to believe that a violation of subsection (a) or (b) has occurred, the Secretary of Labor shall accompany the Secretary of Labor's findings with a preliminary order providing the relief prescribed by paragraph (3)(B). Not later than 30 days after the date of notification of findings under this paragraph, either the person alleged to have committed the violation or the complainant may file objections to the findings or preliminary order, or both, and request a hearing on the record. The filing of objections shall not operate to stay a reinstatement remedy contained in the preliminary order. Hearings shall be conducted expeditiously. If a hearing is not requested in the 30-day period, the preliminary order shall be deemed a final order that is not subject to judicial review.

(B) REQUIREMENTS.—

(i) REQUIRED SHOWING BY COMPLAINANT.—The Secretary of Labor shall dismiss a complaint filed under this subsection and shall not conduct an investigation otherwise required under subparagraph (A) unless the complainant makes a prima facie showing that any behavior described in subsection (a) or (b) was a contributing factor in the unfavorable personnel action alleged in the complaint.

(ii) SHOWING BY EMPLOYER.—Notwithstanding a finding by the Secretary of Labor that the complainant has made the showing required under clause (i), no investigation otherwise

required under paragraph (A) shall be conducted if the employer demonstrates, by clear and convincing evidence, that the employer would have taken the same unfavorable personnel action in the absence of that behavior.

(iii) CRITERION FOR DETERMINATION BY SECRETARY OF LABOR.—The Secretary of Labor may determine that a violation of subsection (a) or (b) has occurred only if the complainant demonstrates that any behavior described in subsection (a) or (b) was a contributing factor in the unfavorable personnel action alleged in the complaint.

(iv) PROHIBITION.—Relief may not be ordered under paragraph (A) if the employer demonstrates by clear and convincing evidence that the employer would have taken the same unfavorable personnel action in the absence of that behavior.

(3) FINAL ORDER.—

(A) DEADLINE FOR ISSUANCE; SETTLEMENT AGREEMENTS.—Not later than 120 days after the date of conclusion of a hearing under paragraph (2), the Secretary of Labor shall issue a final order providing the relief prescribed by this paragraph or denying the complaint. At any time before issuance of a final order, a proceeding under this subsection may be terminated on the basis of a settlement agreement entered into by the Secretary of Labor, the complainant, and the person alleged to have committed the violation.

(B) REMEDY.—If, in response to a complaint filed under paragraph (1), the Secretary of Labor determines that a violation of subsection (a) or (b) has occurred, the Secretary of Labor shall order the person who committed the violation to—

(i) take affirmative action to abate the violation; and

(ii) provide the remedies described in subsection (d).

(C) ORDER.—If an order is issued under subparagraph (B), the Secretary of Labor, at the request of the complainant, shall assess against the person against whom the order is issued a sum equal to the aggregate amount of all costs and expenses (including attorney and expert witness fees) reasonably incurred, as determined by the Secretary of Labor, by the complainant for, or in connection with, bringing the complaint on which the order was issued.

(D) FRIVOLOUS COMPLAINTS.—If the Secretary of Labor finds that a complaint under paragraph (1) is frivolous or has been brought in bad faith, the Secretary of Labor may award to the prevailing employer reasonable attorney fees not exceeding $1,000.

(4) REVIEW.—

(A) APPEAL TO COURT OF APPEALS.—A person adversely affected or aggrieved by an order issued under paragraph (3) may obtain review of the order in the United States Court of Appeals for the circuit in which the violation, with respect to which the order was issued, allegedly occurred or the circuit in which the complainant resided on the date of the violation. The petition for review must be filed not later than 60 days after the date of the issuance of the final order of the Secretary of Labor. Review shall conform to chapter 7 of title 5. The commencement of proceedings under this subparagraph shall not, unless ordered by the court, operate as a stay of the order.

(B) LIMITATION ON COLLATERAL ATTACK.—An order of the Secretary of Labor with respect to which review could have been obtained under subparagraph (A) shall not be subject to judicial review in any criminal or other civil proceeding.

(5) ENFORCEMENT OF ORDER BY SECRETARY OF LABOR.—When a person fails to comply with an order issued under paragraph (3), the Secretary of Labor may file a civil action in the United States district court for the district in which the violation was found to occur to enforce the order. In actions brought under this paragraph, the district courts have jurisdiction to grant all appropriate relief including injunctive relief and compensatory damages.

(6) ENFORCEMENT OF ORDER BY PARTIES.—

(A) COMMENCEMENT OF ACTION.—An individual on whose behalf an order was issued under paragraph (3) may commence a civil action against the person to whom the order was issued to require compliance with the order. The appropriate United States district court has jurisdiction, without regard to the amount in controversy or the citizenship of the parties, to enforce the order.

(B) ATTORNEY FEES.—The court, in issuing a final order under this paragraph, may award costs of litigation (including reasonable attorney and expert witness fees) to any party when the court determines an award is appropriate.

(7) DE NOVO REVIEW.—With respect to a complaint under paragraph (1), if the Secretary of Labor has not issued a final decision within 210 days after the filing of the complaint and if the delay is not due to the bad faith of the employee, the employee may bring an original action at law or equity for de novo review in the appropriate district court of the United States, which has jurisdiction over the action without regard to the amount in controversy, and which action

shall, at the request of either party to the action, be tried by the court with a jury. The action shall be governed by the same legal burdens of proof specified in paragraph (2)(B) for review by the Secretary of Labor.

(d) REMEDIES.—

(1) IN GENERAL.—An employee prevailing in any action under subsection (c) is entitled to all relief necessary to make the employee whole.

(2) DAMAGES.—Relief in an action under subsection (c) (including an action described in subsection (c)(7)) includes—

(A) reinstatement with the same seniority status that the employee would have had, but for the discrimination;

(B) any backpay, with interest; and

(C) compensatory damages, including compensation for any special damages sustained as a result of the discrimination, including litigation costs, expert witness fees, and reasonable attorney fees.

(3) PUNITIVE DAMAGES.—Relief in an action under subsection (c) may include punitive damages in an amount not to exceed $250,000.

(e) ELECTION OF REMEDIES.—An employee may not seek protection under both this section and another provision of law for the same allegedly unlawful act of the public transportation agency.

(f) NO PREEMPTION.—Nothing in this section preempts or diminishes any other safeguards against discrimination, demotion, discharge, suspension, threats, harassment, reprimand, retaliation, or other manner of discrimination provided by Federal or State law.

(g) RIGHTS RETAINED BY EMPLOYEE.—Nothing in this section shall be construed to diminish the rights, privileges, or remedies of an employee under Federal or State law or under a collective bargaining agreement. The rights and remedies in this section may not be waived by an agreement, policy, form, or condition of employment.

(h) DISCLOSURE OF IDENTITY.—

(1) IN GENERAL.—Except as provided in paragraph (2), or with the written consent of the employee, the Secretary of Transportation or the Secretary may not disclose the name of an employee who has provided information described in subsection (a)(1).

(2) EXCEPTION.—The Secretary of Transportation or the Secretary shall disclose to the Attorney General the name of an employee described in paragraph (1) if the matter is referred to the Attorney General for enforcement. The Secretary making the disclosure shall provide reasonable advance notice to the affected employee if disclosure of that individual's identity or identifying information is to occur.

(i) PROCESS FOR REPORTING SECURITY PROBLEMS TO THE DEPARTMENT.—

(1) ESTABLISHMENT OF PROCESS.—The Secretary shall establish through regulations after an opportunity for notice and comment, and provide information to the public regarding, a process by which a person may submit a report to the Secretary regarding public transportation security problems, deficiencies, or vulnerabilities.

(2) ACKNOWLEDGMENT OF RECEIPT.—If a report submitted under paragraph (1) identifies the person making the report, the Secretary shall respond promptly to the person and acknowledge receipt of the report.

(3) STEPS TO ADDRESS PROBLEM.—The Secretary shall review and consider the information provided in a report submitted under paragraph (1) and shall take appropriate steps to address any problems or deficiencies identified.

§ 40512. Security background checks of covered individuals for public transportation

(a) DEFINITIONS.—In this section:

(1) COVERED INDIVIDUAL.—The term ''covered individual'' means an employee of a public transportation agency or a contractor or subcontractor of a public transportation agency.

(2) SECURITY BACKGROUND CHECK.—The term ''security background check'' means reviewing the following for the purpose of identifying an individual who may pose a threat to transportation security, national security, or of terrorism:

(A) Relevant criminal history databases.

(B) In the case of an alien (as defined in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101)), the relevant databases to determine the status of the alien under the immigration laws of the United States.

(C) Other relevant information or databases, as determined by the Secretary.

(b) GUIDANCE.—

(1) IN GENERAL.—Guidance, recommendations, suggested action items, and other widely disseminated voluntary action items issued by the Secretary to a public transportation agency or a contractor or subcontractor of a public transportation agency relating to performing a security background check of a covered individual shall contain recommendations on the appropriate scope and application of a security background check, including the time period covered, the types of dis-

qualifying offenses, and a redress process for adversely impacted covered individuals consistent with subsections (c) and (d).

(2) ADEQUATE REDRESS PROCESS.—If a public transportation agency or a contractor or subcontractor of a public transportation agency performs a security background check on a covered individual to fulfill guidance issued by the Secretary under paragraph (1), the Secretary shall not consider the guidance fulfilled unless an adequate redress process as described in subsection (d) is provided to covered individuals.

(c) REQUIREMENTS.—If the Secretary issues a rule, regulation, or directive requiring a public transportation agency or contractor or subcontractor of a public transportation agency to perform a security background check of a covered individual, then the Secretary shall prohibit a public transportation agency or contractor or subcontractor of a public transportation agency from making an adverse employment decision, including removal or suspension of the employee, due to the rule, regulation, or directive with respect to a covered individual unless the public transportation agency or contractor or subcontractor of a public transportation agency determines that the covered individual—

(1) has been convicted of, has been found not guilty of by reason of insanity, or is under want, warrant, or indictment for a permanent disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations;

(2) was convicted of or found not guilty by reason of insanity of an interim disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations, within 7 years of the date that the public transportation agency or contractor or subcontractor of the public transportation agency performs the security background check; or

(3) was incarcerated for an interim disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations, and released from incarceration within 5 years of the date that the public transportation agency or contractor or subcontractor of a public transportation agency performs the security background check.

(d) REDRESS PROCESS.—If the Secretary issues a rule, regulation, or directive requiring a public transportation agency or contractor or subcontractor of a public transportation agency to perform a security background check of a covered individual, the Secretary shall—

(1) provide an adequate redress process for a covered individual subjected to an adverse employment decision, including removal or suspension of the employee, due to the rule, regulation, or directive that is consistent with the appeals and waiver process established for appli-

cants for commercial motor vehicle hazardous materials endorsements and transportation workers at ports, as required by section 70105(c) of title 46; and

(2) have the authority to order an appropriate remedy, including reinstatement of the covered individual, should the Secretary determine that a public transportation agency or contractor or subcontractor of a public transportation agency wrongfully made an adverse employment decision regarding a covered individual pursuant to the rule, regulation, or directive.

(e) FALSE STATEMENTS.—A public transportation agency or a contractor or subcontractor of a public transportation agency may not knowingly misrepresent 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. The Secretary shall issue a regulation that prohibits a public transportation agency or a contractor or subcontractor of a public transportation agency 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.

(f) RIGHTS AND RESPONSIBILITIES.—Nothing in this section shall be construed to abridge a public transportation agency's or a contractor or subcontractor of a public transportation agency'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 public transportation agency, or a contractor or subcontractor of a public transportation agency under any other Federal, State, or local laws or collective bargaining agreement.

(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.

(h) STATUTORY CONSTRUCTION.—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.

§ 40513. Limitation on fines and civil penalties

(a) INSPECTORS.—Surface transportation inspectors shall be prohibited from issuing fines to public transportation agencies for violations of the De-

partment's regulations or orders except through the process described in subsection (b)

(b) CIVIL PENALTIES.—The Secretary shall be prohibited from assessing civil penalties against public transportation agencies for violations of the Department's regulations or orders, except in accordance with the following:

(1) VIOLATION OF REGULATION OR ORDER.—In the case of a public transportation agency that is found to be in violation of a regulation or order issued by the Secretary, the Secretary shall seek correction of the violation through a written notice to the public transportation agency and shall give the public transportation agency reasonable opportunity to correct the violation or propose an alternative means of compliance acceptable to the Secretary.

(2) NO CORRECTION OR PROPOSED ALTERNATIVE COMPLIANCE.—If the public transportation agency does not correct the violation or propose an alternative means of compliance acceptable to the Secretary within a reasonable time period that is specified in the written notice, the Secretary may take an action authorized in chapter 115 of this title.

(c) LIMITATION ON SECRETARY.—The Secretary shall not initiate civil enforcement actions for violations of administrative and procedural requirements pertaining to the application for and expenditure of funds awarded under transportation security grant programs under this chapter.

Chapter 407—Surface Transportation Security

Subchapter I—General
Part A—Definitions

§ 40701. Chapter definitions

In this chapter (except part C of this subchapter):

(1) AMTRAK.—The term ''Amtrak'' means the National Railroad Passenger Corporation.

(2) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term ''appropriate congressional committee'' means the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House.

(3) DISADVANTAGED BUSINESS CONCERN.—The term ''disadvantaged business concern'' means a small business that is owned and controlled by socially and economically disadvantaged individuals as defined in part 124, title 13, Code of Federal Regulations.

(4) OVER-THE-ROAD BUS.—The term ''over-the-road bus'' means a bus characterized by an elevated passenger deck located over a baggage compartment.

(5) OVER-THE-ROAD BUS FRONTLINE EMPLOYEE.—The term ''over-the-road bus frontline employee'' means an over-the-road bus driver, security employee, dispatcher, maintenance or maintenance support employee, ticket agent, other terminal employee, or any other employee of an over-the-road bus operator or terminal owner or operator that the Secretary determines should receive security training under this title.

(6) RAILROAD.—The term ''railroad'' has the meaning given the term in section 20102 of title 49.

(7) RAILROAD CARRIER.—The term ''railroad carrier'' has the meaning given the term in section 20102 of title 49.

(8) RAILROAD FRONTLINE EMPLOYEE.—The term ''railroad frontline employee'' means a security employee, dispatcher, locomotive engineer, conductor, trainman, other onboard employee, maintenance or maintenance support employee, bridge tender, or any other employee of a rail-

road carrier that the Secretary determines should receive security training under this chapter.

(9) SECURITY-SENSITIVE MATERIAL.—The term ''security-sensitive material'' means a material, or a group or class of material, in a particular amount and form that the Secretary, in consultation with the Secretary of Transportation, determines, through a rulemaking with opportunity for public comment, poses a significant risk to national security while being transported in commerce due to the potential use of the material in an act of terrorism. In making a designation, the Secretary shall, at a minimum, consider the following:

(A) Class 7 radioactive materials.

(B) Division 1.1, 1.2, or 1.3 explosives.

(C) Materials poisonous or toxic by inhalation, including Division 2.3 gases and Division 6.1 materials.

(D) A select agent or toxin regulated by the Centers for Disease Control and Prevention under part 73 of title 42, Code of Federal Regulations.

(10) STATE.—The term ''State'' means a State, the District of Columbia, Puerto Rico, the Northern Mariana Islands, the Virgin Islands, Guam, American Samoa, and any other territory (including a possession) of the United States.

(11) TERRORISM.—The term ''terrorism'' has the meaning given the term in section 10101 of this title.

(12) TRANSPORTATION.—The term ''transportation'', as used with respect to an over-the-road bus, means the movement of passengers or property by an over-the-road bus—

(A) in the jurisdiction of the United States between a place in a State and a place outside the State (including a place outside the United States); or

(B) in a State that affects trade, traffic, and transportation described in subparagraph (A).

(13) UNITED STATES.—The term ''United States'' means the States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, the Virgin Islands, Guam, American Samoa, and any other territory (including a possession) of the United States.

Part B—Duties of Secretary

§ 40711. Oversight and grant procedures

(a) SECRETARIAL OVERSIGHT.—The Secretary, in coordination with the Secretary of Transportation for grants awarded to Amtrak, shall establish necessary procedures, including monitoring and audits, to ensure that grants made under this chapter are expended in accordance with the pur-

poses of this chapter and the priorities and other criteria developed by the Secretary.

(b) ADDITIONAL AUDITS AND REVIEWS.—The Secretary, and the Secretary of Transportation for grants awarded to Amtrak, may award contracts to undertake additional audits and reviews of the safety, security, procurement, management, and financial compliance of a recipient of amounts under this chapter.

(c) PROCEDURES FOR GRANT AWARD.—The Secretary shall prescribe procedures and schedules for the awarding of grants under this chapter, including application and qualification procedures, and a record of decision on applicant eligibility. The procedures shall include the execution of a grant agreement between the grant recipient and the Secretary and shall be consistent, to the extent practicable, with the grant procedures established under section 70107(i) and (j) of title 46.

(d) ADDITIONAL AUTHORITY.—

(1) ISSUANCE.—The Secretary may issue non-binding letters of intent to recipients of a grant under this chapter, to commit funding from future budget authority of an amount, not more than the Federal Government's share of the project's cost, for a capital improvement project.

(2) SCHEDULE.—The letter of intent under this subsection shall establish a schedule under which the Secretary will reimburse the recipient for the Government's share of the project's costs, as amounts become available, if the recipient, after the Secretary issues that letter, carries out the project without receiving amounts under a grant issued under this chapter.

(3) NOTICE TO SECRETARY.—A recipient that has been issued a letter of intent under this section shall notify the Secretary of the recipient's intent to carry out a project before the project begins.

(4) NOTICE TO CONGRESS.—The Secretary shall transmit to the appropriate congressional committees a written notification at least 5 days before the issuance of a letter of intent under this subsection.

(5) LIMITATIONS.—A letter of intent issued under this subsection is not an obligation of the Federal Government under section 1501 of title 31, and the letter is not deemed to be an administrative commitment for financing. An obligation or administrative commitment may be made only as amounts are provided in authorization and appropriations laws.

(e) RETURN OF MISSPENT GRANT FUNDS.—As part of the grant agreement under subsection (c), the Secretary shall require grant applicants to return misspent grant funds received under this chapter that the Secretary

considers to have been spent for a purpose other than one of those specified in the grant award. The Secretary shall take all necessary actions to recover those funds.

(f) CONGRESSIONAL NOTIFICATION.—Not later than 5 days before the award of a grant is made under this chapter, the Secretary shall notify the appropriate congressional committees of the intent to award the grant.

(g) GUIDELINES.—The Secretary shall ensure, to the extent practicable, that grant recipients under this chapter who use contractors or subcontractors use small, minority, women-owned, or disadvantaged business concerns as contractors or subcontractors when appropriate.

§ 40712. Public awareness and outreach

The Secretary shall implement a national plan for railroad and over-the-road bus security public outreach and awareness. The plan shall—

(1) be designed to increase awareness of measures that the general public, passengers, and employees of railroad carriers and over-the-road bus operators can take to increase the security of the national railroad and over-the-road bus transportation systems; and

(2) provide outreach to railroad carriers and over-the-road bus operators and their employees to improve their awareness of available technologies, ongoing research and development efforts, and available Federal funding sources to improve security.

§ 40713. Nuclear material and explosive detection technology

The Secretary, in coordination with the Director of the National Institute of Standards and Technology and the head of each relevant Federal department or agency researching nuclear material detection systems or explosive detection systems, shall research, facilitate, and, to the extent practicable, deploy next generation technologies, including active neutron interrogation, to detect nuclear material and explosives in transportation systems and transportation facilities.

Part C—Duties of Administrator

§ 40721. Definition of appropriate committees of Congress

In this subchapter, the term ''appropriate committees of Congress'' means—

(1) the Committee on Commerce, Science, and Transportation of the Senate;

(2) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(3) the Committee on Homeland Security of the House of Representatives.

§ 40722. Surface Transportation Security Advisory Committee

(a) ESTABLISHMENT.—The Administrator shall establish in the Transportation Security Administration the Surface Transportation Security Advisory Committee (in this section referred to as the ''Advisory Committee'').

(b) MEMBERSHIP.—

(1) IN GENERAL.—The Advisory Committee shall be composed of—

(A) voting members appointed by the Administrator under paragraph (2); and

(B) nonvoting members, serving in an advisory capacity, who shall be designated by—

(i) the Transportation Security Administration;

(ii) the Department of Transportation;

(iii) the Coast Guard; and

(iv) such other Federal department or agency as the Administrator considers appropriate.

(2) APPOINTMENT.—The Administrator shall appoint voting members from among stakeholders representing each mode of surface transportation, such as passenger rail, freight rail, mass transit, pipelines, highways, over-the-road bus, school bus industry, and trucking, including representatives from—

(A) associations representing those modes of surface transportation;

(B) labor organizations representing those modes of surface transportation;

(C) groups representing the users of those modes of surface transportation, including asset manufacturers, as appropriate;

(D) relevant law enforcement, first responders, and security experts; and

(E) such other groups as the Administrator considers appropriate.

(3) TERM OF OFFICE.—

(A) IN GENERAL.—The term of each voting member of the Advisory Committee shall be 2 years, but a voting member may continue to serve until the Administrator appoints a successor.

(B) REAPPOINTMENT.—A voting member of the Advisory Committee may be reappointed.

(4) CHAIRPERSON.—The Advisory Committee shall select a chairperson from among its voting members.

(5) PROHIBITION ON COMPENSATION.—The members of the Advisory Committee shall not receive compensation from the Government by reason of their service on the Advisory Committee.

(6) REMOVAL.—The Administrator may review the participation of a member of the Advisory Committee and remove the member for cause at any time.

(7) VOTING MEMBER ACCESS TO CLASSIFIED AND SENSITIVE SECURITY INFORMATION.—

(A) DETERMINATIONS.—Not later than 60 days after the date on which a voting member is appointed to the Advisory Committee and before that voting member may be granted any access to classified information or sensitive security information, the Administrator shall determine if the voting member should be restricted from reviewing, discussing, or possessing classified information or sensitive security information.

(B) ACCESS.—

(i) SENSITIVE SECURITY INFORMATION.—If a voting member is not restricted from reviewing, discussing, or possessing sensitive security information under subparagraph (A) and voluntarily signs a nondisclosure agreement, the voting member may be granted access to sensitive security information that is relevant to the voting member's service on the Advisory Committee.

(ii) CLASSIFIED INFORMATION.—Access to classified materials shall be managed in accordance with Executive Order 13526 of December 29, 2009 (75 Fed. Reg. 707), or a subsequent corresponding Executive order.

(C) PROTECTIONS.—

(i) SENSITIVE SECURITY INFORMATION.—Voting members shall protect sensitive security information in accordance with part 1520 of title 49, Code of Federal Regulations.

(ii) CLASSIFIED INFORMATION.—Voting members shall protect classified information in accordance with the applicable requirements for the particular level of classification.

(D) REMOVAL BECAUSE OF RESTRICTED ACCESS.—The Administrator may remove a member of the Advisory Committee whom the Administrator determines should be restricted from reviewing, discussing, or possessing classified information or sensitive security information under subparagraph (A).

(c) Duties.—The Advisory Committee—

(1) may advise, consult with, report to, and make recommendations to the Administrator on surface transportation security matters, including the development, refinement, and implementation of policies, programs, initiatives, rulemakings, and security directives pertaining to surface transportation security; and

(2) shall consider risk-based security approaches in the performance of its duties.

(d) MEETINGS.—

(1) IN GENERAL.—

(A) FREQUENCY.—The Administrator shall require the Advisory Committee to meet at least semiannually in person or through web conferencing and may convene additional meetings as necessary.

(B) PUBLIC MEETINGS.—At least 1 of the meetings of the Advisory Committee each year shall be—

(i) announced in the Federal Register;

(ii) announced on a public website; and

(iii) open to the public.

(C) ATTENDANCE.—The Advisory Committee shall maintain a record of the individuals present at each meeting.

(D) MINUTES.—

(i) IN GENERAL.—Unless otherwise prohibited by other Federal law, minutes of the meetings shall be published on the public website under subsection (g)(5).

(ii) PROTECTION OF CLASSIFIED AND SENSITIVE INFORMATION.—The Advisory Committee may redact or summarize, as necessary, minutes of the meetings to protect classified or other sensitive information in accordance with law.

(2) JOINT COMMITTEE MEETINGS.—The Advisory Committee may meet with 1 or more of the following advisory committees to discuss multimodal security issues and other security-related issues of common concern:

(A) The Aviation Security Advisory Committee established under section 40963 of title 49.

(B) The Maritime Security Advisory Committee established under section 70112 of title 46.

(C) The Railroad Safety Advisory Committee established by the Federal Railroad Administration.

(e) SUBJECT MATTER EXPERTS.—The Advisory Committee may request the assistance of subject matter experts with expertise related to the jurisdiction of the Advisory Committee.

(f) REPORTS.—

(1) PERIODIC REPORTS.—The Advisory Committee shall periodically submit reports to the Administrator on matters requested by the Administrator or by a majority of the members of the Advisory Committee.

(2) ANNUAL REPORTS.—

(A) SUBMISSION.—The Advisory Committee shall submit to the Administrator and the appropriate congressional committees an annual report that provides information on the activities, findings, and recommendations of the Advisory Committee during the preceding year.

(B) PUBLICATION.—Not later than 6 months after the date on which the Administrator receives an annual report under subparagraph (A), the Administrator shall publish a public version of the report, in accordance with section 552a(b) of title 5.

(g) ADMINISTRATOR'S RESPONSE.—

(1) CONSIDERATION OF INFORMATION, ADVICE, AND RECOMMENDATIONS.—The Administrator shall consider the information, advice, and recommendations of the Advisory Committee in formulating policies, programs, initiatives, rulemakings, and security directives pertaining to surface transportation security.

(2) FEEDBACK.—Not later than 90 days after the date on which the Administrator receives a recommendation from the Advisory Committee under subsection (d)(2), the Administrator shall submit to the Advisory Committee written feedback on the recommendation, including—

(A) if the Administrator agrees with the recommendation, a plan describing the actions that the Administrator has taken, will take, or recommends that the head of another Federal department or agency take to implement the recommendation; or

(B) if the Administrator disagrees with the recommendation, a justification for that determination.

(3) NOTIFICATION AND BRIEFING.—Not later than 30 days after the date on which the Administrator submits feedback under paragraph (2), the Administrator shall-

(A) notify the appropriate congressional committees of the feedback, including the determination under subparagraph (A) or (B) of paragraph (2), as applicable; and

(B) provide the appropriate congressional committees with a briefing upon request.

(4) UPDATES.—Not later than 90 days after the date on which the Administrator receives a recommendation from the Advisory Committee under subsection (f)(2) that the Administrator agrees with, and quar-

terly thereafter until the recommendation is fully implemented, the Administrator shall submit a report to the appropriate congressional committees or post on the public website under paragraph (5) an update on the status of the recommendation.

(5) WEBSITE.—The Administrator shall maintain a public website that—

(A) lists the members of the Advisory Committee; and

(B) provides the contact information for the Advisory Committee.

(h) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of title 5 shall not apply to the Advisory Committee or a subcommittee established under this section.

§ 40723. Surface transportation security assessment and implementation of risk-based strategy

(a) SECURITY ASSESSMENT.—

(1) IN GENERAL.—Not later than 1 year after October 5, 2018, the Administrator shall complete an assessment of the vulnerabilities of and risks to surface transportation systems.

(2) CONSIDERATIONS.—In conducting the security assessment under paragraph (1), the Administrator shall, at a minimum—

(A) complete appropriate intelligence;

(B) consider security breaches and attacks at domestic and international surface transportation facilities;

(C) consider the vulnerabilities and risks associated with specific modes of surface transportation;

(D) evaluate the vetting and security training of—

(i) employees in surface transportation; and

(ii) other individuals with access to sensitive or secure areas of surface transportation networks; and

(E) consider input from—

(i) representatives of different modes of surface transportation;

(ii) representatives of critical infrastructure entities;

(iii) the Transportation Systems Sector Coordinating Council; and

(iv) the heads of other relevant Federal departments or agencies.

(b) RISK-BASED SURFACE TRANSPORTATION SECURITY STRATEGY.—

(1) IN GENERAL.—Not later the 180 days after the date on which the security assessment under subsection (a) is complete, the Administrator shall use the results of the assessment—

(A) to develop and implement a cross-cutting, risk-based surface transportation security strategy that includes—

(i) all surface transportation modes;

(ii) a mitigating strategy that aligns with each vulnerability and risk identified in subsection (a);

(iii) a planning process to inform resource allocation;

(iv) priorities, milestones, and performance metrics to measure the effectiveness of the risk-based surface transportation security strategy; and

(v) processes for sharing relevant and timely intelligence threat information with appropriate stakeholders;

(B) to develop a management oversight strategy that—

(i) identifies the parties responsible for the implementation, management, and oversight of the risk-based surface transportation security strategy; and

(ii) includes a plan for implementing the risk-based surface transportation security strategy; and

(C) to modify the risk-based budget and resource allocations, in accordance with section 40724(c) of this title, for the Transportation Security Administration.

(2) COORDINATED APPROACH.—In developing and implementing the risk-based surface transportation security strategy under paragraph (1), the Administrator shall coordinate with the heads of other relevant Federal departments or agencies, and stakeholders, as appropriate—

(A) to evaluate existing surface transportation security programs, policies, and initiatives, including the explosives detection canine teams, for consistency with the risk-based security strategy and, to the extent practicable, avoid unnecessary duplication of effort;

(B) to determine the extent to which stakeholder security programs, policies, and initiatives address the vulnerabilities of, and risks to, surface transportation systems identified in subsection (a); and

(C) subject to subparagraph (B), to mitigate each vulnerability and risk to surface transportation systems identified in subsection (a).

(c) REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date the security assessment under subsection (a) is complete, the Administrator shall submit to the appropriate committees of Congress and the Inspector General of the Department a report that—

(A) describes the process used to complete the security assessment;

(B) describes the process used to develop the risk-based security strategy;

(C) describes the risk-based security strategy;

(D) includes the management oversight strategy;

(E) includes—

(i) the findings of the security assessment;

(ii) a description of the actions recommended or taken by the Administrator to mitigate the vulnerabilities and risks identified in subsection (a)(2), including interagency coordination;

(iii) recommendations for improving the coordinated approach to mitigating vulnerabilities and risks to surface transportation systems; and

(iv) recommended changes to the National Infrastructure Protection Plan, the modal annexes to the National Infrastructure Protection Plan, or relevant surface transportation security programs, policies, or initiatives; and

(F) may contain a classified annex.

(2) PROTECTIONS AGAINST DISCLOSURE.—In preparing the report, the Administrator shall take appropriate actions to safeguard information described by section 552(b) of title 5 or protected from disclosure by any other law of the United States.

(d) UPDATES.—Not less frequently than semiannually, the Administrator shall report to, or brief, the appropriate committees of Congress on the vulnerabilities of, and risks to, surface transportation systems and how those vulnerabilities and risks affect the risk-based security strategy.

§ 40724. Risk-based budgeting and resource allocation

(a) REPORT.—In conjunction with the submission of the Department's annual budget request to the Office of Management and Budget, the Administrator shall submit to the appropriate committees of Congress a report that describes a risk-based budget and resource allocation plan for surface transportation sectors, within and across modes, that—

(1) reflects the risk-based surface transportation security strategy under section 40723(b) of this title; and

(2) is organized by appropriations account, program, project, and initiative.

(b) BUDGET TRANSPARENCY.—In submitting the annual budget of the United States Government under section 1105 of title 31, the President

shall clearly distinguish the resources requested for surface transportation security from the resources requested for aviation security.

(c) RESOURCE REALLOCATION.—

(1) IN GENERAL.—Not less than 15 days after the date on which the Transportation Security Administration allocates resources or personnel, including personnel sharing, detailing, or assignment, or the use of facilities, technology systems, or vetting resources, for a nontransportation security purpose or National Special Security Event (as defined in section 12701 of this title), the Secretary shall provide the notification described in paragraph (2) to the appropriate committees of Congress.

(2) NOTIFICATION.—A notification described in this paragraph shall include—

(A) the reason for, and a justification of, the resource or personnel allocation;

(B) the expected end date of the resource or personnel allocation; and

(C) the proposed cost to the Transportation Security Administration of the resource or personnel allocation.

(d) FIVE-YEAR CAPITAL INVESTMENT PLAN.—Not later than 180 days after October 5, 2018, the Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives a 5-year capital investment plan, consistent with the 5-year technology investment plan under section 11542 of this title.

§ 40725. Transparency

(a) REGULATIONS.—

(1) PUBLICATION OF STATUS OF REGULATIONS.—Not later than 180 days after October 5, 2018, and every 180 days thereafter, the Administrator shall publish on a public website information regarding the status of each regulation relating to surface transportation security that is directed by law to be issued and that has not been issued if not less than 2 years have passed since the date of enactment of the law.

(2) CONTENTS.—Information published under paragraph (1) shall include—

(A) an updated rulemaking schedule for the outstanding regulation;

(B) current staff allocations;

(C) data collection or research relating to the development of the rulemaking;

(D) current efforts, if any, with security experts, advisory committees, and other stakeholders; and

(E) other relevant details associated with the development of the rulemaking that impact the progress of the rulemaking.

(b) INSPECTOR GENERAL REVIEW.—Not later than 180 days after October 5, 2016, and every 2 years thereafter until all the requirements under this chapter, chapters 401 through 405 of this title, titles XIII, XIV, and XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 389, and the TSA Modernization Act (Public Law 115–254, div. K, 132 Stat. 3542) have been fully implemented, the Inspector General of the Department shall submit to the appropriate committees of Congress a report that—

(1) identifies the requirements under this chapter, chapters 401 through 405 of this title, titles XIII, XIV, and XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 389, and the TSA Modernization Act (Public Law 115–254, div. K, 132 Stat. 3542) that have not been fully implemented;

(2) describes what, if any, additional action is necessary; and

(3) includes recommendations regarding whether any of the requirements under this chapter, chapters 401 through 405 of this title, titles XIII, XIV, and XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 389, and the TSA Modernization Act (Public Law 115–254, div. K, 132 Stat. 3542) should be amended or repealed.

Subchapter II—Railroad Security

§ 40741. Railroad transportation security risk assessment and National Strategy

(a) RISK ASSESSMENT.—The Secretary shall establish a Federal task force, including the Transportation Security Administration and other agencies in the Department, the Department of Transportation, and other appropriate Federal agencies, to complete a nationwide risk assessment of a terrorist attack on railroad carriers. The assessment shall include—

(1) a methodology for conducting the risk assessment, including timelines, that addresses how the Department will work with the entities described in subsection (c) and make use of existing Federal expertise in the Department, the Department of Transportation, and other appropriate agencies;

(2) identification and evaluation of critical assets and infrastructure, including tunnels used by railroad carriers in high-threat urban areas;

(3) identification of risks to those assets and infrastructure;

(4) identification of risks that are specific to the transportation of hazardous materials via railroad;

(5) identification of risks to passenger and cargo security, transportation infrastructure protection systems, operations, communications systems, and any other area identified by the assessment;

(6) an assessment of employee training and emergency response planning;

(7) an assessment of public and private operational recovery plans, taking into account the plans for the maritime sector required under section 70103 of title 46, to expedite, to the maximum extent practicable, the return of an adversely affected railroad transportation system or facility to its normal performance level after a major terrorist attack or other security event on that system or facility; and

(8) an account of actions taken or planned by both public and private entities to address identified railroad security issues and an assessment of the effective integration of the actions.

(b) NATIONAL STRATEGY.—

(1) REQUIREMENT.—Based upon the assessment conducted under subsection (a), the Secretary, consistent with and as required by section 11514 of this title, shall develop and implement the modal plan for railroad transportation, entitled the ''National Strategy for Railroad Transportation Security''.

(2) CONTENTS.—The modal plan shall include prioritized goals, actions, objectives, policies, mechanisms, and schedules for, at a minimum—

(A) improving the security of railroad tunnels, railroad bridges, railroad switching and car storage areas, other railroad infrastructure and facilities, information systems, and other areas identified by the Secretary as posing significant railroad-related risks to public safety and the movement of interstate commerce, taking into account the impact that a proposed security measure might have on the provision of railroad service or on operations served or otherwise affected by railroad service;

(B) deploying equipment and personnel to detect security threats, including those posed by explosives and hazardous chemical, biological, and radioactive substances, and appropriate countermeasures;

(C) consistent with section 40746 of this title, training railroad employees in terrorism prevention, preparedness, passenger evacuation, and response activities;

(D) conducting public outreach campaigns for railroads regarding security, including educational initiatives designed to inform the public on how to prevent, prepare for, respond to, and recover from a terrorist attack on railroad transportation;

(E) providing additional railroad security support for railroads at high or severe threat levels of alert;

(F) ensuring, in coordination with freight and intercity and commuter passenger railroads, the continued movement of freight and passengers in the event of an attack affecting the railroad system, including the possibility of rerouting traffic due to the loss of critical infrastructure, such as a bridge, tunnel, yard, or station;

(G) coordinating existing and planned railroad security initiatives undertaken by the public and private sectors;

(H) assessing—

(i) the usefulness of covert testing of railroad security systems;

(ii) the ability to integrate security into infrastructure design; and

(iii) the implementation of random searches of passengers and baggage; and

(I) identifying the immediate and long-term costs of measures that may be required to address those risks and public- and private-sector sources to fund the measures.

(3) RESPONSIBILITIES.—The Secretary shall include in the modal plan a description of the roles, responsibilities, and authorities of Federal, State, and local agencies, government-sponsored entities, tribal governments, and appropriate stakeholders described in subsection (c). The plan also shall include—

(A) the identification of, and a plan to address, gaps and unnecessary overlaps in the roles, responsibilities, and authorities described in this paragraph;

(B) a methodology for how the Department will work with the entities described in subsection (c), and make use of existing Federal expertise within the Department, the Department of Transportation, and other appropriate agencies;

(C) a process for facilitating security clearances for the purpose of intelligence and information sharing with the entities described in subsection (c), as appropriate;

(D) a strategy and timeline, coordinated with the research and development program established under section 40747 of this title, for the Department, the Department of Transportation, other ap-

propriate Federal agencies, and private entities to research and develop new technologies for securing railroad systems; and

(E) a process for coordinating existing or future security strategies and plans for railroad transportation, including—

(i) the National Infrastructure Protection Plan required by Homeland Security Presidential Directive–7;

(ii) Executive Order No. 13416, 71 Fed. Reg. 71033 (Dec. 5, 2006); and

(iii) the Memorandum of Understanding between the Department and the Department of Transportation on Roles and Responsibilities, dated September 28, 2004, subsequent annexes to this Memorandum of Understanding, and other relevant agreements between the two Departments.

(c) CONSULTATION WITH STAKEHOLDERS.—In developing the National Strategy required under this section, the Secretary shall consult with railroad management, nonprofit employee organizations representing railroad employees, owners or lessors of railroad cars used to transport hazardous materials, emergency responders, offerors of security-sensitive materials, public safety officials, and other relevant parties.

(d) ADEQUACY OF EXISTING PLANS AND STRATEGIES.—In developing the risk assessment and National Strategy required under this section, the Secretary shall utilize relevant existing plans, strategies, and risk assessments developed by the Department or other Federal agencies, including those developed or implemented under section 11514 of this title, or Homeland Security Presidential Directive–7, and, as appropriate, assessments developed by other public and private stakeholders.

(e) ANNUAL UPDATES.—Consistent with the requirements of section 11514 of this title, the Secretary shall update the assessment and National Strategy each year and transmit a report, which may be submitted in both classified and redacted formats, to the appropriate congressional committees, containing the updated assessment and recommendations.

§ 40742. Railroad carrier assessments and plans

(a) IN GENERAL.—The Secretary shall issue regulations that—

(1) require each railroad carrier assigned to a high-risk tier under this section to—

(A) conduct a vulnerability assessment under subsections (c) and (d); and

(B) prepare, submit to the Secretary for approval, and implement a security plan under this section that addresses security performance requirements; and

(2) establish standards and guidelines, based on and consistent with the risk assessment and National Strategy for Railroad Transportation Security developed under section 40741 of this title, for developing and implementing the vulnerability assessments and security plans for railroad carriers assigned to high-risk tiers.

(b) NON-HIGH-RISK PROGRAMS.—The Secretary may establish a security program for railroad carriers not assigned to a high-risk tier, including—

(1) guidance for the carriers in conducting vulnerability assessments and preparing and implementing security plans, as determined appropriate by the Secretary; and

(2) a process to review and approve the assessments and plans, as appropriate.

(c) SUBMISSION OF ASSESSMENTS AND SECURITY PLANS.—The vulnerability assessments and security plans required by the regulations for railroad carriers assigned to a high-risk tier shall be completed and submitted to the Secretary for review and approval.

(d) VULNERABILITY ASSESSMENTS.—

(1) REQUIREMENTS.—The Secretary shall provide technical assistance and guidance to railroad carriers in conducting vulnerability assessments under this section and shall require that each vulnerability assessment of a railroad carrier assigned to a high-risk tier under this section, include, as applicable—

(A) identification and evaluation of critical railroad carrier assets and infrastructure, including platforms, stations, intermodal terminals, tunnels, bridges, switching and storage areas, and information systems as appropriate;

(B) identification of the vulnerabilities of those assets and infrastructure;

(C) identification of strengths and weaknesses in—

(i) physical security;

(ii) passenger and cargo security, including the security of security-sensitive materials being transported by railroad or stored on railroad property;

(iii) programmable electronic devices, computers, or other automated systems that are used in providing the transportation;

(iv) alarms, cameras, and other protection systems;

(v) communications systems and utilities needed for railroad security purposes, including dispatching and notification systems;

(vi) emergency response planning;

(vii) employee training; and

(viii) other matters the Secretary determines appropriate; and

(D) identification of redundant and backup systems required to ensure the continued operation of critical elements of a railroad carrier's system in the event of an attack or other incident, including disruption of commercial electric power or a communications network.

(2) THREAT INFORMATION.—The Secretary shall provide in a timely manner to the appropriate employees of a railroad carrier, as designated by the railroad carrier, threat information that is relevant to the carrier when preparing and submitting a vulnerability assessment and security plan, including an assessment of the most likely methods that could be used by terrorists to exploit weaknesses in railroad security.

(e) SECURITY PLANS.—

(1) REQUIREMENTS.—The Secretary shall provide technical assistance and guidance to railroad carriers in preparing and implementing security plans under this section, and shall require that each security plan of a railroad carrier assigned to a high-risk tier under this section include, as applicable—

(A) identification of a security coordinator having authority—

(i) to implement security actions under the plan;

(ii) to coordinate security improvements; and

(iii) to receive immediate communications from appropriate Federal officials regarding railroad security;

(B) a list of needed capital and operational improvements;

(C) procedures to be implemented or used by the railroad carrier in response to a terrorist attack, including evacuation and passenger communication plans that include individuals with disabilities as appropriate;

(D) identification of steps taken with State and local law enforcement agencies, emergency responders, and Federal officials to coordinate security measures and plans for response to a terrorist attack;

(E) a strategy and timeline for conducting training under section 40746 of this title;

(F) enhanced security measures to be taken by the railroad carrier when the Secretary declares a period of heightened security risk;

(G) plans for providing redundant and backup systems required to ensure the continued operation of critical elements of the railroad carrier's system in the event of a terrorist attack or other incident;

(H) a strategy for implementing enhanced security for shipments of security-sensitive materials, including plans for quickly locating and securing the shipments in the event of a terrorist attack or security incident; and

(I) other actions or procedures the Secretary determines are appropriate to address the security of railroad carriers.

(2) SECURITY COORDINATOR REQUIREMENTS.—The Secretary shall require that the individual serving as the security coordinator identified in paragraph (1)(A) is a citizen of the United States. The Secretary may waive this requirement with respect to an individual if the Secretary determines that it is appropriate to do so based on a background check of the individual and a review of the consolidated terrorist watchlist.

(3) CONSISTENCY WITH OTHER PLANS.—The Secretary shall ensure that the security plans developed by railroad carriers under this section are consistent with the risk assessment and National Strategy for Railroad Transportation Security developed under section 40741 of this title.

(f) DEADLINE FOR REVIEW PROCESS.—Not later than 6 months after receiving the assessments and plans required under this section, the Secretary shall—

(1) review each vulnerability assessment and security plan submitted to the Secretary under subsection (c);

(2) require amendments to a security plan that does not meet the requirements of this section; and

(3) approve a vulnerability assessment or security plan that meets the requirements of this section.

(g) TIER ASSIGNMENT.—

(1) IN GENERAL.—Utilizing the risk assessment and National Strategy for Railroad Transportation Security required under section 40741 of this title, the Secretary shall assign each railroad carrier to a risk-based tier established by the Secretary.

(2) PROVIDING INFORMATION.—The Secretary may request, and a railroad carrier shall provide, information necessary for the Secretary to assign a railroad carrier to the appropriate tier under this subsection.

(3) NOTIFICATION.—Not later than 60 days after the date a railroad carrier is assigned to a tier under this subsection, the Secretary shall notify the railroad carrier of the tier to which it is assigned and the reasons for the assignment.

(4) HIGH-RISK TIERS.—At least one of the tiers established by the Secretary under this subsection shall be designated a tier for high-risk railroad carriers.

(5) REASSIGNMENT.—The Secretary may reassign a railroad carrier to another tier, as appropriate, in response to changes in risk. The Secretary shall notify the railroad carrier not later than 60 days after the reassignment and provide the railroad carrier with the reasons for the reassignment.

(h) NONDISCLOSURE OF INFORMATION.—

(1) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this section shall be construed as authorizing the withholding of information from Congress.

(2) DISCLOSURE OF INDEPENDENTLY FURNISHED INFORMATION.—Nothing in this section shall be construed as affecting the authority or obligation of a Federal agency to disclose a record or information that the Federal agency obtains from a railroad carrier under another Federal law.

(i) EXISTING PROCEDURES, PROTOCOLS, AND STANDARDS.—

(1) DETERMINATION.—In response to a petition by a railroad carrier or at the discretion of the Secretary, the Secretary may determine that existing procedures, protocols, and standards meet all or part of the requirements of this section, including regulations issued under subsection (a), regarding vulnerability assessments and security plans.

(2) ELECTION.—Upon review and written determination by the Secretary that existing procedures, protocols, or standards of a railroad carrier satisfy the requirements of this section, the railroad carrier may elect to comply with those procedures, protocols, or standards instead of the requirements of this section.

(3) PARTIAL APPROVAL.—If the Secretary determines that the existing procedures, protocols, or standards of a railroad carrier satisfy only part of the requirements of this section, the Secretary may accept the submission, but shall require submission by the railroad carrier of additional information relevant to the vulnerability assessment and security plan of the railroad carrier to ensure that the remaining requirements of this section are fulfilled.

(4) NOTIFICATION.—If the Secretary determines that particular existing procedures, protocols, or standards of a railroad carrier under

this subsection do not satisfy the requirements of this section, the Secretary shall provide to the railroad carrier a written notification that includes an explanation of the determination.

(5) REVIEW.—Nothing in this subsection shall relieve the Secretary of the obligation—

(A) to review the vulnerability assessment and security plan submitted by a railroad carrier under this section; and

(B) to approve or disapprove each submission on an individual basis.

(j) PERIODIC EVALUATION BY RAILROAD CARRIERS REQUIRED.—

(1) SUBMISSION.—Not later than 3 years after the date on which a vulnerability assessment or security plan required to be submitted to the Secretary under subsection (c) is approved, and at least once every 5 years after the approval (or on another schedule the Secretary may establish by regulation), a railroad carrier that submitted a vulnerability assessment and security plan and that is still assigned to the high-risk tier must submit to the Secretary an evaluation of the adequacy of the vulnerability assessment and security plan that includes a description of material changes made to the vulnerability assessment or security plan.

(2) REVIEW.—Not later than 180 days after the date on which an evaluation is submitted, the Secretary shall review the evaluation and notify the railroad carrier submitting the evaluation of the Secretary's approval or disapproval of the evaluation.

(k) SHARED FACILITIES.—The Secretary may permit under this section the development and implementation of coordinated vulnerability assessments and security plans to the extent that a railroad carrier shares facilities with, or is co-located with, other transportation entities or providers that are required to develop vulnerability assessments and security plans under Federal law.

(l) CONSULTATION.—In carrying out this section, the Secretary shall consult with railroad carriers, nonprofit employee labor organizations representation railroad employees, and public safety and law enforcement officials.

§ 40743. Railroad security assistance

(a) SECURITY IMPROVEMENT GRANTS.—

(1) IN GENERAL.—The Secretary, in consultation with the Administrator of the Transportation Security Administration and other appropriate agencies or officials, may make grants to railroad carriers, the Alaska Railroad, security-sensitive materials offerors who ship by railroad, owners of railroad cars used in the transportation of security-sensitive materials, State and local governments (for railroad passenger fa-

cilities and infrastructure not owned by Amtrak), and Amtrak for intercity passenger railroad and freight railroad security improvements described in subsection (b) as approved by the Secretary.

(2) GRANT ELIGIBILITY.—A railroad carrier is eligible for a grant under this section if the carrier has completed a vulnerability assessment and developed a security plan that the Secretary has approved under section 40742 of this title.

(3) USE OF GRANTS.—A recipient of a grant under this section may use grant funds only for permissible uses under subsection (b) to further a railroad security plan that meets the requirements of paragraph (2).

(4) GRANTS FOR ASSESSMENTS AND PLANS.—Notwithstanding the requirement for eligibility and uses of funds in paragraphs (2) and (3), a railroad carrier is eligible for a grant under this section if the carrier uses the funds solely for the development of assessments or security plans under section 40742 of this title.

(b) USES OF FUNDS.—A recipient of a grant under this section shall use the grant funds for one or more of the following:

(1) Security and redundancy for critical communications, computer, and train control systems essential for secure railroad operations, including communication interoperability where appropriate with relevant outside agencies and entities.

(2) Accommodation of railroad cargo or passenger security inspection facilities, related infrastructure, and operations at or near United States international borders or other ports of entry.

(3) The security of security-sensitive materials transportation by railroad.

(4) Chemical, biological, radiological, or explosive detection, including canine patrols for detection.

(5) The security and preparedness of intercity passenger railroad stations, trains, and infrastructure, including security capital improvement projects that the Secretary determines enhance railroad station security.

(6) Technologies to reduce the vulnerabilities of railroad cars, including structural modification of railroad cars transporting security-sensitive materials to improve their resistance to acts of terrorism.

(7) The sharing of intelligence and information about security threats and preparedness, including connectivity to the National Terrorist Screening Center.

(8) The obtaining of train tracking and communications equipment, including equipment that is interoperable with Federal, State, and local agencies and tribal governments.

(9) The hiring, training, and employment of police, security, and preparedness officers, including canine units, assigned to full-time security or counterterrorism duties related to railroad transportation.

(10) Overtime reimbursement, including reimbursement of State, local, and tribal governments for costs, for enhanced security personnel assigned to duties related to railroad security during periods of high or severe threat levels and National Special Security Events or other periods of heightened security as determined by the Secretary.

(11) Perimeter protection systems, including access control, installation of improved lighting, fencing, and barricades at railroad facilities.

(12) Tunnel protection systems.

(13) Passenger evacuation and evacuation-related capital improvements.

(14) Railroad security inspection technologies, including verified visual inspection technologies using hand-held readers.

(15) Surveillance equipment.

(16) Cargo or passenger screening equipment.

(17) Emergency response equipment, including fire suppression and decontamination equipment, personal protective equipment, and defibrillators.

(18) Operating and capital costs associated with security awareness, preparedness, and response training, including training under section 40746 of this title, and training developed by universities, institutions of higher education, and nonprofit employee labor organizations, for railroad employees, including frontline employees.

(19) Live or simulated exercises, including exercises described in section 40745 of this title.

(20) Public awareness campaigns for enhanced railroad security.

(21) Development of assessments or security plans under section 40742 of this title.

(22) Other security improvements—

(A) identified, required, or recommended under sections 40741 and 40742 of this title, including infrastructure, facilities, and equipment upgrades; or

(B) that the Secretary considers appropriate.

(c) DEPARTMENTAL RESPONSIBILITIES.—In carrying out the responsibilities under subsection (a), the Secretary shall—

(1) determine the requirements for recipients of grants;

(2) establish priorities for uses of funds for grant recipients;

(3) award the funds authorized by this section based on risk, as identified by the plans required under sections 40741 and 40742 of this title;

(4) take into account whether stations or facilities are used by commuter railroad passengers as well as intercity railroad passengers in reviewing grant applications;

(5) encourage non-Federal financial participation in projects funded by grants; and

(6) not later than 5 business days after awarding a grant to Amtrak under this section, transfer grant funds to the Secretary of Transportation to be disbursed to Amtrak.

(d) MULTIYEAR AWARDS.—Grant funds awarded under this section may be awarded for projects that span multiple years.

(e) LIMITATION ON USES OF FUNDS.—A grant made under this section may not be used to make a State or local government cost-sharing contribution under any other Federal law.

(f) ANNUAL REPORTS.—Each recipient of a grant under this section shall report annually to the Secretary on the use of grant funds.

(g) SUBJECT TO CERTAIN STANDARDS.—A recipient of a grant under this section and section 40744 of this title shall be required to comply with the standards of section 24312 of title 49, as in effect on January 1, 2007, with respect to the project, in the same manner as Amtrak is required to comply with the standards for construction work financed under an agreement made under section 24308(a) of title 49.

§ 40744. Systemwide Amtrak security upgrades

(a) IN GENERAL.—

(1) GRANTS.—Subject to subsection (b), the Secretary, in consultation with the Administrator of the Transportation Security Administration, may make grants to Amtrak under this section.

(2) GENERAL PURPOSES.—The Secretary may make grants for the purposes of—

(A) protecting underwater and underground assets and systems;

(B) protecting high-risk and high-consequence assets identified through system-wide risk assessments;

(C) providing counterterrorism or security training;

(D) providing both visible and unpredictable deterrence; and

(E) conducting emergency preparedness drills and exercises.

(3) SPECIFIC PROJECTS.—The Secretary shall make grants—

(A) to secure major tunnel access points and ensure tunnel integrity in New York, New Jersey, Maryland, and Washington, DC;

(B) to secure Amtrak trains;

(C) to secure Amtrak stations;

(D) to obtain a watchlist identification system approved by the Secretary, or to connect to the National Terrorist Screening Center watchlist;

(E) to obtain train tracking and interoperable communications systems that are coordinated with Federal, State, and local agencies and tribal governments to the maximum extent possible;

(F) to hire, train, and employ police and security officers, including canine units, assigned to full-time security or counterterrorism duties related to railroad transportation;

(G) for operating and capital costs associated with security awareness, preparedness, and response training, including training under section 40746 of this title, and training developed by universities, institutions of higher education, and nonprofit employee labor organizations, for railroad employees, including frontline employees;

(H) for live or simulated exercises, including exercises described in section 40745 of this title;

(I) for improvements to passenger verification systems;

(J) for improvements to employee and contractor verification systems, including identity verification technology; and

(K) for improvements to the security of Amtrak computer systems, including cybersecurity assessments and programs.

(b) CONDITIONS.—The Secretary shall award grants to Amtrak under this section for projects contained in a system-wide security plan approved by the Secretary developed under section 40742 of this title. Not later than 5 business days after awarding a grant to Amtrak under this section, the Secretary shall transfer the grant funds to the Secretary of Transportation to be disbursed to Amtrak.

(c) EQUITABLE GEOGRAPHIC ALLOCATION.—The Secretary shall ensure that, subject to meeting the highest security needs on Amtrak's entire system and consistent with the risk assessment required under section 40741 of this title and Amtrak's vulnerability assessment and security plan developed under section 40742 of this title, stations and facilities located outside of the Northeast Corridor receive an equitable share of the security funds authorized by this section.

(d) PASSENGER RAIL VETTING.—

(1) DECISION BY ADMINISTRATOR.—Not later than 180 days after the date on which the Amtrak Board of Directors submits a request to the Administrator, the Administrator shall issue a decision on the

use by Amtrak of the Transportation Security Administration's Secure Flight Program or a similar passenger vetting system to enhance passenger rail security.

(2) CONSIDERATIONS.—In making a decision under paragraph (1), the Administrator shall—

(A) consider the technological, privacy, operational, and security impacts of the decision; and

(B) describe the impacts in a strategic plan developed under paragraph (3).

(3) STRATEGIC PLAN.—If the Administrator decides to grant the request by Amtrak under paragraph (1), the decision shall include a strategic plan for working with rail stakeholders to enhance passenger rail security—

(A) by vetting passengers using terrorist watch lists maintained by the Federal Government or a similar passenger vetting system maintained by the Transportation Security Administration; and

(B) where applicable and in consultation with the Commissioner of U.S. Customs and Border Protection, by assessing whether the vetting process shall be integrated into preclearance operations established under section 813 of the Preclearance Authorization Act of 2015 (19 U.S.C. 4432).

(4) NOTICE.—

(B) IN GENERAL.—The Administrator shall notify the Committees on Commerce, Science, and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives of any decision made under paragraph (1) and the details of the strategic plan under paragraph (3).

(5) AUTHORITY OF ADMINISTRATOR NOT LIMITED.—Nothing in this subsection shall be considered to limit the Administrator's authority to set the access to, or the terms and conditions of using, the Secure Flight Program or similar passenger vetting systems.

§ 40745. Railroad carrier exercises

(a) IN GENERAL.—The Secretary shall establish a program for conducting security exercises for railroad carriers for the purpose of assessing and improving the capabilities of entities described in subsection (b) to prevent, prepare for, mitigate, respond to, and recover from acts of terrorism.

(b) COVERED ENTITIES.—Entities to be assessed under the program include—

(1) Federal, State, and local agencies and tribal governments;

(2) railroad carriers;

(3) governmental and nongovernmental emergency response providers, law enforcement agencies, and railroad and transit police, as appropriate; and

(4) any other organization or entity that the Secretary determines appropriate.

(c) REQUIREMENTS.—The Secretary shall ensure that the program—

(1) consolidates existing security exercises for railroad carriers administered by the Department and the Department of Transportation, as jointly determined by the Secretary and the Secretary of Transportation, unless the Secretary waives this consolidation requirement as appropriate;

(2) consists of exercises that are—

(A) scaled and tailored to the needs of the carrier, including addressing the needs of the elderly and individuals with disabilities;

(B) live, in the case of the facilities most at risk to a terrorist attack;

(C) coordinated with appropriate officials;

(D) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(E) inclusive, as appropriate, of railroad frontline employees; and

(F) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, and other national initiatives of this type;

(3) provides that exercises described in paragraph (2) will be—

(A) evaluated by the Secretary against clear and consistent performance measures;

(B) assessed by the Secretary to identify best practices, which shall be shared, as appropriate, with railroad carriers, nonprofit employee organizations that represent railroad carrier employees, Federal, State, local, and tribal officials, governmental and nongovernmental emergency response providers, law enforcement personnel, including railroad carrier and transit police, and other stakeholders; and

(C) used to develop recommendations, as appropriate, from the Secretary to railroad carriers on remedial action to be taken in response to lessons learned;

(4) allows for proper advanced notification of communities and local governments in which exercises are held, as appropriate; and

(5) assists State, local, and tribal governments and railroad carriers in designing, implementing, and evaluating additional exercises that conform to the requirements of paragraph (2).

(d) NATIONAL EXERCISE PROGRAM.—The Secretary shall ensure that the exercise program developed under subsection (c) is a component of the national exercise program established under section 20508 of this title.

§ 40746. Railroad security training program

(a) IN GENERAL.—The Secretary shall develop and issue regulations for a training program to prepare railroad frontline employees for potential security threats and conditions. The regulations shall take into consideration current security training requirements or best practices.

(b) CONSULTATION.—The Secretary shall develop the regulations under subsection (a) in consultation with—

(1) appropriate law enforcement, fire service, emergency response, security, and terrorism experts;

(2) railroad carriers;

(3) railroad shippers; and

(4) nonprofit employee labor organizations representing railroad employees or emergency response personnel.

(c) PROGRAM ELEMENTS.—The regulations developed under subsection (a) shall require security training programs described in subsection (a) to include, at a minimum, elements to address the following, as applicable:

(1) The determination of the seriousness of an occurrence or threat.

(2) Crew and passenger communication and coordination.

(3) Appropriate responses to defend or protect oneself.

(4) The use of personal and other protective equipment.

(5) Evacuation procedures for passengers and railroad employees, including individuals with disabilities and the elderly.

(6) The psychology, behavior, and methods of terrorists, including observation and analysis.

(7) Training related to psychological responses to terrorist incidents, including the ability to cope with hijacker behavior and passenger responses.

(8) Live situational training exercises regarding various threat conditions, including tunnel evacuation procedures.

(9) The recognition and reporting of dangerous substances, suspicious packages, and situations.

(10) The understanding of security incident procedures, including procedures for communicating with governmental and nongovernmental emergency response providers and for on-scene interaction with emergency response providers.

(11) The operation and maintenance of security equipment and systems.

(12) Other security training activities that the Secretary considers appropriate.

(d) SUBMITTING PROGRAM TO SECRETARY FOR APPROVAL.—Each railroad carrier shall develop a security training program under this section and submit the program to the Secretary for approval. Not later than 60 days after receiving a security training program proposal under this subsection, the Secretary shall approve the program or require the railroad carrier that developed the program to make revisions to the program that the Secretary considers necessary for the program to meet the requirements of this section. A railroad carrier shall respond to the Secretary's comments within 30 days after receiving them.

(e) TRAINING.—Not later than 1 year after the Secretary approves a security training program under subsection (d), the railroad carrier that developed the program shall complete the training of all railroad frontline employees who were hired by a carrier more than 30 days preceding the approval date. For employees employed by a carrier for fewer than 30 days preceding the approval date, training shall be completed within the first 60 days of employment.

(f) UPDATES OF REGULATIONS AND PROGRAM REVISIONS.—The Secretary periodically shall review and update as appropriate the training regulations issued under subsection (a) to reflect new or changing security threats. Each railroad carrier shall revise its training program accordingly and provide additional training as necessary to its frontline employees within a reasonable time after the regulations are updated.

(g) PROGRAM COMPONENT OF NATIONAL TRAINING PROGRAM.—The Secretary shall ensure that the training program developed under subsection (a) is a component of the national training program established under section 20508 of this title.

(h) OTHER EMPLOYEES.—The Secretary shall issue guidance and best practices for a railroad shipper employee security program containing the elements listed under subsection (c).

§ 40747. Railroad security research and development

(a) ESTABLISHMENT OF RESEARCH AND DEVELOPMENT PROGRAM.—The Secretary, acting through the Under Secretary for Science and Technology and the Administrator of the Transportation Security Administration, shall carry out a research and development program for the purpose of improving the security of railroad transportation systems.

(b) ELIGIBLE PROJECTS.—The research and development program may include projects—

(1) to reduce the vulnerability of passenger trains, stations, and equipment to explosives and hazardous chemical, biological, and radioactive substances, including the development of technology to screen passengers in large numbers at peak commuting times with minimal interference and disruption;

(2) to test new emergency response and recovery techniques and technologies, including those used at international borders;

(3) to develop improved railroad security technologies, including—

(A) technologies for sealing or modifying railroad tank cars;

(B) automatic inspection of railroad cars;

(C) communication-based train control systems;

(D) emergency response training, including training in a tunnel environment;

(E) security and redundancy for critical communications, electrical power, computer, and train control systems; and

(F) technologies for securing bridges and tunnels;

(4) to test wayside detectors that can detect tampering;

(5) to support enhanced security for the transportation of security-sensitive materials by railroad;

(6) to mitigate damages in the event of a cyberattack; and

(7) to address other vulnerabilities and risks identified by the Secretary.

(c) COORDINATION WITH OTHER RESEARCH INITIATIVES.—The Secretary—

(1) shall ensure that the research and development program is consistent with the National Strategy for Railroad Transportation Security developed under section 40741 of this title and other transportation security research and development programs required by section 30304 and chapters 401 through 407 of this title;

(2) shall, to the extent practicable, coordinate the research and development activities of the Department with other ongoing research and development security-related initiatives, including research being conducted by—

(A) the Department of Transportation, including University Transportation Centers and other institutes, centers, and simulators funded by the Department of Transportation;

(B) the National Academy of Sciences;

(C) the Technical Support Working Group;

(D) other Federal departments and agencies; and

(E) other Federal and private research laboratories, research entities, and universities and institutions of higher education, in-

cluding Historically Black Colleges and Universities, Hispanic-serving institutions, or Indian tribally controlled colleges and universities;

(3) shall carry out a research and development project authorized by this section through a reimbursable agreement with an appropriate Federal agency, if the agency—

(A) is currently sponsoring a research and development project in a similar area; or

(B) has a unique facility or capability that would be useful in carrying out the project;

(4) may award grants to, or enter into cooperative agreements, contracts, other transactions, or reimbursable agreements with, the entities described in paragraph (2) and eligible grant recipients under section 40743 of this title; and

(5) shall make reasonable efforts to enter into memoranda of understanding, contracts, grants, cooperative agreements, or other transactions with railroad carriers willing to contribute both physical space and other resources.

(d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES.—

(1) CONSULTATION.—In carrying out research and development projects under this section, the Secretary shall consult with the Chief Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department as appropriate and under section 10520 of this title.

(2) PRIVACY IMPACT ASSESSMENTS.—In accordance with sections 10520 and 11705 of this title, the Chief Privacy Officer shall conduct privacy impact assessments, and the Officer for Civil Rights and Civil Liberties shall conduct reviews, as appropriate, for research and development initiatives developed under this section that the Secretary determines could have an impact on privacy, civil rights, or civil liberties.

§ 40748. Railroad tank car security testing

(a) VULNERABILITY ASSESSMENT.—

(1) LIKELY METHODS AND SUCCESS.—The Secretary shall assess the likely methods of a deliberate terrorist attack against a railroad tank car used to transport toxic-inhalation-hazard materials, and for each method assessed, the degree to which it may be successful in causing death, injury, or serious adverse effects to human health, the environment, critical infrastructure, national security, the national economy, or public welfare.

(2) THREATS.—In carrying out paragraph (1), the Secretary shall consider the most current threat information as to likely methods of

a successful terrorist attack on a railroad tank car transporting toxic-inhalation-hazard materials, and may consider the following:

(A) Explosive devices placed along the tracks or attached to a railroad tank car.

(B) The use of missiles, grenades, rockets, mortars, or other high-caliber weapons against a railroad tank car.

(3) PHYSICAL TESTING.—In developing the assessment required under paragraph (1), the Secretary shall conduct physical testing of the vulnerability of railroad tank cars used to transport toxic-inhalation-hazard materials to different methods of a deliberate attack, using technical information and criteria to evaluate the structural integrity of railroad tank cars.

(b) DISPERSION MODELING.—

(1) IN GENERAL.—The Secretary, acting through the National Infrastructure Simulation and Analysis Center, shall conduct an air dispersion modeling analysis of release scenarios of toxic-inhalation-hazard materials resulting from a terrorist attack on a loaded railroad tank car carrying these materials in urban and rural environments.

(2) CONSIDERATIONS.—The analysis under this subsection shall take into account the following considerations:

(A) The most likely means of attack and the resulting dispersal rate.

(B) Different times of day, to account for differences in cloud coverage and other atmospheric conditions in the environment being modeled.

(C) Differences in population size and density.

(D) Historically accurate wind speeds, temperatures, and wind directions.

(E) Differences in dispersal rates or other relevant factors related to whether a railroad tank car is in motion or stationary.

(F) Emergency response procedures by local officials.

(G) Other considerations the Secretary believes would develop an accurate, plausible dispersion model for toxic-inhalation-hazard materials released from a railroad tank car as a result of a terrorist act.

(3) CONSULTATION.—In conducting the dispersion modeling under paragraph (1), the Secretary shall consult with the Secretary of Transportation, hazardous materials experts, railroad carriers, nonprofit employee labor organizations representing railroad employees, appropriate State, local, and tribal officials, and other Federal agencies, as appropriate.

(4) INFORMATION SHARING.—On completion of the analysis required under paragraph (1), the Secretary shall share the information developed with the appropriate stakeholders, given appropriate information protection provisions as may be required by the Secretary.

§ 40749. Security background checks of covered individuals

(a) DEFINITIONS.—In this section:

(1) COVERED INDIVIDUAL.—The term ''covered individual'' means an employee of a railroad carrier or a contractor or subcontractor of a railroad carrier.

(2) SECURITY BACKGROUND CHECK.—The term ''security background check'' means for the purpose of identifying individuals who may pose a threat to transportation security or national security, or of terrorism—

(A) relevant criminal history databases;

(B) in the case of an alien (as defined in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101)), the relevant databases to determine the status of the alien under the immigration laws of the United States; and

(C) other relevant information or databases, as determined by the Secretary.

(b) GUIDANCE.—

(1) IN GENERAL.—Guidance, recommendations, suggested action items, and other widely disseminated voluntary action items issued by the Secretary to a railroad carrier or a contractor or subcontractor of a railroad carrier relating to performing a security background check of a covered individual shall contain recommendations on the appropriate scope and application of a security background check, including the time period covered, the types of disqualifying offenses, and a redress process for adversely impacted covered individuals consistent with subsections (c) and (d).

(2) UPDATE OF EXISTING GUIDANCE.—Guidance, recommendations, suggested action items, and other widely disseminated voluntary action items issued by the Secretary prior to August 3, 2007, to a railroad carrier or a contractor or subcontractor of a railroad carrier relating to performing a security background check of a covered individual shall be updated in compliance with paragraph (1).

(3) NECESSARY REDRESS PROCEDURE.—If a railroad carrier or a contractor or subcontractor of a railroad carrier performs a security background check on a covered individual to fulfill guidance issued by the Secretary under paragraph (1) or (2), the Secretary shall not con-

sider the guidance fulfilled unless an adequate redress process as described in subsection (d) is provided to covered individuals.

(c) REQUIREMENTS.—If the Secretary issues a rule, regulation, or directive requiring a railroad carrier or contractor or subcontractor of a railroad carrier to perform a security background check of a covered individual, the Secretary shall prohibit the railroad carrier or contractor or subcontractor of a railroad carrier from making an adverse employment decision, including removal or suspension of the covered individual, due to the rule, regulation, or directive with respect to a covered individual unless the railroad carrier or contractor or subcontractor of a railroad carrier determines that the covered individual—

(1) has been convicted of, has been found not guilty by reason of insanity, or is under want, warrant, or indictment for a permanent disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations;

(2) was convicted of or found not guilty by reason of insanity of an interim disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations, within 7 years of the date that the railroad carrier or contractor or subcontractor of a railroad carrier performs the security background check; or

(3) was incarcerated for an interim disqualifying criminal offense listed in part 1572 of title 49, Code of Federal Regulations, and released from incarceration within 5 years of the date that the railroad carrier or contractor or subcontractor of a railroad carrier performs the security background check.

(d) REDRESS PROCESS.—If the Secretary issues a rule, regulation, or directive requiring a railroad carrier or contractor or subcontractor of a railroad carrier to perform a security background check of a covered individual, the Secretary shall—

(1) provide an adequate redress process for a covered individual subjected to an adverse employment decision, including removal or suspension of the employee, due to the rule, regulation, or directive that is consistent with the appeals and waiver process established for applicants for commercial motor vehicle hazardous materials endorsements and transportation employees at ports, as required by section 70105(c) of title 46; and

(2) have the authority to order an appropriate remedy, including reinstatement of the covered individual, should the Secretary determine that a railroad carrier or contractor or subcontractor of a railroad carrier wrongfully made an adverse employment decision regarding a covered individual pursuant to the rule, regulation, or directive.

(e) FALSE STATEMENTS.—A railroad carrier or a contractor or subcontractor of a railroad carrier may not knowingly misrepresent 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. The Secretary shall issue a regulation that prohibits a railroad carrier or 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.

(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.

(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.

(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.

§ 40750. International railroad security program

(a) DEFINITIONS.—In this section:

(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.

(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.

(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.

(b) IN GENERAL.—

(1) DETECTION SYSTEM.—The Secretary shall develop a system to detect both undeclared passengers and contraband, with a primary focus on the detection of nuclear and radiological materials entering the United States by railroad.

(2) SYSTEM REQUIREMENTS.—In developing the system under paragraph (1), the Secretary may, in consultation with the Domestic Nuclear Detection Office, U.S. Customs and Border Protection, and Transportation Security Administration—

(A) deploy radiation detection equipment and nonintrusive imaging equipment at locations where railroad shipments cross an international border to enter the United States;

(B) consider the integration of radiation detection technologies with other nonintrusive inspection technologies where feasible;

(C) ensure appropriate training, operations, and response protocols are established for Federal, State, and local personnel;

(D) implement alternative procedures to check railroad shipments at locations where the deployment of nonintrusive inspection imaging equipment is determined to not be practicable;

(E) ensure, to the extent practicable, that the technologies deployed can detect terrorists or weapons, including weapons of mass destruction; and

(F) take other actions, as appropriate, to develop the system.

(c) ADDITIONAL INFORMATION.—The Secretary shall—

(1) identify and seek the submission of additional data elements for improved high-risk targeting related to the movement of cargo through the international supply chain utilizing a railroad prior to importation into the United States;

(2) utilize data collected and maintained by the Secretary of Transportation in the targeting of high-risk cargo identified under paragraph (1); and

(3) analyze the data provided in this subsection to identify high-risk cargo for inspection.

Subchapter III—Over-the-Road Bus Security

§ 40761. Assessments and plans

(a) IN GENERAL.—The Secretary shall issue regulations that—

(1) require each over-the-road bus operator assigned to a high-risk tier under this section—

(A) to conduct a vulnerability assessment under subsections (c) and (d); and

(B) to prepare, submit to the Secretary for approval, and implement a security plan under subsection (e); and

(2) establish standards and guidelines for developing and implementing the vulnerability assessments and security plans for carriers assigned to high-risk tiers consistent with this section.

(b) NON-HIGH-RISK PROGRAMS.—The Secretary may establish a security program for over-the-road bus operators not assigned to a high-risk tier, including—

(1) guidance for operators in conducting vulnerability assessments and preparing and implementing security plans, as determined appropriate by the Secretary; and

(2) a process to review and approve the assessments and plans, as appropriate.

(c) SUBMISSION OF ASSESSMENTS AND SECURITY PLANS.—The vulnerability assessments and security plans required by the regulations for over-the-road bus operators assigned to a high-risk tier shall be completed and submitted to the Secretary for review and approval.

(d) VULNERABILITY ASSESSMENTS.—

(1) REQUIREMENTS.—The Secretary shall provide technical assistance and guidance to over-the-road bus operators in conducting vulnerability assessments under this section and shall require that each vulnerability assessment of an operator assigned to a high-risk tier under this section includes, as appropriate—

(A) identification and evaluation of critical assets and infrastructure, including platforms, stations, terminals, and information systems;

(B) identification of the vulnerabilities of those assets and infrastructure; and

(C) identification of weaknesses in—

(i) physical security;

(ii) passenger and cargo security;

(iii) the security of programmable electronic devices, computers, or other automated systems which are used in providing over-the-road bus transportation;

(iv) alarms, cameras, and other protection systems;

(v) communications systems and utilities needed for over-the-road bus security purposes, including dispatching systems;

(vi) emergency response planning;

(vii) employee training; and

(viii) other matters the Secretary determines appropriate.

(2) THREAT INFORMATION.—The Secretary shall provide in a timely manner to the appropriate employees of an over-the-road bus operator, as designated by the over-the-road bus operator, threat information that is relevant to the operator when preparing and submitting a vulnerability assessment and security plan, including an assessment of the most likely methods that could be used by terrorists to exploit weaknesses in over-the-road bus security.

(e) SECURITY PLANS.—

(1) REQUIREMENTS.—The Secretary shall provide technical assistance and guidance to over-the-road bus operators in preparing and implementing security plans under this section and shall require that each security plan of an over-the-road bus operator assigned to a high-risk tier under this section includes, as appropriate—

(A) the identification of a security coordinator having authority—

(i) to implement security actions under the plan;

(ii) to coordinate security improvements; and

(iii) to receive communications from appropriate Federal officials regarding over-the-road bus security;

(B) a list of needed capital and operational improvements;

(C) procedures to be implemented or used by the over-the-road bus operator in response to a terrorist attack, including evacuation and passenger communication plans that include individuals with disabilities, as appropriate;

(D) the identification of steps taken with State and local law enforcement agencies, emergency responders, and Federal officials to coordinate security measures and plans for response to a terrorist attack;

(E) a strategy and timeline for conducting training under section 40764 of this title;

(F) enhanced security measures to be taken by the over-the-road bus operator when the Secretary declares a period of heightened security risk;

(G) plans for providing redundant and backup systems required to ensure the continued operation of critical elements of the over-the-road bus operator's system in the event of a terrorist attack or other incident; and

(H) other actions or procedures the Secretary determines are appropriate to address the security of over-the-road bus operators.

(2) SECURITY COORDINATOR REQUIREMENTS.—The Secretary shall require that the individual serving as the security coordinator identified in paragraph (1)(A) is a citizen of the United States. The Secretary may waive this requirement with respect to an individual if the Secretary determines that it is appropriate to do so based on a background check of the individual and a review of the consolidated terrorist watchlist.

(f) DEADLINE FOR REVIEW PROCESS.—Not later than 6 months after receiving the assessments and plans required under this section, the Secretary shall—

(1) review each vulnerability assessment and security plan submitted to the Secretary under subsection (c);

(2) require amendments to a security plan that does not meet the requirements of this section; and

(3) approve a vulnerability assessment or security plan that meets the requirements of this section.

(g) TIER ASSIGNMENT.—

(1) IN GENERAL.—The Secretary shall assign each over-the-road bus operator to a risk-based tier established by the Secretary.

(2) PROVIDING INFORMATION.—The Secretary may request, and an over-the-road bus operator shall provide, information necessary for the Secretary to assign an over-the-road bus operator to the appropriate tier under this subsection.

(3) NOTIFICATION.—Not later than 60 days after the date an over-the-road bus operator is assigned to a tier under this section, the Secretary shall notify the operator of the tier to which it is assigned and the reasons for the assignment.

(4) HIGH-RISK TIERS.—At least one of the tiers established by the Secretary under this section shall be a tier designated for high-risk over-the-road bus operators.

(5) REASSIGNMENT.—The Secretary may reassign an over-the-road bus operator to another tier, as appropriate, in response to changes in risk, and the Secretary shall notify the over-the-road bus operator within 60 days after the reassignment and provide the operator with the reasons for the reassignment.

(h) EXISTING PROCEDURES, PROTOCOLS, AND STANDARDS.—

(1) DETERMINATION.—In response to a petition by an over-the-road bus operator or at the discretion of the Secretary, the Secretary may determine that existing procedures, protocols, and standards meet all

or part of the requirements of this section regarding vulnerability assessments and security plans.

(2) ELECTION.—On review and written determination by the Secretary that existing procedures, protocols, or standards of an over-the-road bus operator satisfy the requirements of this section, the over-the-road bus operator may elect to comply with those procedures, protocols, or standards instead of the requirements of this section.

(3) PARTIAL APPROVAL.—If the Secretary determines that the existing procedures, protocols, or standards of an over-the-road bus operator satisfy only part of the requirements of this section, the Secretary may accept a submission, but shall require submission by the operator of additional information relevant to the vulnerability assessment and security plan of the operator to ensure that the remaining requirements of this section are fulfilled.

(4) NOTIFICATION.—If the Secretary determines that particular existing procedures, protocols, or standards of an over-the-road bus operator under this subsection do not satisfy the requirements of this section, the Secretary shall provide to the operator a written notification that includes an explanation of the reasons for non-acceptance.

(5) REVIEW.—Nothing in this subsection shall relieve the Secretary of the obligation—

(A) to review the vulnerability assessment and security plan submitted by an over-the-road bus operator under this section; and

(B) to approve or disapprove each submission on an individual basis.

(i) PERIODIC EVALUATION BY OVER-THE-ROAD BUS PROVIDER REQUIRED.—

(1) SUBMISSION.—Not later than 3 years after the date on which a vulnerability assessment or security plan required to be submitted to the Secretary under subsection (c) is approved, and at least once every 5 years thereafter (or on another schedule the Secretary may establish by regulation), an over-the-road bus operator who submitted a vulnerability assessment and security plan and who is still assigned to the high-risk tier shall also submit to the Secretary an evaluation of the adequacy of the vulnerability assessment and security plan that includes a description of material changes made to the vulnerability assessment or security plan.

(2) REVIEW.—Not later than 180 days after the date on which an evaluation is submitted, the Secretary shall review the evaluation and notify the over-the-road bus operator submitting the evaluation of the Secretary's approval or disapproval of the evaluation.

(j) SHARED FACILITIES.—The Secretary may permit under this section the development and implementation of coordinated vulnerability assessments and security plans to the extent that an over-the-road bus operator shares facilities with, or is co-located with, other transportation entities or providers that are required to develop vulnerability assessments and security plans under Federal law.

(k) NONDISCLOSURE OF INFORMATION.—

(1) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this section shall be construed as authorizing the withholding of information from Congress.

(2) DISCLOSURE OF INDEPENDENTLY FURNISHED INFORMATION.—Nothing in this section shall be construed as affecting the authority or obligation of a Federal agency to disclose a record or information that the Federal agency obtains from an over-the-road bus operator under any other Federal law.

§ 40762. Assistance

(a) IN GENERAL.—The Secretary shall establish a program for making grants to eligible private operators providing transportation by an over-the-road bus for security improvements described in subsection (b).

(b) USES OF FUNDS.—A recipient of a grant received under subsection (a) shall use the grant funds for one or more of the following:

(1) Constructing and modifying terminals, garages, and facilities, including terminals and other over-the-road bus facilities owned by State or local governments, to increase their security.

(2) Modifying over-the-road buses to increase their security.

(3) Protecting or isolating the driver of an over-the-road bus.

(4) Acquiring, upgrading, installing, or operating equipment, software, or accessorial services for collection, storage, or exchange of passenger and driver information through ticketing systems or other means and for information links with government agencies, for security purposes.

(5) Installing cameras and video surveillance equipment on over-the-road buses and at terminals, garages, and over-the-road bus facilities.

(6) Establishing and improving an emergency communications system linking drivers and over-the-road buses to the recipient's operations center or linking the operations center to law enforcement and emergency personnel.

(7) Implementing and operating passenger screening programs for weapons and explosives.

(8) Public awareness campaigns for enhanced over-the-road bus security.

(9) Operating and capital costs associated with over-the-road bus security awareness, preparedness, and response training, including training under section 40764 of this title and training developed by institutions of higher education and by nonprofit employee labor organizations, for over-the-road bus employees, including frontline employees.

(10) Chemical, biological, radiological, or explosive detection, including canine patrols for detection.

(11) Overtime reimbursement, including reimbursement of State, local, and tribal governments for costs, for enhanced security personnel assigned to duties related to over-the-road bus security during periods of high or severe threat levels, National Special Security Events, or other periods of heightened security as determined by the Secretary.

(12) Live or simulated exercises, including those described in section 40763 of this title.

(13) Operational costs to hire, train, and employ police and security officers, including canine units, assigned to full-time security or counterterrorism duties related to over-the-road bus transportation, including reimbursement of State, local, and tribal government costs for the personnel.

(14) Development of assessments or security plans under section 40761 of this title.

(15) Other improvements the Secretary considers appropriate.

(c) DUE CONSIDERATION.—In making grants under this section, the Secretary shall prioritize grant funding based on security risks to bus passengers and the ability of a project to reduce, or enhance response to, that risk, and shall not penalize private operators of over-the-road buses that took measures to enhance over-the-road bus transportation security prior to September 11, 2001.

(d) SECRETARY'S RESPONSIBILITIES.—In carrying out the responsibilities under subsection (a), the Secretary shall—

(1) determine the requirements for recipients of grants under this section, including application requirements;

(2) select grant recipients;

(3) award the funds authorized by this section based on risk, as identified by the plans required under section 40761 of this title or an assessment or plan described in subsection (f)(2); and

(4) under subsection (c), establish priorities for the use of funds for grant recipients.

(e) DISTRIBUTION OF GRANTS.—The Secretary and the Secretary of Transportation shall determine the most effective and efficient way to distribute grant funds to the recipients of grants determined by the Secretary

under subsection (a). Subject to the determination made by the Secretaries, the Secretary may transfer funds to the Secretary of Transportation for the purposes of disbursing funds to the grant recipient.

(f) ELIGIBILITY.—

(1) IN GENERAL.—A private operator providing transportation by an over-the-road bus is eligible for a grant under this section if the operator has completed a vulnerability assessment and developed a security plan that the Secretary has approved under section 40761 of this title. Grant funds may only be used for permissible uses under subsection (b) to further an over-the-road bus security plan.

(2) INTERIM ELIGIBILITY.—Notwithstanding the requirements for eligibility and uses in paragraph (1), the Secretary may award grants under this section for over-the-road bus security improvements listed under subsection (b) based on over-the-road bus vulnerability assessments and security plans that the Secretary considers sufficient for the purposes of this section but have not been approved by the Secretary under section 40761 of this title.

(g) GRANT TERMS AND CONDITIONS.—Except as otherwise specifically provided in this section, a grant made under this section shall be subject to the terms and conditions applicable to subrecipients who provide over-the-road bus transportation under 5311(f) of title 49 and other terms and conditions that the Secretary determines are necessary.

(h) LIMITATION ON USES OF FUNDS.—A grant made under this section may not be used to make a State or local government cost-sharing contribution under any other Federal law.

(i) ANNUAL REPORTS.—Each recipient of a grant under this section shall report annually to the Secretary on the use of the grant funds.

(j) CONSULTATION.—In carrying out this section, the Secretary shall consult with over-the-road bus operators and nonprofit employee labor organizations representing over-the-road bus employees and public safety and law enforcement officials.

§ 40763. Exercises

(a) IN GENERAL.—The Secretary shall establish a program for conducting security exercises for over-the-road bus transportation for the purpose of assessing and improving the capabilities of entities described in subsection (b) to prevent, prepare for, mitigate, respond to, and recover from acts of terrorism.

(b) COVERED ENTITIES.—Entities to be assessed under the program include—

(1) Federal, State, and local agencies and tribal governments;

(2) over-the-road bus operators and over-the-road bus terminal owners and operators;

(3) governmental and nongovernmental emergency response providers and law enforcement agencies; and

(4) other organizations or entities that the Secretary determines appropriate.

(c) REQUIREMENTS.—The Secretary shall ensure that the program—

(1) consolidates existing security exercises for over-the-road bus operators and terminals administered by the Department and the Department of Transportation, as jointly determined by the Secretary and the Secretary of Transportation, unless the Secretary waives this consolidation requirement, as appropriate;

(2) consists of exercises that are—

(A) scaled and tailored to the needs of the over-the-road bus operators and terminals, including addressing the needs of the elderly and individuals with disabilities;

(B) live, in the case of the facilities most at risk to a terrorist attack;

(C) coordinated with appropriate officials;

(D) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(E) inclusive, as appropriate, of over-the-road bus frontline employees; and

(F) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, and other such national initiatives;

(3) provides that exercises described in paragraph (2) will be—

(A) evaluated by the Secretary against clear and consistent performance measures;

(B) assessed by the Secretary to identify best practices, which shall be shared, as appropriate, with operators providing over-the-road bus transportation, nonprofit employee organizations that represent over-the-road bus employees, Federal, State, local, and tribal officials, governmental and nongovernmental emergency response providers, and law enforcement personnel; and

(C) used to develop recommendations, as appropriate, provided to over-the-road bus operators and terminal owners and operators on remedial action to be taken in response to lessons learned;

(4) allows for proper advanced notification of communities and local governments in which exercises are held, as appropriate; and

(5) assists State, local, and tribal governments and over-the-road bus operators and terminal owners and operators in designing, implementing, and evaluating additional exercises that conform to the requirements of paragraph (2).

(d) CONSISTENT WITH NATIONAL EXERCISE PROGRAM.—The Secretary shall ensure that the exercise program developed under subsection (c) is consistent with the national exercise program established under section 20508 of this title.

§ 40764. Training program

(a) IN GENERAL.—The Secretary shall develop and issue regulations for an over-the-road bus training program to prepare over-the-road bus frontline employees for potential security threats and conditions. The regulations shall take into consideration current security training requirements or best practices.

(b) CONSULTATION.—The Secretary shall develop regulations under subsection (a) in consultation with—

(1) appropriate law enforcement, fire service, emergency response, security, and terrorism experts;

(2) operators providing over-the-road bus transportation; and

(3) nonprofit employee labor organizations representing over-the-road bus employees and emergency response personnel.

(c) PROGRAM ELEMENTS.—The regulations developed under subsection (a) shall require security training programs to include, at a minimum, elements to address the following, as applicable:

(1) Determination of the seriousness of an occurrence or threat.

(2) Driver and passenger communication and coordination.

(3) Appropriate responses to defend or protect oneself.

(4) Use of personal and other protective equipment.

(5) Evacuation procedures for passengers and over-the-road bus employees, including individuals with disabilities and the elderly.

(6) Psychology, behavior, and methods of terrorists, including observation and analysis.

(7) Training related to psychological responses to terrorist incidents, including the ability to cope with hijacker behavior and passenger responses.

(8) Live situational training exercises regarding various threat conditions, including tunnel evacuation procedures.

(9) Recognition and reporting of dangerous substances, suspicious packages, and situations.

(10) Understanding security incident procedures, including procedures for communicating with emergency response providers and for on-scene interaction with emergency response providers.

(11) Operation and maintenance of security equipment and systems.

(12) Other security training activities that the Secretary considers appropriate.

(d) REQUIRED PROGRAMS.—

(1) DEVELOPMENT AND SUBMISSION TO SECRETARY.—Not later than 90 days after the Secretary issues the regulations under subsection (a), each over-the-road bus operator shall develop a security training program in accordance with the regulations and submit the program to the Secretary for approval.

(2) APPROVAL.—Not later than 60 days after receiving a security training program proposal under this subsection, the Secretary shall approve the program or require the over-the-road bus operator that developed the program to make revisions to the program that the Secretary considers necessary for the program to meet the requirements of the regulations. An over-the-road bus operator shall respond to the Secretary's comments not later than 30 days after receiving them.

(3) TRAINING.—Not later than 1 year after the Secretary approves a security training program under this subsection, the over-the-road bus operator that developed the program shall complete the training of all over-the-road bus frontline employees who were hired by the operator more than 30 days preceding the approval date. For employees employed by an operator for fewer than 30 days preceding the approval date, training shall be completed within the first 60 days of employment.

(4) UPDATES OF REGULATIONS AND PROGRAM REVISIONS.—The Secretary shall periodically review and update, as appropriate, the training regulations issued under subsection (a) to reflect new or changing security threats. Each over-the-road bus operator shall revise its training program accordingly and provide additional training as necessary to its employees within a reasonable time after the regulations are updated.

(e) NATIONAL TRAINING PROGRAM.—The Secretary shall ensure that the training program developed under subsection (a) is a component of the national training program established under section 20508 of this title.

§ 40765. Research and development

(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology and the Administrator of the Transportation

Security Administration, shall carry out a research and development program for the purpose of improving the security of over-the-road buses.

(b) ELIGIBLE PROJECTS.—The research and development program may include projects—

(1) to reduce the vulnerability of over-the-road buses, stations, terminals, and equipment to explosives and hazardous chemical, biological, and radioactive substances, including the development of technology to screen passengers in large numbers with minimal interference and disruption;

(2) to test new emergency response and recovery techniques and technologies, including those used at international borders;

(3) to develop improved technologies, including those for—

(A) emergency response training, including training in a tunnel environment, if appropriate; and

(B) security and redundancy for critical communications, electrical power, computer, and over-the-road bus control systems; and

(4) to address other vulnerabilities and risks identified by the Secretary.

(c) COORDINATION WITH OTHER RESEARCH INITIATIVES.—The Secretary—

(1) shall ensure that the research and development program is consistent with the other transportation security research and development programs required by section 30304 and chapters 401 through 407 of this title;

(2) shall, to the extent practicable, coordinate the research and development activities of the Department with other ongoing research and development security-related initiatives, including research being conducted by—

(A) the Department of Transportation, including University Transportation Centers and other institutes, centers, and simulators funded by the Department of Transportation;

(B) the National Academy of Sciences;

(C) the Technical Support Working Group;

(D) other Federal departments and agencies; and

(E) other Federal and private research laboratories, research entities, and institutions of higher education, including Historically Black Colleges and Universities, Hispanic-serving institutions, and Indian tribally controlled colleges and universities;

(3) shall carry out a research and development project authorized by this section through a reimbursable agreement with an appropriate Federal agency, if the agency—

(A) is currently sponsoring a research and development project in a similar area; or

(B) has a unique facility or capability that would be useful in carrying out the project;

(4) may award grants to, and enter into cooperative agreements, contracts, other transactions, or reimbursable agreements with, the entities described in paragraph (2) and eligible recipients under section 40762 of this title; and

(5) shall make reasonable efforts to enter into memoranda of understanding, contracts, grants, cooperative agreements, or other transactions with private operators providing over-the-road bus transportation willing to contribute assets, physical space, and other resources.

(d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES.—

(1) CONSULTATION.—In carrying out research and development projects under this section, the Secretary shall consult with the Chief Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department as appropriate and under section 10520 of this title.

(2) PRIVACY IMPACT ASSESSMENTS.—In accordance with sections 10520 and 11705 of this title, the Chief Privacy Officer shall conduct privacy impact assessments, and the Officer for Civil Rights and Civil Liberties shall conduct reviews, as appropriate, of research and development initiatives developed under this section that the Secretary determines could have an impact on privacy, civil rights, or civil liberties.

Subchapter IV—Hazardous Material and Pipeline Security

§ 40781. Railroad routing of security-sensitive materials

(a) DEFINITIONS.—In this section:

(1) HIGH-CONSEQUENCE TARGET.—The term ''high-consequence target'' means a property, natural resource, location, area, or other target designated by the Secretary that is a viable terrorist target of national significance, which may include a facility or specific critical infrastructure, the attack of which by railroad could result in—

(A) catastrophic loss of life;

(B) significant damage to national security or defense capabilities; or

(C) national economic harm.

(2) ROUTE.—The term ''route'' includes storage facilities and trackage used by railroad cars in transportation in commerce.

(b) SECURITY-SENSITIVE MATERIALS COMMODITY DATA.—The Secretary of Transportation shall ensure that the final rule published as provided in

section 1551(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 469) requires each railroad carrier transporting security-sensitive materials in commerce to, no later than 90 days after the end of each calendar year, compile security-sensitive materials commodity data. The data must be collected by route, line segment, or series of line segments, as aggregated by the railroad carrier. Within the railroad-carrier-selected route, the commodity data must identify the geographic location of the route and the total number of shipments by the United Nations identification number for the security-sensitive materials.

(c) RAILROAD TRANSPORTATION ROUTE ANALYSIS FOR SECURITY-SENSITIVE MATERIALS.—The Secretary of Transportation shall ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to, for each calendar year, provide a written analysis of the safety and security risks for the transportation routes identified in the security-sensitive materials commodity data collected as required by subsection (b). The safety and security risks present shall be analyzed for the route, railroad facilities, railroad storage facilities, and high-consequence targets along or in proximity to the route.

(d) ALTERNATIVE ROUTE ANALYSIS FOR SECURITY-SENSITIVE MATERIALS.—The Secretary of Transportation shall ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to—

(1) for each calendar year—

(A) identify practicable alternative routes over which the railroad carrier has authority to operate as compared to the current route for a shipment analyzed under subsection (c); and

(B) perform a safety and security risk assessment of the alternative route for comparison to the route analysis specified in subsection (c);

(2) ensure that the analysis under paragraph (1) includes—

(A) identification of safety and security risks for an alternative route;

(B) comparison of those risks identified under subparagraph (A) to the primary railroad transportation route, including the risk of a catastrophic release from a shipment traveling along the alternate route compared to the primary route;

(C) remediation or mitigation measures implemented on the primary or alternative route; and

(D) potential economic effects of using an alternative route; and

(3) consider when determining the practicable alternative routes under paragraph (1)(A) the use of interchange agreements with other railroad carriers.

(e) ALTERNATIVE ROUTE SELECTION FOR SECURITY-SENSITIVE MATERIALS.—The Secretary of Transportation shall ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to use the analyses required by subsections (c) and (d) to select the safest and most secure route to be used in transporting security-sensitive materials.

(f) REVIEW.—The Secretary of Transportation shall ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to annually review and select the practicable route posing the least overall safety and security risk under this section. The railroad carrier must retain in writing all route review and selection decision documentation and restrict the distribution, disclosure, and availability of information contained in the route analysis to appropriate persons. This documentation should include, but is not limited to, comparative analyses, charts, graphics, or railroad system maps.

(g) RETROSPECTIVE ANALYSIS.—The Secretary of Transportation shall ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to, not less than once every 3 years, analyze the route selection determinations required under this section. The analysis shall include a comprehensive, system-wide review of all operational changes, infrastructure modifications, traffic adjustments, changes in the nature of high-consequence targets located along or in proximity to the route, or other changes affecting the safety and security of the movements of security-sensitive materials that were implemented since the previous analysis was completed.

(h) CONSULTATION.—In carrying out subsection (c), railroad carriers transporting security-sensitive materials in commerce shall seek relevant information from State, local, and tribal officials, as appropriate, regarding security risks to high-consequence targets along or in proximity to a route used by a railroad carrier to transport security-sensitive materials.

§ 40782. Railroad security-sensitive material tracking

(a) IN GENERAL.—In conjunction with the research and development program established under section 40747 of this title and consistent with the results of research relating to wireless and other tracking technologies, the Secretary, in consultation with the Administrator of the Transportation Security Administration, shall develop a program that will encourage the equipping of railroad cars transporting security-sensitive materials, as defined in section 40701 of this title, with technology that provides—

(1) car position location and tracking capabilities; and

(2) notification of railroad car depressurization, breach, unsafe temperature, or release of hazardous materials, as appropriate.

(b) COORDINATION.—In developing the program required by subsection (a), the Secretary shall—

(1) consult with the Secretary of Transportation to coordinate the program with ongoing or planned efforts for railroad car tracking at the Department of Transportation; and

(2) ensure that the program is consistent with recommendations and findings of the Department of Homeland Security's hazardous material railroad tank car tracking pilot programs.

§ 40783. Motor carrier security-sensitive material tracking

(a) COMMUNICATIONS.—

(1) IN GENERAL.—Consistent with the findings of the Transportation Security Administration's hazardous materials truck security pilot program, the Secretary, through the Administrator of the Transportation Security Administration and in consultation with the Secretary of Transportation, shall develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials and to equip vehicles used in the shipments with technology that provides—

(A) frequent or continuous communications;

(B) vehicle position location and tracking capabilities; and

(C) a feature that allows a driver of the vehicles to broadcast an emergency distress signal.

(2) CONSIDERATIONS.—In developing the program required by paragraph (1), the Secretary shall—

(A) consult with the Secretary of Transportation to coordinate the program with ongoing or planned efforts for motor carrier or security-sensitive materials tracking at the Department of Transportation;

(B) take into consideration the recommendations and findings of the report on the hazardous material safety and security operational field test released by the Federal Motor Carrier Safety Administration on November 11, 2004; and

(C) evaluate—

(i) new information related to the costs and benefits of deploying, equipping, and utilizing tracking technology, including portable tracking technology, for motor carriers transporting security-sensitive materials not included in the hazardous material safety and security operational field test re-

port released by the Federal Motor Carrier Safety Administration on November 11, 2004;

(ii) the ability of tracking technology to resist tampering and disabling;

(iii) the capability of tracking technology to collect, display, and store information regarding the movement of shipments of security-sensitive materials by commercial motor vehicles;

(iv) the appropriate range of contact intervals between the tracking technology and a commercial motor vehicle transporting security-sensitive materials;

(v) technology that allows the installation by a motor carrier of concealed electronic devices on commercial motor vehicles that can be activated by law enforcement authorities to disable the vehicle or alert emergency response resources to locate and recover security-sensitive materials in the event of loss or theft of the materials;

(vi) whether installation of the technology described in clause (v) should be incorporated into the program under paragraph (1);

(vii) the costs, benefits, and practicality of the technology described in clause (v) in the context of the overall benefit to national security, including commerce in transportation; and

(viii) other systems and information that the Secretary determines appropriate.

(b) LIMITATION.—The Secretary may not mandate the installation or utilization of a technology described under this section without additional congressional authority provided after August 3, 2007.

§ 40784. Use of transportation security card in hazmat licensing

(a) BACKGROUND CHECK.—An individual who has a valid transportation employee identification card issued by the Secretary under section 70105 of title 46 is deemed to have met the background records check required under section 5103a of title 49.

(b) STATE REVIEW.—Nothing in this section prevents or preempts a State from conducting a criminal records check of an individual who has applied for a license to operate a motor vehicle transporting in commerce a hazardous material.

§ 40785. Pipeline security inspections and enforcement

(a) IN GENERAL.—Consistent with the Annex to the Memorandum of Understanding executed on August 9, 2006, between the Department of Transportation and the Department, the Secretary, in consultation with the

Secretary of Transportation, shall establish a program for reviewing pipeline operator adoption of recommendations of the September 5, 2002, Department of Transportation Research and Special Programs Administration's Pipeline Security Information Circular, including the review of pipeline security plans and critical facility inspections.

(b) REVIEW AND INSPECTION.—The Secretary and the Secretary of Transportation shall develop and implement a plan for reviewing the pipeline security plans and for inspecting the critical facilities of the 100 most critical pipeline operators covered by the September 5, 2002, circular, where the facilities have not been inspected for security purposes since September 5, 2002, by either the Department or the Department of Transportation.

(c) COMPLIANCE REVIEW METHODOLOGY.—In reviewing pipeline operator compliance under subsections (a) and (b), the Secretary and the Secretary of Transportation shall use risk assessment methodologies to prioritize risks and to target inspection and enforcement actions to the highest risk pipeline assets.

(d) REGULATIONS.—The Secretary and the Secretary of Transportation shall develop and transmit to pipeline operators security recommendations for natural gas and hazardous liquid pipelines and pipeline facilities. If the Secretary determines that regulations are appropriate, the Secretary shall consult with the Secretary of Transportation on the extent of risk and appropriate mitigation measures, and the Secretary or the Secretary of Transportation, consistent with the Annex to the Memorandum of Understanding executed on August 9, 2006, shall promulgate regulations and carry out necessary inspection and enforcement actions. Regulations shall incorporate the guidance provided to pipeline operators by the September 5, 2002, Department of Transportation Research and Special Programs Administration's Pipeline Security Information Circular and contain additional requirements as necessary based upon the results of the inspections performed under subsection (b). The regulations shall include the imposition of civil penalties for noncompliance.

§ 40786. Pipeline security and incident recovery plan

(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Transportation and the Administrator of the Pipeline and Hazardous Materials Safety Administration, and in accordance with the Annex to the Memorandum of Understanding executed on August 9, 2006, the National Strategy for Transportation Security, and Homeland Security Presidential Directive–7, shall develop a pipeline security and incident recovery protocols plan. The plan shall include—

(1) a security plan for the Government to provide increased security support to the most critical interstate and intrastate natural gas and

hazardous liquid transmission pipeline infrastructure and operations as determined under section 40785 of this title when—

(A) the pipeline infrastructure or operations are under severe security threat levels of alert; or

(B) specific security threat information relating to the pipeline infrastructure or operations exists; and

(2) an incident recovery protocol plan, developed in conjunction with interstate and intrastate transmission and distribution pipeline operators and terminals and facilities operators connected to pipelines, to develop protocols to ensure the continued transportation of natural gas and hazardous liquids to essential markets and for essential public health or national defense uses in the event of an incident affecting the interstate and intrastate natural gas and hazardous liquid transmission and distribution pipeline system, including protocols for restoring essential services supporting pipelines and granting access to pipeline operators for pipeline infrastructure repair, replacement, or bypass following an incident.

(b) EXISTING PRIVATE- AND PUBLIC-SECTOR EFFORTS.—The plan shall take into account actions taken or planned by both private and public entities to address identified pipeline security issues and assess the effective integration of the actions.

(c) CONSULTATION.—In developing the plan under subsection (a), the Secretary shall consult with the Secretary of Transportation, interstate and intrastate transmission and distribution pipeline operators, nonprofit employee organizations representing pipeline employees, emergency responders, offerors, State pipeline safety agencies, public safety officials, and other relevant parties.

Chapter 409—Air Transportation Security

Sec.

Subchapter I—General

§ 40901. Definitions

(a) TITLE 49 DEFINITIONS.—Unless otherwise specifically provided, the definitions in section 40102 of title 49 apply to this chapter.

(b) ADMINISTRATOR.—In this chapter, the term ''Administrator'' means the Administrator of the Transportation Security Administration.

Subchapter II—Requirements

§ 40911. Screening passengers and property

(a) IN GENERAL.—The Administrator shall provide for the screening of all passengers and property, including United States mail, cargo, carry-on and checked baggage, and other articles, that will be carried aboard a passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation. In the case of flights and flight segments originating in the United States, the screening shall take place before boarding and shall be carried out by a Federal Government employee (as defined in section 2105 of title 5), except as otherwise provided in section 40931 of this title and except for identifying passengers and baggage for screening under the CAPPS and known shipper programs and conducting positive bag-match programs.

(b) SUPERVISION OF SCREENING.—All screening of passengers and property at airports in the United States where screening is required under this section shall be supervised by uniformed Federal personnel of the Transpor-

tation 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 in place at an airport, all checked baggage at the airport is screened by those systems;

(B) all systems deployed under subparagraph (A) are fully utilized; and

(C) if explosives detection equipment at an airport is unavailable, all checked baggage is screened by an alternative means.

(2) PRECLEARANCE AIRPORTS.—

(A) DEFINITION OF AVIATION SECURITY PRECLEARANCE AGREEMENT.—In this paragraph, the term ''aviation security preclearance agreement'' means an agreement that delineates and implements security standards and protocols that are determined by the Administrator, in coordination with U.S. Customs and Border Protection, to be comparable to those of the United States and therefore sufficiently effective to enable passengers to deplane into sterile areas of airports in the United States.

(B) IN GENERAL.—For a flight or flight segment originating at an airport outside the United States and traveling to the United States with respect to which checked baggage has been screened in accordance with an aviation security preclearance agreement between the United States and the country in which the airport is located, the Administrator may, in coordination with U.S. Customs and Border Protection, determine whether the baggage must be re-screened in the United States by an explosives detection system before the baggage continues on any additional flight or flight segment.

(C) RE-SCREENING REQUIREMENT.—If the Administrator determines that the government of a foreign country has not maintained security standards and protocols comparable to those of the United States at airports at which preclearance operations have

been established in accordance with this paragraph, the Administrator shall ensure that Transportation Security Administration personnel re-screen passengers arriving from those airports and their property in the United States before the passengers are permitted into sterile area of airports in the United States.

(D) REPORT.—The Administrator shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, and the Committee on Homeland Security and Governmental Affairs of the Senate an annual report on the re-screening of baggage under this paragraph. Each report shall include the following for the year covered by the report:

(i) A list of airports outside the United States from which a flight or flight segment traveled to the United States for which the Administrator determined, in accordance with the authority under subparagraph (B), that checked baggage was not required to be re-screened in the United States by an explosives detection system before the baggage continued on an additional flight or flight segment.

(ii) The amount of Federal savings generated from the exercise of the authority.

(e) ONE-STOP PILOT PROGRAM

(1)DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, the term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Committee on Foreign Affairs of the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on Foreign Relations of the Senate.

(2)IMPLEMENTATION.—Notwithstanding subsection (a), the Administrator, in coordination with the Commissioner of U.S. Customs and Border Protection and the Secretary of State, may implement a pilot program at not more than 6 foreign last point of departure airports to permit passengers and their accessible property arriving on direct flights or flight segments originating at those participating foreign airports to continue on additional flights or flight segments originating in the United States without additional security re-screening if—

(A) the initial screening was conducted in accordance with an aviation security screening agreement described in paragraph (5);

(B) passengers arriving from participating foreign airports are unable to access their checked baggage until the arrival at their final destination; and

(C) on arrival in the United States, passengers arriving from participating foreign airports do not come into contact with other arriving international passengers, those passengers' property, or other individuals who have not been screened or subjected to other appropriate security controls required for entry into the airport's sterile area.

(3)REQUIREMENTS.—In carrying out this subsection, the Administrator shall ensure that there is no reduction in the level of security or specific Transportation Security Administration aviation security standards or requirements for screening passengers and their property prior to boarding an international flight bound for the United States, including specific aviation security standards and requirements regarding the following:

(A) High risk passengers and their property.

(B) Weapons, explosives, and incendiaries.

(C) Screening passengers and property transferring at a foreign last point of departure airport from another airport and bound for the United States, and addressing any commingling of the passengers and property with passengers and property screened under the pilot program described in paragraph (2).

(D) Insider risk at foreign last point of departure airports.

(4)RE-SCREENING OF CHECKED BAGGAGE.—Subject to paragraph (6), the Administrator may determine whether checked baggage arriving from participating foreign airports referenced in paragraph (2) that screen using an explosives detection system must be re-screened in the United States by an explosives detection system before the baggage continues on any additional flight or flight segment.

(5)AVIATION SECURITY SCREENING AGREEMENT.—

(A)IN GENERAL.—An aviation security screening agreement described in this paragraph is a treaty, executive agreement, or non-binding instrument entered into with a foreign country that delineates and implements security standards and protocols utilized at a foreign last point of departure airport that are determined by the Administrator—

(i) to be comparable to those of the United States; and

(ii) sufficiently effective to enable passengers and their accessible property to deplane into sterile areas of airports in the United States without the need for re-screening.

(B)NON-DELEGATION.—The authority to approve an aviation security screening agreement may not be delegated below the level of the Secretary of State, the Secretary, or the Administrator.

(6)RE-SCREENING REQUIREMENT.—

(A)IN GENERAL.—If the Administrator determines that a foreign country participating in the aviation security screening agreement has not maintained and implemented security standards and protocols comparable to those of the United States at foreign last point of departure airports at which a pilot program has been established in accordance with this subsection, the Administrator shall ensure that passengers and their property arriving from those airports are re-screened in the United States, including by using explosives detection systems in accordance with subsection (d) and implementing regulations and directives, before the passengers and their property are permitted into sterile areas of airports in the United States.

(B)CONSULTATION.—If the Administrator has reasonable grounds to believe the other party to an aviation security screening agreement has not complied with the agreement, the Administrator shall request immediate consultation with the party.

(C)SUSPENSION OR TERMINATION OF AGREEMENT.—If a satisfactory resolution between the Transportation Security Administration and a foreign country is not reached within 45 days after a consultation request under subparagraph (B) or in the case of the foreign country's continued or egregious failure to maintain the security standards and protocols described in subparagraph (A), the President, or with the concurrence of the Secretary of State, the Secretary, or the Administrator, as appropriate, shall suspend or terminate the aviation security screening agreement with the country, as determined appropriate by the President, the Secretary, or the Administrator. The Administrator shall notify the appropriate congressional committees of the consultation and suspension or termination, not later than 7 days after the consultation and suspension or termination.

(7)BRIEFINGS TO CONGRESS.—Not later than 45 days before an aviation security screening agreement described in paragraph (5) enters into force, the Administrator, in coordination with the Secretary of State, shall submit to the appropriate congressional committees the following:

(A) An aviation security threat assessment for the country in which the foreign last point of departure airport is located.

(B) Information regarding any corresponding mitigation efforts to address any security issues identified in the threat assessment, including any plans for joint covert testing.

(C) Information on potential security vulnerabilities associated with commencing a pilot program at the foreign last point of departure airport pursuant to paragraph (2) and mitigation plans to address the potential security vulnerabilities.

(D) An assessment of the impacts the pilot program will have on aviation security.

(E) An assessment of the screening performed at the foreign last point of departure airport, including the feasibility of Transportation Security Administration personnel monitoring screening, security protocols, and standards.

(F) Information regarding identifying the entity responsible for screening passengers and property at the foreign last point of departure airport.

(G) The name of the entity or local authority and any contractor or subcontractor.

(H) Information regarding the screening requirements relating to the aviation security screening agreement.

(I) Details regarding information sharing mechanisms between the Transportation Security Administration and the foreign last point of departure airport, screening authority, or entity responsible for screening provided for under the aviation security screening agreement.

(J) A copy of the aviation security screening agreement, which shall identify the foreign last point of departure airports at which a pilot program under this section is to be established.

(8)CERTIFICATIONS.—For each aviation security screening agreement described in paragraph (5), the Administrator, in coordination with the Secretary of State, shall submit to the appropriate congressional committees the following:

(A)(i) A certification that the agreement satisfies all of the requirements specified in paragraph (3); or

(ii) in the event that one or more of the requirements are not so satisfied, a description of the unsatisfied requirements and information on what actions the Administrator will take to ensure that the remaining requirements are satisfied before the agreement enters into force.

(B) A certification that the Transportation Security Administration and U.S. Customs and Border Protection have ensured that

any necessary physical modifications or appropriate mitigations exist in the domestic one-stop security pilot program airport prior to receiving international passengers from a last point of departure airport under the aviation security screening agreement.

(C) A certification that a foreign last point of departure airport covered by an aviation security screening agreement has an operation to screen all checked bags as required by law, regulation, or international agreement, including the full utilization of explosives detection systems to the extent applicable.

(D) A certification that the Administrator consulted with stakeholders, including air carriers, aviation nonprofit labor organizations, airport operators, relevant interagency partners, and other stakeholders that the Administrator determines appropriate.

(9)REPORT TO CONGRESS.—Not later than December 23, 2027, the Secretary, in coordination with the Administrator, shall submit to the appropriate congressional committees a report regarding the implementation of the pilot program authorized under this subsection, including information relating to the following:

(A) The impact of the program on homeland security and international aviation security, including any benefits and challenges of the program.

(B) The impact of the program on passengers, airports, and air carriers, including any benefits and challenges of the program.

(C) The impact and feasibility of continuing the program or expanding it into a more permanent program, including any benefits and challenges of the continuation or expansion.

(10)RULE OF CONSTRUCTION.—Nothing in this subsection may be construed as limiting the authority of U.S. Customs and Border Protection to inspect persons and baggage arriving in the United States in accordance with applicable law.

(11)SUNSET.—The pilot program authorized under this subsection shall terminate on December 23, 2028.

(f) CARGO DEADLINE.—A system must be in operation to screen, inspect, or otherwise ensure the security of all cargo that is to be transported in all-cargo aircraft in air transportation and intrastate air transportation as soon as practicable.

(g) AIR CARGO ON PASSENGER AIRCRAFT.—

(1) DEFINITION OF SCREENING.—In this subsection, the term ''screening'' means a physical examination or nonintrusive methods of assessing whether cargo poses a threat to transportation security, including x-ray systems, explosives detection systems, explosives trace de-

tection, explosives detection canine teams certified by the Transportation Security Administration, or a physical search together with manifest verification.

(2) IN GENERAL.—The Secretary shall establish a system to screen 100 percent of cargo transported on passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation to ensure the security of all passenger aircraft carrying cargo.

(3) MINIMUM STANDARDS.—The system referred to in paragraph (2) shall require, at a minimum, that equipment, technology, procedures, personnel, or other methods approved by the Administrator, are used to screen cargo carried on passenger aircraft described in paragraph (2) to provide a level of security commensurate with the level of security for the screening of passenger checked baggage.

(4) ADDITIONAL CARGO SCREENING METHODS.—

(A) IN GENERAL.—The Administrator may approve additional methods to ensure that the cargo does not pose a threat to transportation security and to assist in meeting the requirements of this subsection.

(B) MINIMUM REQUIREMENTS.—The additional cargo screening methods shall not include solely performing a review of information about the contents of cargo or verifying the identity of a shipper of the cargo that is not performed in conjunction with other security methods authorized under this subsection, including whether a known shipper is registered in the known shipper database.

(C) CERTIFICATION PROGRAM.—The additional cargo screening methods may include a program to certify the security methods used by shippers under paragraphs (2) and (3) and alternative screening methods pursuant to exemptions referred to in subsection (b) of section 1602 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53, 121 Stat. 479).

(5) REGULATIONS.—The Secretary shall issue a final rule as a permanent regulation to implement this subsection in accordance with chapter 5 of title 5.

(h) DEPLOYMENT OF ARMED LAW ENFORCEMENT PERSONNEL.—

(1) IN GENERAL.—The Administrator shall order the deployment of law enforcement personnel authorized to carry firearms at each airport security screening location to ensure passenger safety and national security.

(2) MINIMUM REQUIREMENTS.—Except at airports required to enter into agreements under subsection (c), the Administrator shall order the deployment of at least one law enforcement officer at each airport security screening location. At the 100 largest airports in the United States, in terms of annual passenger enplanements for the most recent calendar year for which data are available, the Secretary shall order the deployment of additional law enforcement personnel at airport security screening locations if the Administrator determines that the additional deployment is necessary to ensure passenger safety and national security.

(i) EXEMPTIONS AND ADVISING CONGRESS ON REGULATIONS.—The Administrator—

(1) may exempt from this section air transportation operations, except scheduled passenger operations of an air carrier providing air transportation under a certificate issued under section 41102 of title 49 or a permit issued under section 41302 of title 49; and

(2) shall advise Congress of a regulation to be prescribed under this section at least 30 days before the effective date of the regulation, unless the Administrator decides an emergency exists requiring the regulation to become effective in fewer than 30 days and notifies Congress of that decision.

(j) BLAST-RESISTANT CARGO CONTAINERS.—

(1) IN GENERAL.—The Administrator shall—

(A) evaluate the results of the blast-resistant cargo container pilot program that was initiated before August 3, 2007; and

(B) prepare and distribute through the Aviation Security Advisory Committee to the appropriate committees of Congress and air carriers a report on that evaluation, which may contain nonclassified and classified sections.

(2) ACQUISITION, MAINTENANCE, AND REPLACEMENT.—On completion and consistent with the results of the evaluation that paragraph (1)(A) requires, the Administrator shall—

(A) develop and implement a program, as the Administrator determines appropriate, to acquire, maintain, and replace blast-resistant cargo containers;

(B) pay for the program; and

(C) make available blast-resistant cargo containers to air carriers under paragraph (3).

(3) DISTRIBUTION TO AIR CARRIERS.—The Administrator shall make available blast-resistant cargo containers to air carriers for use on a risk-managed basis as determined by the Secretary.

(k) GENERAL AVIATION AIRPORT SECURITY PROGRAM.—

(1) IN GENERAL.—The Administrator shall—

(A) develop a standardized threat and vulnerability assessment program for general aviation airports; and

(B) implement a program to perform the assessments on a risk-managed basis at general aviation airports.

(2) GRANT PROGRAM.—The Administrator shall complete a study of the feasibility of a program, based on a risk-managed approach, to provide grants to operators of general aviation airports for projects to upgrade security at the airports. If the Secretary determines that a program is feasible, the Secretary shall establish a program.

(3) REQUIRED SUBMISSIONS BY GENERAL AVIATION AIRCRAFT.—The Administrator shall develop a risk-based system under which—

(A) general aviation aircraft, as identified by the Administrator, in coordination with the Administrator of the Federal Aviation Administration, are required to submit passenger information and advance notification requirements for U. S. Customs and Border Protection before entering United States airspace; and

(B) the information is checked against appropriate databases.

(l) LIMITATIONS ON USE OF ADVANCED IMAGING TECHNOLOGY FOR SCREENING PASSENGERS.—

(1) DEFINITIONS.—In this subsection:

(A) ADVANCED IMAGING TECHNOLOGY.—The term ''advanced imaging technology''—

(i) means a device used in the screening of passengers that creates a visual image of an individual showing the surface of the skin and revealing other objects on the body; and

(ii) may include devices using backscatter x-rays or millimeter waves and devices referred to as ''whole-body imaging technology'' or ''body scanning machines''.

(B) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(i) the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(ii) the Committee on Homeland Security of the House of Representatives.

(C) AUTOMATIC TARGET RECOGNITION SOFTWARE.—The term ''automatic target recognition software'' means software installed on an advanced imaging technology that produces a generic image

of the individual being screened that is the same as the images produced for all other screened individuals.

(2) USE OF ADVANCED IMAGING TECHNOLOGY.—The Administrator shall ensure that an advanced imaging technology used for the screening of passengers under this section—

(A) is equipped with and employs automatic target recognition software; and

(B) complies with other requirements the Administrator determines necessary to address privacy considerations.

§ 40912. Refusal to transport passengers and property

(a) MANDATORY REFUSAL.—The Administrator shall prescribe regulations requiring an air carrier, intrastate air carrier, or foreign air carrier to refuse to transport—

(1) a passenger who does not consent to a search under section 40911(a) of this title establishing whether the passenger is carrying unlawfully a dangerous weapon, explosive, or other destructive substance; or

(2) property of a passenger who does not consent to a search of the property establishing whether the property unlawfully contains a dangerous weapon, explosive, or other destructive substance.

(b) PERMISSIVE REFUSAL.—Subject to regulations of the Administrator, an air carrier, intrastate air carrier, or foreign air carrier may refuse to transport a passenger or property the carrier decides is, or might be, inimical to safety.

(c) AGREEING TO CONSENT TO SEARCH.—An agreement to carry passengers or property in air transportation or intrastate air transportation by an air carrier, intrastate air carrier, or foreign air carrier is deemed to include an agreement that the passenger or property will not be carried if consent to search the passenger or property for a purpose referred to in this section is not given.

§ 40913. Air transportation security

(a) DEFINITION OF LAW ENFORCEMENT PERSONNEL.—In this section, ''law enforcement personnel'' means individuals—

(1) authorized to carry and use firearms;

(2) vested with the degree of the police power of arrest the Administrator considers necessary to carry out this section; and

(3) identifiable by appropriate indicia of authority.

(b) PROTECTION AGAINST VIOLENCE AND PIRACY.—The Administrator shall prescribe regulations to protect passengers and property on an aircraft operating in air transportation or intrastate air transportation against an

act of criminal violence or aircraft piracy. When prescribing a regulation under this subsection, the Administrator shall—

(1) consult with the Secretary of Transportation, the Attorney General, the heads of other departments, agencies, and instrumentalities of the United States Government, and State and local authorities;

(2) consider whether a proposed regulation is consistent with—

(A) protecting passengers; and

(B) the public interest in promoting air transportation and intrastate air transportation;

(3) to the maximum extent practicable, require a uniform procedure for searching and detaining passengers and property to ensure—

(A) their safety; and

(B) courteous and efficient treatment by an air carrier, an agent or employee of an air carrier, and Government, State, and local law enforcement personnel carrying out this section; and

(4) consider the extent to which a proposed regulation will carry out this section.

(c) SECURITY PROGRAMS.—

(1) IN GENERAL.—The Administrator shall prescribe regulations under subsection (b) that require each operator of an airport regularly serving an air carrier holding a certificate issued by the Secretary of Transportation to establish an air transportation security program that provides a law enforcement presence and capability at each of those airports that is adequate to ensure the safety of passengers. The regulations shall authorize the operator to use the services of qualified State, local, and private law enforcement personnel. When the Administrator decides, after being notified by an operator in the form the Administrator prescribes, that not enough qualified State, local, and private law enforcement personnel are available to carry out subsection (b), the Administrator may authorize the operator to use, on a reimbursable basis, personnel employed by the Administrator, or by another department, agency, or instrumentality of the Government with the consent of the head of the department, agency, or instrumentality, to supplement State, local, and private law enforcement personnel. When deciding whether additional personnel are needed, the Administrator shall consider the number of passengers boarded at the airport, the extent of anticipated risk of criminal violence or aircraft piracy at the airport or to the air carrier aircraft operations at the airport, and the availability of qualified State or local law enforcement personnel at the airport.

(2) INCLUSION OF AIRPORT TENANT SECURITY PROGRAM.—

(A) IN GENERAL.—The Administrator may approve a security program of an airport operator, or an amendment to an existing program, that incorporates a security program of an airport tenant (except an air carrier separately complying with part 108 or 129 of title 14, Code of Federal Regulations) having access to a secured area of the airport, if the program or amendment incorporates—

(i) the measures the tenant will use, within the tenant's leased areas or areas designated for the tenant's exclusive use under an agreement with the airport operator, to carry out the security requirements imposed by the Administrator on the airport operator under the access control system requirements of section 107.14 of title 14, Code of Federal Regulations, or under other requirements of part 107 of title 14; and

(ii) the methods the airport operator will use to monitor and audit the tenant's compliance with the security requirements and provides that the tenant will be required to pay monetary penalties to the airport operator if the tenant fails to carry out a security requirement under a contractual provision or requirement imposed by the airport operator.

(B) OPERATOR NOT IN VIOLATION.—If the Administrator approves a program or amendment described in subparagraph (A), the airport operator may not be found to be in violation of a requirement of this subsection or subsection (b) when the airport operator demonstrates that the tenant or an employee, permittee, or invitee of the tenant is responsible for the violation and that the airport operator has complied with all measures in its security program for securing compliance with its security program by the tenant.

(C) MAXIMUM USE OF CHEMICAL AND BIOLOGICAL WEAPONS DETECTION EQUIPMENT.—The Secretary of Transportation may require airports to maximize the use of technology and equipment that is designed to detect or neutralize potential chemical or biological weapons.

(3) PILOT PROGRAMS.—The Administrator shall establish pilot programs in no fewer than 20 airports to test and evaluate new and emerging technology for providing access control and other security protections for closed or secure areas of the airports. The technology may include biometric or other technology that ensures only authorized access to secure areas.

(d) AUTHORIZING INDIVIDUALS TO CARRY FIREARMS AND MAKE ARRESTS.—With the approval of the Attorney General and the Secretary of State, the Administrator may authorize an individual who carries out air transportation security duties—

(1) to carry firearms; and

(2) to make arrests without warrant for an offense against the United States committed in the presence of the individual or for a felony under the laws of the United States, if the individual reasonably believes the individual to be arrested has committed or is committing a felony.

(e) EXCLUSIVE RESPONSIBILITY OVER PASSENGER SAFETY.—The Administrator has the exclusive responsibility to direct law enforcement activity related to the safety of passengers on an aircraft involved in an offense under section 41062 of this title from the moment all external doors of the aircraft are closed following boarding until those doors are opened to allow passengers to leave the aircraft. When requested by the Administrator, other departments, agencies, and instrumentalities of the Government shall provide assistance necessary to carry out this subsection.

(f) GOVERNMENT AND INDUSTRY CONSORTIA.—The Administrator may establish at airports consortia of government and aviation industry representatives to provide advice on matters related to aviation security and safety. The consortia shall not be considered Federal advisory committees for purposes of chapter 10 of title 5.

(g) IMPROVEMENT OF SECURED-AREA ACCESS CONTROL.—

(1) EMPLOYEE SANCTIONS.—

(A) PUBLICATION.—The Administrator shall publish in the Federal Register a list of sanctions for use as guidelines in the discipline of employees for infractions of airport access control requirements.

(B) DISCIPLINARY APPROACH.—The guidelines shall incorporate a progressive disciplinary approach that relates proposed sanctions to the severity or recurring nature of the infraction and shall include measures such as remedial training, suspension from security-related duties, suspension from all duties without pay, and termination of employment.

(C) USE.—Each airport operator, air carrier, and security screening company shall include the list of sanctions published by the Administrator in its security program. The security program shall include a process for taking prompt disciplinary action against an employee who commits an infraction of airport access control requirements.

(2) ACTIONS TO IMPROVE ACCESS CONTROL.—The Administrator shall—

(A) work with airport operators and air carriers to implement and strengthen existing controls to eliminate airport access control weaknesses;

(B) require airport operators and air carriers to develop and implement comprehensive and recurring training programs that teach employees their roles in airport security, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform;

(C) require airport operators and air carriers to develop and implement programs that foster and reward compliance with airport access control requirements and discourage and penalize noncompliance in accordance with guidelines issued by the Administrator to measure employee compliance;

(D) on an ongoing basis, assess and test for compliance with access control requirements, report annually findings of the assessments, and assess the effectiveness of penalties in ensuring compliance with security procedures and take other appropriate enforcement actions when noncompliance is found;

(E) improve and better administer the Administrator's security database to ensure its efficiency, reliability, and usefulness for identification of systemic problems and allocation of resources;

(F) improve the execution of the Administrator's quality control program; and

(G) work with airport operators to strengthen access control points in secured areas (including air traffic control operations areas, maintenance areas, crew lounges, baggage handling areas, concessions, and catering delivery areas) to ensure the security of passengers and aircraft and consider the deployment of biometric or similar technologies that identify individuals based on unique personal characteristics.

(h) IMPROVED AIRPORT PERIMETER ACCESS SECURITY.—

(1) DEFINITIONS.—In this subsection:

(A) BIOMETRIC IDENTIFIER.—The term ''biometric identifier'' means a technology that enables the automated identification, or verification of the identity, of an individual based on biometric information.

(B) BIOMETRIC IDENTIFIER INFORMATION.—The term ''biometric identifier information'' means the distinct physical or behav-

ioral characteristics of an individual that are used for unique identification, or verification of the identity, of an individual.

(C) FAILURE TO ENROLL.—The term ''failure to enroll'' means the inability of an individual to enroll in a biometric identifier system due to an insufficiently distinctive biometric sample, the lack of a body part necessary to provide the biometric sample, a system design that makes it difficult to provide consistent biometric identifier information, or other factors.

(D) FALSE MATCH.—The term ''false match'' means the incorrect matching of one individual's biometric identifier information to another individual's biometric identifier information by a biometric identifier system.

(E) FALSE NON-MATCH.—The term ''false non-match'' means the rejection of a valid identity by a biometric identifier system.

(F) SECURE AREA OF AN AIRPORT.—The term ''secure area of an airport'' means the sterile area and the Security Identification Display Area of an airport (as the terms are defined in section 1540.5 of title 49, Code of Federal Regulations, or a successor regulation to that section).

(2) IN GENERAL.—The Administrator, in consultation with the airport operator and law enforcement authorities, may order the deployment of necessary personnel at a secure area of the airport to counter the risk of criminal violence, the risk of aircraft piracy at the airport, or the risk to air carrier aircraft operations at the airport, or to meet national security concerns.

(3) CONSIDERATION OF SECURITY OF AIRCRAFT AND GROUND ACCESS TO SECURE AREAS.—In determining where to deploy the personnel, the Administrator shall consider the physical security needs of air traffic control facilities, parked aircraft, aircraft servicing equipment, aircraft supplies (including fuel), automobile parking facilities within airport perimeters or adjacent to secured facilities, and access and transition areas at airports served by other means of ground or water transportation.

(4) DEPLOYMENT OF FEDERAL LAW ENFORCEMENT PERSONNEL.—The Secretary may enter into a memorandum of understanding or other agreement with the Attorney General or the head of another appropriate Federal law enforcement agency to deploy Federal law enforcement personnel at an airport in order to meet aviation safety and security concerns.

(5) AIRPORT PERIMETER SCREENING.—The Administrator shall—

(A) require screening or inspection of all individuals, goods, property, vehicles, and other equipment before entry into a secured area of an airport in the United States described in subsection (c);

(B) prescribe specific requirements for the screening and inspection that will ensure at least the same level of protection as will result from screening of passengers and their baggage;

(C) establish procedures to ensure the safety and integrity of—

(i) all persons providing services with respect to aircraft providing passenger air transportation or intrastate air transportation and facilities of those persons at an airport in the United States described in subsection (c);

(ii) all supplies, including catering and passenger amenities, placed aboard the aircraft, including the sealing of supplies to ensure easy visual detection of tampering; and

(iii) all persons providing the supplies and facilities of those persons;

(D) require vendors having direct access to the airfield and aircraft to develop security programs; and

(E) issue guidance for the use of biometric or other technology that positively verifies the identity of each employee and law enforcement officer who enters a secure area of an airport.

(6) USE OF BIOMETRIC TECHNOLOGY IN AIRPORT ACCESS CONTROL SYSTEMS.—In issuing guidance under paragraph (5)(E), the Administrator in consultation with representatives of the aviation industry, the biometric identifier industry, and the National Institute of Standards and Technology, shall establish, at a minimum—

(A) comprehensive technical and operational system requirements and performance standards for the use of biometric identifier technology in airport access control systems (including airport perimeter access control systems) to ensure that the biometric identifier systems are effective, reliable, and secure;

(B) a list of products and vendors that meet the requirements and standards set forth in subparagraph (A);

(C) procedures for implementing biometric identifier systems—

(i) to ensure that individuals do not use an assumed identity to enroll in a biometric identifier system; and

(ii) to resolve failures to enroll, false matches, and false nonmatches; and

(D) best practices for incorporating biometric identifier technology into airport access control systems in the most effective manner, including a process to best utilize existing airport access

control systems, facilities, and equipment, and existing data networks connecting airports.

(7) USE OF BIOMETRIC TECHNOLOGY FOR ARMED LAW ENFORCEMENT TRAVEL.—

(A) IN GENERAL.—The Secretary, in consultation with the Attorney General, shall—

(i) implement this paragraph by publication in the Federal Register; and

(ii) establish a national registered armed law enforcement program, that shall be federally managed, for law enforcement officers needing to be armed when traveling by commercial aircraft.

(B) PROGRAM REQUIREMENTS.—The program shall—

(i) establish a credential or a system that incorporates biometric technology and other applicable technologies;

(ii) establish a system for law enforcement officers who need to be armed when traveling by commercial aircraft on a regular basis and for those who need to be armed during temporary travel assignments;

(iii) comply with other uniform credentialing initiatives, including the Homeland Security Presidential Directive–12;

(iv) apply to all Federal, State, local, tribal, and territorial government law enforcement agencies; and

(v) establish a process by which the travel credential or system may be used to verify the identity, using biometric technology, of a Federal, State, local, tribal, or territorial law enforcement officer seeking to carry a weapon on board a commercial aircraft, without unnecessarily disclosing to the public that the individual is a law enforcement officer.

(C) PROCEDURES.—In establishing the program, the Secretary shall develop procedures—

(i) to ensure that a law enforcement officer of a Federal, State, local, tribal, or territorial government flying armed has a specific reason for flying armed and the reason is within the scope of the duties of the officer;

(ii) to preserve the anonymity of the armed law enforcement officer;

(iii) to resolve failures to enroll, false matches, and false nonmatches relating to the use of the law enforcement travel credential or system;

(iv) to determine the method of issuance of the biometric credential to law enforcement officers needing to be armed when traveling by commercial aircraft;

(v) to invalidate a law enforcement travel credential or system that is lost, stolen, or no longer authorized for use;

(vi) to coordinate the program with the Federal Air Marshal Service, including the force multiplier program of the Service; and

(vii) to implement a phased approach to launching the program, addressing the immediate needs of the relevant Federal agent population before expanding the program to other law enforcement populations.

(i) AUTHORITY TO ARM FLIGHT DECK CREW WITH LESS-THAN-LETHAL WEAPONS.—

(1) IN GENERAL.—If the Administrator, after receiving the recommendations of the National Institute of Justice, determines, with the approval of the Attorney General and the Secretary of State, that it is appropriate and necessary and would effectively serve the public interest in avoiding air piracy, the Administrator may authorize members of the flight deck crew on an aircraft providing air transportation or intrastate air transportation to carry a less-than-lethal weapon while the aircraft is engaged in providing the transportation.

(2) USAGE.—If the Administrator grants authority under paragraph (1) for flight deck crew members to carry a less-than-lethal weapon while engaged in providing air transportation or intrastate air transportation, the Administrator shall—

(A) prescribe rules requiring that the crew member be trained in the proper use of the weapon; and

(B) prescribe guidelines setting forth the circumstances under which weapons may be used.

(3) REQUEST OF AIR CARRIERS TO USE LESS-THAN-LETHAL WEAPONS.—If the Administrator receives a request from an air carrier for authorization to allow pilots of the air carrier to carry less-than-lethal weapons, the Administrator shall respond to that request within 90 days.

(j) SHORT-TERM ASSESSMENT AND DEPLOYMENT OF EMERGING SECURITY TECHNOLOGIES AND PROCEDURES.—

(1) DEFINITION OF SECURE AREA OF AN AIRPORT.—In this subsection, the term ''secure area of an airport'' means the sterile area and the Security Identification Display Area of an airport (as the

terms are defined in section 1540.5 of title 49, Code of Federal Regulations, or a successor regulation to that section).

(2) IN GENERAL.—The Administrator shall periodically recommend to airport operators commercially available measures or procedures to prevent access to secure airport areas by unauthorized persons.

(3) SECURE FLIGHT PROGRAM.—

(A) IN GENERAL.—The Administrator shall ensure that the Secure Flight Program, or a successor program—

(i) is used to evaluate all passengers before they board an aircraft; and

(ii) includes procedures to ensure that individuals selected by the program and their carry-on and checked baggage are adequately screened.

(B) MODIFICATIONS.—The Administrator may modify a requirement under the Secure Flight Program for flights that originate and terminate in the same State, if the Administrator determines that—

(i) the State has extraordinary air transportation needs or concerns due to its isolation and dependence on air transportation; and

(ii) the routine characteristics of passengers, given the nature of the market, regularly triggers primary selectee status.

(C) ADVANCED AIRLINE PASSENGER PRESCREENING.—

(i) TESTING.—The Administrator shall commence testing of an advanced passenger prescreening system that will allow the Department to assume the performance of comparing passenger information, as defined by the Administrator, to the automatic selectee and no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government.

(ii) ASSUMPTION OF PERFORMANCE.—After completion of testing under clause (i), the Administrator, or the designee of the Administrator, shall begin to assume the performance of the passenger prescreening function of comparing passenger information to the automatic selectee and no fly lists and utilize all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government in performing that function.

(iii) DUTIES IN ASSUMING PERFORMANCE.—In assuming performance of the function under clause (ii), the Administrator shall—

(I) establish a procedure to enable airline passengers, who are delayed or prohibited from boarding a flight because the advanced passenger prescreening system determined that they might pose a security threat, to appeal a determination and correct information contained in the system;

(II) ensure that Federal Government databases that will be used to establish the identity of a passenger under the system will not produce a large number of false positives;

(III) establish an internal oversight board to oversee and monitor the manner in which the system is being implemented;

(IV) establish sufficient operational safeguards to reduce the opportunities for abuse;

(V) implement substantial security measures to protect the system from unauthorized access;

(VI) adopt policies establishing effective oversight of the use and operation of the system; and

(VII) ensure that there are no specific privacy concerns with the technological architecture of the system.

(iv) REQUIREMENT TO PROVIDE PASSENGER INFORMATION.—After the completion of the testing of the advanced passenger prescreening system, the Administrator, by order or interim final rule—

(I) shall require air carriers to supply to the Administrator the passenger information needed to begin implementing the advanced passenger prescreening system; and

(II) shall require entities that provide systems and services to air carriers in the operation of air carrier reservations systems to provide to air carriers passenger information in possession of the entities, but only to the extent necessary to comply with subclause (I).

(v) INCLUSION OF DETAINEE ON NO FLY LIST.—

(I) DEFINITION OF DETAINEE.—For purposes of this clause, the term ''detainee'' means an individual in the custody or under the physical control of the United States as a result of armed conflict.

(II) IN GENERAL.—The Administrator, in coordination with the Terrorist Screening Center, shall include on the

No Fly List an individual who was a detainee held at the Naval Station, Guantanamo Bay, Cuba, unless the President certifies in writing to Congress that the detainee poses no threat to the United States, its citizens, or its allies.

(D) SCREENING OF EMPLOYEES AGAINST WATCHLIST.—The Administrator, in coordination with the Secretary of Transportation and the Administrator of the Federal Aviation Administration, shall ensure that individuals are screened against all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government before—

(i) being certificated by the Federal Aviation Administration;

(ii) being granted unescorted access to the secure area of an airport; or

(iii) being granted unescorted access to the air operations area (as defined in section 1540.5 of title 49, Code of Federal Regulations, or a successor regulation to that section) of an airport.

(E) AIRCRAFT CHARTER CUSTOMER AND LESSEE PRESCREENING.—

(i) ESTABLISHMENT.—The Administrator shall establish a process by which operators of aircraft to be used in charter air transportation with a maximum takeoff weight greater than 12,500 pounds and lessors of aircraft with a maximum takeoff weight greater than 12,500 pounds may—

(I) request the Department to use the advanced passenger prescreening system to compare information about an individual seeking to charter an aircraft with a maximum takeoff weight greater than 12,500 pounds, a passenger proposed to be transported aboard the aircraft, and an individual seeking to lease an aircraft with a maximum takeoff weight greater than 12,500 pounds, to the automatic selectee and no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government; and

(II) refuse to charter or lease an aircraft with a maximum takeoff weight greater than 12,500 pounds to, or transport aboard the aircraft, individuals identified on the watch list.

(ii) APPLICABILITY.—The requirements of subparagraph (C)(iii) apply to this subparagraph.

(iii) DESIGN AND REVIEW OF GUIDELINES, POLICIES, AND OPERATING PROCEDURES.—The Secretary, in consultation with the Terrorist Screening Center, shall design and review, as necessary, guidelines, policies, and operating procedures for the collection, removal, and updating of data maintained, or to be maintained, in the no fly and automatic selectee lists.

(F) APPLICABILITY.—Section 607 of the Vision 100—Century of Aviation Reauthorization Act (Public Law 108–176, 117 Stat. 2568) does not apply to the advanced passenger prescreening system established under subparagraph (C).

(G) APPEAL PROCEDURES.—

(i) ESTABLISHMENT.—The Administrator shall establish a timely and fair process for individuals identified as a threat under one or more of subparagraphs (C), (D), and (E) to appeal to the Transportation Security Administration the determination and correct erroneous information.

(ii) MAINTENANCE OF RECORD OF MISIDENTIFIED INDIVIDUALS.—The process shall include the establishment of a method by which the Administrator 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 Transportation Security Administration record shall contain information determined by the Administrator to authenticate the identity of such a passenger or individual.

(k) LIMITATION ON LIABILITY FOR ACTS TO THWART CRIMINAL VIOLENCE OR AIRCRAFT PIRACY.—An individual is not liable for damages in an action brought in a Federal or State court arising out of the acts of the individual in attempting to thwart an act of criminal violence or piracy on an aircraft if that individual reasonably believed that an act of criminal violence or piracy was occurring or was about to occur.

(l) AIR CHARTER PROGRAM.—

(1) IN GENERAL.—The Administrator shall implement an aviation security program for charter air carriers with a maximum certificated takeoff weight of more than 12,500 pounds.

(2) EXEMPTION FOR ARMED FORCES CHARTERS.—

(A) DEFINITION OF ARMED FORCES.—In this paragraph, the term ''armed forces'' has the meaning given the term in section 101(a)(4) of title 10.

(B) IN GENERAL.—Paragraph (1) and the other requirements of this chapter do not apply to passengers and property carried by aircraft when employed to provide charter transportation to members of the armed forces.

(C) SECURITY PROCEDURES.—The Secretary of Defense, in consultation with the Secretary and the Secretary of Transportation, shall establish security procedures relating to the operation of aircraft when employed to provide charter transportation to members of the armed forces to or from an airport described in subsection (c).

(m) SECURITY SCREENING FOR MEMBERS OF THE ARMED FORCES.—

(1) IN GENERAL.—The Administrator, in consultation with the Department of Defense, shall develop and implement a plan to provide expedited security screening services for a member of the armed forces, and, to the extent possible, an accompanying family member, if the member of the armed forces, while in uniform, presents documentation indicating official orders for air transportation departing from a primary airport (as defined in section 47102 of title 49).

(2) PROTOCOLS.—In developing the plan, the Administrator shall consider—

(A) leveraging existing security screening models used to reduce passenger wait times;

(B) establishing standard guidelines for the screening of military uniform items, including combat boots; and

(C) incorporating new screening protocols into an existing trusted passenger program, as established under section 109(a)(3) of the Aviation and Transportation Security Act (Public Law 107–71, 115 Stat. 613), or into the development of a new credential or system that incorporates biometric technology and other applicable technologies to verify the identity of individuals traveling in air transportation.

(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall affect the authority of the Administrator to require additional screening of a member of the armed forces if intelligence or law enforcement information indicates that additional screening is necessary.

(4) REPORT.—The Administrator shall submit to the appropriate committees of Congress a report on the implementation of the plan.

(n) PASSENGER EXIT POINTS FROM STERILE AREA.—

(1) DEFINITION OF STERILE AREA.—In this subsection, the term ''sterile area'' has the meaning given the term in section 1540.5 of title 49, Code of Federal Regulations, or any corresponding similar regulation or ruling.

(2) IN GENERAL.—The Secretary shall ensure that the Transportation Security Administration is responsible for monitoring passenger exit points from the sterile area of airports at which the Transportation Security Administration provided the monitoring as of December 1, 2013.

§ 40914. Domestic air transportation system security

(a) ASSESSING THREATS.—The Administrator and the Director of the Federal Bureau of Investigation jointly shall assess current and potential threats to the domestic air transportation system. The assessment shall include consideration of the extent to which there are individuals with the capability and intent to carry out terrorist or related unlawful acts against that system and the ways in which those individuals might carry out those acts. The Administrator and the Director jointly shall decide on and carry out the most effective method for continuous analysis and monitoring of security threats to that system.

(b) ASSESSING SECURITY.—In coordination with the Director of the Federal Bureau of Investigation, the Administrator shall carry out periodic threat and vulnerability assessments on security at each airport that is part of the domestic air transportation system. Each assessment shall include consideration of—

(1) the adequacy of security procedures related to the handling and transportation of checked baggage and cargo;

(2) space requirements for security personnel and equipment;

(3) separation of screened and unscreened passengers, baggage, and cargo;

(4) separation of the controlled and uncontrolled areas of airport facilities; and

(5) coordination of the activities of security personnel of the Transportation Security Administration, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and air carriers, and of other law enforcement personnel.

(c) MODAL SECURITY PLAN FOR AVIATION.—In addition to the requirements set forth in paragraphs (2) through (6) of section 11514(c) of this title, the modal security plan for aviation prepared under section 11514 of this title shall—

(1) establish a damage mitigation and recovery plan for the aviation system in the event of a terrorist attack; and

(2) include a threat matrix document that outlines each threat to the United States civil aviation system and the corresponding layers of security in place to address the threat.

(d) OPERATIONAL CRITERIA.—The Administrator shall issue operational criteria to protect airport infrastructure and operations against the threats identified in the plans prepared under section 11514(a) of this title and shall approve best practices guidelines for airport assets.

(e) IMPROVING SECURITY.—The Administrator shall take necessary actions to improve domestic air transportation security by correcting deficiencies in that security discovered in the assessments, analyses, and monitoring carried out under this section.

§ 40915. Information about threats to civil aviation

(a) PROVIDING INFORMATION.—Under guidelines the Administrator prescribes, an air carrier, airport operator, ticket agent, or individual employed by an air carrier, airport operator, or ticket agent, receiving information (except a communication directed by the United States Government) about a threat to civil aviation shall provide the information promptly to the Administrator.

(b) FLIGHT CANCELLATION.—If a decision is made that a particular threat cannot be addressed in a way adequate to ensure, to the extent feasible, the safety of passengers and crew of a particular flight or series of flights, the Administrator shall cancel the flight or series of flights.

(c) GUIDELINES ON PUBLIC NOTICE.—

(1) IN GENERAL.—The President shall develop guidelines for ensuring that public notice is provided in appropriate cases about threats to civil aviation. The guidelines shall identify officials responsible for—

(A) deciding, on a case-by-case basis, if public notice of a threat is in the best interest of the United States and the traveling public;

(B) ensuring that public notice is provided in a timely and effective way, including the use of a toll-free telephone number; and

(C) canceling the departure of a flight or series of flights under subsection (b).

(2) CONTENTS.—The guidelines shall provide for consideration of—

(A) the specificity of the threat;

(B) the credibility of intelligence information related to the threat;

(C) the ability to counter the threat effectively;

(D) the protection of intelligence information sources and methods;

(E) cancellation, by an air carrier or the Administrator, of a flight or series of flights instead of public notice;

(F) the ability of passengers and crew to take steps to reduce the risk to their safety after receiving public notice of a threat; and

(G) other factors the Administrator considers appropriate.

(d) GUIDELINES ON NOTICE TO CREWS.—The Administrator shall develop guidelines for ensuring that notice in appropriate cases of threats to the security of an air carrier flight is provided to the flight crew and cabin crew of that flight.

(e) LIMITATION ON NOTICE TO SELECTIVE TRAVELERS.—Notice of a threat to civil aviation may be provided to selective potential travelers only if the threat applies only to those travelers.

(f) RESTRICTING ACCESS TO INFORMATION.—In cooperation with the departments, agencies, and instrumentalities of the Government that collect, receive, and analyze intelligence information related to aviation security, the Administrator shall develop procedures to minimize the number of individuals who have access to information about threats. However, a restriction on access to that information may be imposed only if the restriction does not diminish the ability of the Government to carry out its duties and powers related to aviation security effectively, including providing notice to the public and flight and cabin crews under this section.

(g) DISTRIBUTION OF GUIDELINES.—The guidelines developed under this section shall be distributed for use by appropriate officials of the Department of Transportation, the Department of State, the Department of Justice, and air carriers.

§ 40916. Foreign air carrier security programs

The Administrator shall continue in effect the requirement of section 129.25 of title 14, Code of Federal Regulations, that a foreign air carrier must adopt and use a security program approved by the Administrator. The Administrator shall not approve a security program of a foreign air carrier under section 129.25 of title 14, Code of Federal Regulations, or a successor regulation, unless the security program requires the foreign air carrier in its operations to and from airports in the United States to adhere to the identical security measures that the Administrator requires air carriers serving the same airports to adhere to. The foregoing requirement shall not be interpreted to limit the ability of the Administrator to impose additional security measures on a foreign air carrier or an air carrier when the Administrator determines that a specific threat warrants additional measures. The Administrator shall prescribe regulations to carry out this section.

§ 40917. Security standards at foreign airports

(a) ASSESSMENT.—

(1) IN GENERAL.—At intervals the Secretary of Transportation considers necessary, the Secretary of Transportation shall assess the effectiveness of the security measures maintained at—

(A) a foreign airport—

(i) served by an air carrier;

(ii) from which a foreign air carrier serves the United States; or

(iii) that poses a high risk of introducing danger to international air travel; and

(B) other foreign airports the Secretary of Transportation considers appropriate.

(2) MEANS OF ASSESSMENT.—The Secretary of Transportation shall conduct an assessment under paragraph (1)—

(A) in consultation with appropriate aeronautic authorities of the government of a foreign country concerned and each air carrier serving the foreign airport for which the Secretary of Transportation is conducting the assessment;

(B) to establish the extent to which a foreign airport effectively maintains and carries out security measures, including the screening and vetting of airport workers; and

(C) by using a standard that will result in an analysis of the security measures at the airport based at least on the standards and appropriate recommended practices contained in Annex 17 to the Convention on International Civil Aviation in effect on the date of the assessment.

(3) REPORT.—Each report to Congress required under section 40958(b) of this title shall contain a summary of the assessments conducted under this subsection.

(b) CONSULTATION.—In carrying out subsection (a), the Secretary of Transportation shall consult with the Secretary of State—

(1) on the terrorist threat that exists in each country; and

(2) to establish which foreign airports are not under the de facto control of the government of the foreign country in which they are located and pose a high risk of introducing danger to international air travel.

(c) NOTIFYING FOREIGN AUTHORITIES.—When the Secretary of Transportation, after conducting an assessment under subsection (a), decides that an airport does not maintain and carry out effective security measures, the Secretary of Transportation, after advising the Secretary of State, shall no-

tify the appropriate authorities of the government of the foreign country of the decision and recommend the steps necessary to bring the security measures in use at the airport up to the standard used by the Secretary of Transportation in making the assessment.

(d) ACTIONS WHEN AIRPORTS NOT MAINTAINING AND CARRYING OUT EFFECTIVE SECURITY MEASURES.—

(1) IDENTIFICATION OF AIRPORT.—When the Secretary of Transportation decides under this section that an airport does not maintain and carry out effective security measures—

(A) the Secretary of Transportation shall—

(i) publish the identity of the airport in the Federal Register;

(ii) have the identity of the airport posted and displayed prominently at all United States airports at which scheduled air carrier operations are provided regularly; and

(iii) notify the news media of the identity of the airport;

(B) each air carrier and foreign air carrier providing transportation between the United States and the airport shall provide written notice of the decision, on or with the ticket, to each passenger buying a ticket for transportation between the United States and the airport;

(C) notwithstanding section 40105(b) of title 49, the Secretary of Transportation, after consulting with the appropriate aeronautic authorities of the foreign country concerned and each air carrier serving the airport and with the approval of the Secretary of State, may withhold, revoke, or prescribe conditions on the operating authority of an air carrier or foreign air carrier that uses that airport to provide foreign air transportation; and

(D) the President may prohibit an air carrier or foreign air carrier from providing transportation between the United States and any other foreign airport that is served by aircraft flying to or from the airport with respect to which a decision is made under this section.

(2) EFFECTIVENESS.—

(A) IN GENERAL.—Paragraph (1) becomes effective—

(i) 90 days after the government of a foreign country is notified under subsection (c) if the Secretary of Transportation finds that the government has not brought the security measures at the airport up to the standard the Secretary of Transportation used in making an assessment under subsection (a); or

(ii) immediately on the decision of the Secretary of Transportation under subsection (c) if the Secretary of Transportation decides, after consulting with the Secretary of State, that a condition exists that threatens the safety or security of passengers, aircraft, or crew traveling to or from the airport.

(B) STATE DEPARTMENT NOTICE.—The Secretary of Transportation immediately shall notify the Secretary of State of a decision under subparagraph (A)(ii) so that the Secretary of State may issue a travel advisory required under section 40918(a) of this title.

(3) REPORT TO CONGRESS.—The Secretary of Transportation promptly shall submit to Congress a report (and classified annex if necessary) on action taken under paragraph (1) or (2), including information on attempts made to obtain the cooperation of the government of a foreign country in meeting the standard the Secretary of Transportation used in assessing the airport under subsection (a).

(4) TERMINATION OF ACTION.—An action required under paragraph (1)(A) and (B) is no longer required only if the Secretary of Transportation, in consultation with the Secretary of State, decides that effective security measures are maintained and carried out at the airport. The Secretary of Transportation shall notify Congress when the action is no longer required to be taken.

(e) SUSPENSIONS.—Notwithstanding sections 40105(b) and 40106(b) of title 49, the Secretary of Transportation, with the approval of the Secretary of State and without notice or a hearing, shall suspend the right of an air carrier or foreign air carrier to provide foreign air transportation, and the right of a person to operate aircraft in foreign air commerce, to or from a foreign airport when the Secretary of Transportation decides that—

(1) a condition exists that threatens the safety or security of passengers, aircraft, or crew traveling to or from that airport; and

(2) the public interest requires an immediate suspension of transportation between the United States and that airport.

(f) CONDITION OF CARRIER AUTHORITY.—This section is a condition of authority the Secretary of Transportation grants under part A of subtitle VII of title 49 to an air carrier or foreign air carrier.

§ 40918. Travel advisory and suspension of foreign assistance

(a) TRAVEL ADVISORIES.—On being notified by the Administrator that the Administrator has decided under section 40917(d)(2)(A)(ii) of this title that a condition exists that threatens the safety or security of passengers,

aircraft, or crew traveling to or from a foreign airport that the Administrator has decided under section 40917 of this title does not maintain and carry out effective security measures, the Secretary of State—

(1) immediately shall issue a travel advisory for that airport; and

(2) shall publicize the advisory widely.

(b) SUSPENDING ASSISTANCE.—The President shall suspend assistance provided under the Foreign Assistance Act of 1961 (22 U.S.C. 2151 et seq.) or the Arms Export Control Act (22 U.S.C. 2751 et seq.) to a country in which is located an airport with respect to which section 40917(d)(1) of this title becomes effective if the Secretary of State decides the country is a high terrorist threat country. The President may waive this subsection if the President decides, and reports to Congress, that the waiver is required because of national security interests or a humanitarian emergency.

(c) ACTIONS NO LONGER REQUIRED.—An action required under this section is no longer required only if the Administrator has made a decision as provided under section 40917(d)(4) of this title. The Administrator shall notify Congress when the action is no longer required to be taken.

§ 40919. Passenger manifests

(a) AIR CARRIER REQUIREMENTS.—

(1) IN GENERAL.—The Secretary of Transportation shall require each air carrier to provide a passenger manifest for a flight to an appropriate representative of the Secretary of State—

(A) not later than 1 hour after that carrier is notified of an aviation disaster outside the United States involving that flight; or

(B) if it is not technologically feasible or reasonable to comply with subparagraph (A), then as expeditiously as possible, but not later than 3 hours after the carrier is so notified.

(2) CONTENTS.—The passenger manifest should include the following information:

(A) The full name of each passenger.

(B) The passport number of each passenger, if required for travel.

(C) The name and telephone number of a contact for each passenger.

(3) CONSIDERATION OF REQUIREMENT TO COLLECT INFORMATION.—In carrying out this subsection, the Secretary of Transportation shall consider the necessity and feasibility of requiring air carriers to collect passenger manifest information as a condition for passengers boarding a flight of the carrier.

(b) FOREIGN AIR CARRIER REQUIREMENTS.—The Secretary of Transportation shall consider imposing a requirement on foreign air carriers comparable to that imposed on air carriers under subsection (a)(1) and (2).

(c) FLIGHTS IN FOREIGN AIR TRANSPORTATION TO THE UNITED STATES.—

(1) IN GENERAL.—Each air carrier and foreign air carrier operating a passenger flight in foreign air transportation to the United States shall provide to the Commissioner of U.S. Customs and Border Protection by electronic transmission a passenger and crew manifest containing the information specified in paragraph (2). Carriers may use the advanced passenger information system to provide the information.

(2) CONTENTS.—A passenger and crew manifest for a flight required under paragraph (1) shall contain the following information:

(A) The full name of each passenger and crew member.

(B) The date of birth and citizenship of each passenger and crew member.

(C) The sex of each passenger and crew member.

(D) The passport number and country of issuance of each passenger and crew member if required for travel.

(E) The United States visa number or resident alien card number of each passenger and crew member, as applicable.

(F) Other information the Administrator, in consultation with the Commissioner of U.S. Customs and Border Protection, determines is reasonably necessary to ensure aviation safety.

(3) PASSENGER NAME RECORDS.—The carriers shall make passenger name record information available to U. S. Customs and Border Protection on request.

(4) TRANSMISSION OF MANIFEST.—Subject to paragraphs (5) and (6), a passenger and crew manifest required for a flight under paragraph (1) shall be transmitted to U. S. Customs and Border Protection in advance of the aircraft's landing in the United States in the manner, time, and form U.S. Customs and Border Protection prescribes.

(5) TRANSMISSION OF MANIFESTS TO OTHER FEDERAL AGENCIES.—On request, information provided to the Administrator or U. S. Customs and Border Protection under this subsection may be shared with other Federal agencies for the purpose of protecting national security.

(6) PRESCREENING INTERNATIONAL PASSENGERS.—

(A) IN GENERAL.—The Secretary, or the designee of the Secretary, shall issue a notice of proposed rulemaking that will allow the Department to compare passenger information for an international flight to or from the United States against the consoli-

dated and integrated terrorist watchlist maintained by the Federal Government before departure of the flight.

(B) APPEAL PROCEDURES.—

(i) ESTABLISHMENT.—The Secretary shall establish a timely and fair process for individuals identified as a threat under subparagraph (A) to appeal to the Department the determination 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 of Transportation, 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.

(e) WRITTEN WORKING AGREEMENTS.—The heads of units in the intelligence community, the Secretary, and the Administrator shall review and, as appropriate, revise written working agreements between the intelligence community and the Administrator.

§ 40922. Research and development

(a) PROGRAM REQUIREMENT.—

(1) IN GENERAL.—The Administrator shall establish and carry out a program to accelerate and expand the research, development, and implementation of technologies and procedures to counteract terrorist acts against civil aviation. The program shall provide for developing and having in place new equipment and procedures necessary to meet the technological challenges presented by terrorism. The program shall include research on, and development of, technological improvements and ways to enhance human performance.

(2) REQUIRED ACTIONS.—In designing and carrying out the program established under this subsection, the Administrator shall—

(A) consult and coordinate activities with other departments, agencies, and instrumentalities of the United States Government doing similar research;

(B) identify departments, agencies, and instrumentalities that would benefit from that research; and

(C) seek cost-sharing agreements with those departments, agencies, and instrumentalities.

(3) ANNUAL REPORTS.—In carrying out the program established under this subsection, the Administrator shall review and consider the annual reports the Secretary submits to Congress on transportation security and intelligence.

(4) DESIGNATION OF RESPONSIBLE INDIVIDUAL.—

(A) IN GENERAL.—In carrying out the program established under this subsection, the Administrator shall designate an individual to be responsible for engineering, research, and development with respect to security technology under the program.

(B) DECISION-MAKING.—The individual designated under subparagraph (A) shall use appropriate systems engineering and risk

management models in making decisions regarding the allocation of funds for engineering, research, and development with respect to security technology under the program.

(C) ANNUAL REPORT.—The individual designated under subparagraph (A) shall, on an annual basis, submit to the Administrator a report on activities under this paragraph during the preceding year. Each report shall include, for the year covered by the report, information on—

(i) progress made in engineering, research, and development with respect to security technology;

(ii) the allocation of funds for engineering, research, and development with respect to security technology; and

(iii) engineering, research, and development with respect to technologies drawn from other agencies, including the rationale for engineering, research, and development with respect to the technologies.

(5) GRANTS.—The Administrator may—

(A) make grants to institutions of higher learning and other appropriate research facilities with demonstrated ability to carry out research described in paragraph (1), and fix the amounts and terms of the grants; and

(B) make cooperative agreements with governmental authorities the Administrator decides are appropriate.

(b) REVIEW OF THREATS.—

(1) IN GENERAL.—The Administrator periodically shall review threats to civil aviation, with particular focus on—

(A) a comprehensive systems analysis (employing vulnerability analysis, threat attribute definition, and technology roadmaps) of the civil aviation system, including—

(i) the destruction, commandeering, or diversion of civil aircraft or the use of civil aircraft as a weapon; and

(ii) the disruption of civil aviation service, including by cyberattack;

(B) explosive material that presents the most significant threat to civil aircraft;

(C) the minimum amounts, configurations, and types of explosive material that can cause, or would reasonably be expected to cause, catastrophic damage to aircraft in air transportation;

(D) the amounts, configurations, and types of explosive material that can be detected reliably by existing, or reasonably anticipated, near-term explosive detection technologies;

(E) the potential release of chemical, biological, or similar weapons or devices either within an aircraft or within an airport;

(F) the feasibility of using various ways to minimize damage caused by explosive material that cannot be detected reliably by existing, or reasonably anticipated, near-term explosive detection technologies;

(G) the ability to screen passengers, carry-on baggage, checked baggage, and cargo; and

(H) the technologies that might be used in the future to attempt to destroy or otherwise threaten commercial aircraft and the ways in which those technologies can be countered effectively.

(2) PROGRAM FOCUS AND PRIORITIES.—The Administrator shall use the results of the review under this subsection to develop the focus and priorities of the program established under subsection (a).

(c) SCIENTIFIC ADVISORY PANEL.—

(1) ESTABLISHMENT.—The Administrator shall establish a scientific advisory panel to review, comment on, advise on the progress of, and recommend modifications in, the program established under subsection (a), including the need for long-range research programs to detect and prevent catastrophic damage to commercial aircraft, commercial aviation facilities, commercial aviation personnel and passengers, and other components of the commercial aviation system by the next generation of terrorist weapons.

(2) PANEL MEMBERS.—

(A) QUALIFICATIONS.—The advisory panel shall consist of individuals who have scientific and technical expertise in—

(i) the development and testing of effective explosive detection systems;

(ii) aircraft structure and experimentation to decide on the type and minimum weights of explosives that an effective explosive detection technology must be capable of detecting;

(iii) technologies involved in minimizing airframe damage to aircraft from explosives; and

(iv) other scientific and technical areas the Administrator considers appropriate.

(B) CONSIDERATIONS.—In appointing individuals to the advisory panel, the Administrator should consider individuals from academia and the national laboratories, as appropriate.

(3) ORGANIZATION AS TEAMS.—The Administrator shall organize the advisory panel into teams capable of undertaking the review of policies and technologies upon request.

(4) BIENNIAL REVIEW.—The Administrator shall review the composition of the advisory panel biennially to ensure that the expertise of the individuals on the panel is suited to the current and anticipated duties of the panel.

(d) SECURITY AND RESEARCH AND DEVELOPMENT ACTIVITIES.—

(1) IN GENERAL.—The Administrator shall conduct research (including behavioral research) and development activities appropriate to develop, modify, test, and evaluate a system, procedure, facility, or device to protect passengers and property against acts of criminal violence, aircraft piracy, and terrorism and to ensure security.

(2) DISCLOSURE.—

(A) IN GENERAL.—Notwithstanding section 552 of title 5, the Administrator shall prescribe regulations prohibiting disclosure of information obtained or developed in ensuring security under this title if the Secretary decides disclosing the information would—

(i) be an unwarranted invasion of personal privacy;

(ii) reveal a trade secret or privileged or confidential commercial or financial information; or

(iii) be detrimental to transportation safety.

(B) INFORMATION TO CONGRESS.—Subparagraph (A) does not authorize information to be withheld from a committee of Congress authorized to have the information.

(C) DESIGNATION OF INFORMATION AS SENSITIVE SECURITY INFORMATION NOT AUTHORIZED.—Nothing in subparagraph (A) shall be construed to authorize the designation of information as sensitive security information (as defined in section 15.5 of title 49, Code of Federal Regulations)—

(i) to conceal a violation of law, inefficiency, or administrative error;

(ii) to prevent embarrassment to a person, organization, or agency;

(iii) to restrain competition; or

(iv) to prevent or delay the release of information that does not require protection in the interest of transportation security, including basic scientific research information not clearly related to transportation security.

(D) NONAPPLICABILITY OF SECTION 552A OF TITLE 5.—Section 552a of title 5 shall not apply to disclosures that the Administrator may make from the systems of records of the Transportation Security Administration to a Federal law enforcement, intelligence, protective service, immigration, or national security offi-

cial to assist the official receiving the information in the performance of official duties.

(3) TRANSFERS OF DUTIES AND POWERS PROHIBITED.—Except as otherwise provided by law, the Administrator may not transfer a duty or power under this section to another department, agency, or instrumentality of the United States Government.

§ 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 the Department of Transportation, 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, 40955, and 40956 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 nearest the marshal's home at no cost to the marshal or the United States Government if the marshal is traveling to that airport after completing his or her security duties;

(6) may enter into agreements with Federal, State, and local agencies under which appropriately trained law enforcement personnel from the agencies, when traveling on a flight of an air carrier, will carry a firearm and be prepared to assist Federal air marshals;

(7) shall establish procedures to ensure that Federal air marshals are made aware of armed or unarmed law enforcement personnel on board an aircraft; and

(8) may appoint as a Federal air marshal, regardless of age (if the individual otherwise meets the background and fitness qualifications required for Federal air marshals)—

(A) an individual who is a retired law enforcement officer;

(B) an individual who is a retired member of the armed forces; or

(C) an individual who was furloughed from an air carrier crew position in the 1-year period beginning on September 11, 2011;

(9) shall require the Federal Air Marshal Service to utilize a risk-based strategy when allocating resources between international and domestic flight coverage, including when initially setting its annual target numbers of average daily international and domestic flights to cover;

(10) shall require the Federal Air Marshal Service to utilize a risk-based strategy to support domestic allocation decisions;

(11) shall require the Federal Air Marshal Service to utilize a risk-based strategy to support international allocation decisions; and

(12) shall ensure that the seating arrangements of Federal air marshals on aircraft are determined in a manner that is risk-based and that allows the air marshals to be most capable of responding to current threats to aviation security.

(b) INTERIM MEASURES.—Until the Administrator completes implementation of subsection (a), the Administrator may use, after consultation with and concurrence of the heads of other Federal agencies and departments,

personnel from those agencies and departments, on a nonreimbursable basis, to provide air marshal service.

(c) CONTINUATION OF INITIATIVES TO PROTECT ANONYMITY OF FEDERAL AIR MARSHALS.—The Director of the Federal Air Marshal Service shall continue operational initiatives to protect the anonymity of Federal air marshals.

(d) TRAINING FOR FEDERAL AND LOCAL LAW ENFORCEMENT PERSONNEL.—

(1) AVAILABILITY OF INFORMATION.—The Administrator and the Director of the Federal Air Marshal Service shall make available, as practicable, appropriate information on in-flight counterterrorism and weapons handling procedures and tactics training to Federal law enforcement officers who fly while in possession of a firearm.

(2) IDENTIFICATION OF FRAUDULENT DOCUMENTS.—The Administrator and the Director of the Federal Air Marshal Service shall ensure that Transportation Security Administration screeners and Federal air marshals receive training in identifying fraudulent identification documents, including fraudulent or expired visas and passports. The training also shall be made available to other Federal law enforcement agencies and local law enforcement agencies located in a State that borders Canada or Mexico.

(e) AGREEMENT ON FEDERAL AIR MARSHALS ON FLIGHTS TO AND FROM THE UNITED STATES.—

(1) DEVELOPMENT.—Not later than 60 days after October 5, 2018, the Administrator shall develop a standard written agreement that shall be the basis of all negotiations and agreements that begin after October 5, 2018, between the United States and foreign governments or partners regarding the presence of Federal air marshals on flights to and from the United States, including deployment, technical assistance, and information sharing.

(2) SIGNED AGREEMENT.—Except as provided in paragraph (3), not later than 180 days after October 5, 2018, all agreements between the United States and foreign governments or partners regarding the presence of Federal air marshals on flights to and from the United States shall be in writing and signed by the Administrator or other authorized United States Government representative.

(3) EXCEPTION.—The Administrator may schedule Federal air marshal service on flights operating to a foreign country with which no written agreement is in effect if the Administrator determines that—

(A) the mission is necessary for aviation security; and

(B) the requirements of paragraph (4)(C) are met.

(4) NOTIFICATION TO CONGRESS.—

(A) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this paragraph, the term ''appropriate committees of Congress'' means—

(i) the Committee on Commerce, Science, and Transportation of the Senate;

(ii) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(iii) the Committee on Homeland Security of the House of Representatives.

(B) WRITTEN AGREEMENTS.—Not later than 30 days after the date that the Administrator enters into a written agreement under this subsection, the Administrator shall transmit to the appropriate committees of Congress a copy of the agreement.

(C) NO WRITTEN AGREEMENT.—The Administrator shall submit to the appropriate committees of Congress—

(i) not later than 30 days after October 5, 2018, a list of each foreign government or partner that does not have a written agreement under this subsection, including an explanation for why no written agreement exists and a justification for the determination that a mission under paragraph (3)(A) is necessary for aviation security; and

(ii) not later than 30 days after the date that the Administrator makes a determination to schedule Federal air marshal service on flights operating to a foreign country with which no written agreement is in effect under paragraph (3), the name of the applicable foreign government or partner, an explanation for why no written agreement exists, and a justification for the determination that the mission under paragraph (3)(A) is necessary for aviation security.

(f) AUTOMATED MISSION SCHEDULING.—The Administrator shall endeavor to acquire automated capabilities or technologies for scheduling Federal air marshal service missions based on current risk modeling.

(g) IMPROVING FEDERAL AIR MARSHAL SERVICE DEPLOYMENTS.—

(1) AFTER-ACTION REPORTS.—The Administrator shall strengthen internal controls to ensure that all after-action reports on Federal air marshal service special mission coverage provided to stakeholders include documentation of supervisory review and approval, and mandatory narratives.

(2) STUDY.—-The Administrator shall contract with an independent entity to conduct a validation and verification study of the risk analysis

and risk-based determinations guiding Federal air marshal service deployment, including the use of risk-based strategies under paragraphs (9) through (12) of subsection (a).

(3) COST-BENEFIT ANALYSIS.—The Administrator shall conduct a cost-benefit analysis regarding mitigation of aviation security threats through Federal air marshal service deployment.

(4) PERFORMANCE MEASURES.—The Administrator shall improve existing performance measures to better determine the effectiveness of in-flight operations in addressing the highest risks to aviation transportation based on current intelligence.

(h) TRAINING FOR FOREIGN LAW ENFORCEMENT PERSONNEL.—

(1) IN GENERAL.—The Administrator, after consultation with the Secretary of State, may direct the Federal Air Marshal Service to provide appropriate air marshal training to law enforcement personnel of foreign countries.

(2) WATCHLIST SCREENING.—The Federal Air Marshal Service may only provide appropriate air marshal training to law enforcement personnel of foreign countries after comparing the identifying information and records of law enforcement personnel of foreign countries against all appropriate records in the consolidated and integrated terrorist watchlists maintained by the Federal Government.

(3) FEES.—The Administrator shall establish reasonable fees and charges to pay expenses incurred in carrying out this subsection. Funds collected under this subsection shall be credited to the account in the Treasury from which the expenses were incurred and shall be available to the Administrator for purposes for which amounts in the account are available.

§ 40928. Crew training

(a) BASIC SECURITY TRAINING.—

(1) IN GENERAL.—Each air carrier providing scheduled passenger air transportation shall carry out a training program for flight and cabin crew members to prepare the crew members for potential threat conditions.

(2) PROGRAM ELEMENTS.—An air carrier training program under this subsection shall include, at a minimum, elements that address each of the following:

(A) The recognition of suspicious activities and the determination of the seriousness of an occurrence.

(B) Crew communication and coordination.

(C) The proper commands to give passengers and attackers.

(D) The appropriate responses to defend oneself.

(E) The use of protective devices assigned to crew members (to the extent devices are required by the Administrator and the Administrator of the Federal Aviation Administration).

(F) The psychology of terrorists to cope with hijacker behavior and passenger responses.

(G) Situational training exercises regarding various threat conditions.

(H) Flight deck procedures or aircraft maneuvers to defend the aircraft, and cabin crew responses to the procedures and maneuvers.

(I) The proper conduct of a cabin search, including explosive device recognition.

(J) Other subject matter considered appropriate by the Administrator.

(3) APPROVAL.—An air carrier training program under this subsection shall be subject to approval by the Administrator.

(4) MINIMUM STANDARDS.—The Administrator may establish minimum standards for the training provided under this subsection and for recurrent training.

(5) PROGRAMS TO CONTINUE IN EFFECT.—Notwithstanding paragraphs (3) and (4), a training program of an air carrier to prepare flight and cabin crew members for potential threat conditions that was approved by the Administrator of the Federal Aviation Administration or the Administrator before December 12, 2003, may continue in effect until disapproved or ordered modified by the Administrator.

(6) MONITORING.—The Administrator, in consultation with the Administrator of the Federal Aviation Administration, shall monitor air carrier training programs under this subsection and periodically shall review an air carrier's training program to ensure that the program is adequately preparing crew members for potential threat conditions. In determining when an air carrier's training program should be reviewed under this paragraph, the Administrator shall consider complaints from crew members. The Administrator shall ensure that employees responsible for monitoring the training programs have the necessary resources and knowledge.

(7) UPDATES.—The Administrator, in consultation with the Administrator of the Federal Aviation Administration, shall order air carriers to modify training programs under this subsection to reflect new or different security threats.

(b) ADVANCED SELF-DEFENSE TRAINING.—

(1) IN GENERAL.—The Administrator shall develop and provide a voluntary training program for flight and cabin crew members of air carriers providing scheduled passenger air transportation.

(2) PROGRAM ELEMENTS.—The training program under this subsection shall include both classroom and effective hands-on training in the following elements of self-defense:

(A) The deterrence of a passenger who might present a threat.

(B) Advanced control, striking, and restraint techniques.

(C) Training to defend oneself against edged or contact weapons.

(D) Methods to subdue and restrain an attacker.

(E) The use of available items aboard the aircraft for self-defense.

(F) Appropriate and effective responses to defend oneself, including the use of force against an attacker.

(G) Other elements of training that the Administrator considers appropriate.

(3) PARTICIPATION NOT REQUIRED.—A crew member shall not be required to participate in the training program under this subsection.

(4) COMPENSATION.—Neither the Federal Government nor an air carrier shall be required to compensate a crew member for participating in the training program under this subsection.

(5) FEES.—A crew member is not required to pay a fee for the training program under this subsection.

(6) CONSULTATION.—In developing the training program under this subsection, the Administrator shall consult with law enforcement personnel and security experts who have expertise in self-defense training, terrorism experts, representatives of air carriers, the director of self-defense training in the Federal Air Marshal Service, flight attendants, labor organizations representing flight attendants, and educational institutions offering law enforcement training programs.

(7) DESIGNATION OF TRANSPORTATION SECURITY ADMINISTRATION OFFICIAL.—The Administrator shall designate an official in the Transportation Security Administration to be responsible for implementing the training program under this subsection. The official shall consult with air carriers and labor organizations representing crew members before implementing the program to ensure that it is appropriate for situations that may arise on board an aircraft during a flight.

(c) LIMITATION.—Actions by crew members under this section shall be subject to section 40913(k) of this title.

§ 40929. PreCheck Program

(a) IN GENERAL.—The Administrator shall continue to administer the PreCheck Program in accordance with section 11521(a)(3) of this title

(b) EXPANSION.—Not later than 180 days after October 5, 2018, the Administrator shall enter into an agreement, using other transaction authority under section 11508 of this title, with at least 2 private-sector entities to increase the methods and capabilities available for the public to enroll in the PreCheck Program.

(c) MINIMUM CAPABILITY REQUIREMENTS.—At least 1 agreement under subsection (b) shall include the following capabilities:

(1) Start-to-finish secure online or mobile enrollment capability.

(2) Vetting of an applicant by means other than biometrics, such as a risk assessment, if—

(A) the means—

(i) are evaluated and certified by the Secretary;

(ii) meet the definition of a qualified anti-terrorism technology under section 10931 of this title; and

(iii) are determined by the Administrator to provide a risk assessment that is as effective as a fingerprint-based criminal history records check conducted through the Federal Bureau of Investigation with respect to identifying individuals who are not qualified to participate in the PreCheck Program due to disqualifying criminal history; and

(B) with regard to private-sector risk assessments, the Secretary has certified that reasonable procedures are in place with regard to the accuracy, relevancy, and proper utilization of information employed in the risk assessments.

(d) ADDITIONAL CAPABILITY REQUIREMENTS.—At least 1 agreement under subsection (b) shall include the following capabilities:

(1) Start-to-finish secure online or mobile enrollment capability.

(2) Vetting of an applicant by means of biometrics if the collection—

(A) is comparable with the appropriate and applicable standards developed by the National Institute of Standards and Technology;

(B) protects privacy and data security, including that any personally identifiable information is collected, retained, used, and shared in a manner consistent with section 552a of title 5 and with agency regulations;

(C) is evaluated and certified by the Secretary; and

(D) is determined by the Administrator to provide a risk assessment that is as effective as a fingerprint-based criminal history records check conducted through the Federal Bureau of Investiga-

tion with respect to identifying individuals who are not qualified to participate in the PreCheck Program due to disqualifying criminal history.

(e) TARGET ENROLLMENT.—Subject to subsections (b), (c), and (d), the Administrator shall take actions to expand the total number of individuals enrolled in the PreCheck Program as follows:

(1) 7,000,000 passengers before October 1, 2019.

(2) 10,000,000 passengers before October 1, 2020.

(3) 15,000,000 passengers before October 1, 2021.

(f) MARKETING OF PRECHECK PROGRAM.—Not later than 90 days after October 5, 2018, the Administrator shall—

(1) enter into at least 2 agreements, using other transaction authority under section 11508 of this title, to market the PreCheck Program; and

(2) implement a long-term strategy for partnering with the private sector to encourage enrollment in the PreCheck Program.

(g) IDENTITY VERIFICATION ENHANCEMENT.—The Administrator shall—

(1) coordinate with the heads of appropriate components of the Department to leverage Department-held data and technologies to verify the identity and citizenship of individuals enrolling in the PreCheck Program;

(2) partner with the private sector to use biometrics and authentication standards, such as relevant standards developed by the National Institute of Standards and Technology, to facilitate enrollment in the Precheck Program; and

(3) consider leveraging the existing resources and abilities of airports to collect fingerprints for use in background checks to expedite identity verification.

(h) PRECHECK PROGRAM LANES OPERATION.—The Administrator shall—

(1) ensure that PreCheck Program screening lanes are open and available during peak and high-volume travel times at appropriate airports to individuals enrolled in the PreCheck Program; and

(2) make every practicable effort to provide expedited screening at standard screening lanes to maintain operational efficiency during times when PreCheck Program screening lanes are closed to individuals enrolled in the program.

(i) ELIGIBILITY OF MEMBERS OF THE ARMED FORCES FOR EXPEDITED SECURITY SCREENING.—

(1) IN GENERAL.—Subject to paragraph (3), an individual specified in paragraph (2) is eligible for expedited security screening under the PreCheck Program.

(2) INDIVIDUALS SPECIFIED.—An individual specified in this subsection is any of the following:

(A) A member of the Armed Forces, including a member of a reserve component or the National Guard.

(B) A cadet or midshipman of the United States Military Academy, the United States Naval Academy, the United States Air Force Academy, or the United States Coast Guard Academy.

(C) A family member of an individual specified in subparagraph (A) or (B) who is younger than 12 years old and accompanying the individual.

(3) IMPLEMENTATION.—The eligibility of an individual specified in paragraph (2) for expedited security screening under the PreCheck Program is subject to such policies and procedures as the Administrator may prescribe to carry out this subsection, in consultation with the Secretary of Defense and, with respect to the Coast Guard, the Commandant of the Coast Guard.

(j) IDENTIFYING VULNERABILITIES IN VETTING PROCESS FOR PRECHECK PROGRAM PARTICIPANTS.—The Administrator shall initiate an assessment to identify security vulnerabilities in the vetting process for the PreCheck Program, including determining whether subjecting PreCheck Program participants to recurrent fingerprint-based criminal history records checks, in addition to recurrent checks against the terrorist watchlist, could be done in a cost-effective manner to strengthen the security of the PreCheck Program.

(k) ASSURANCE OF SEPARATE PROGRAM.—In carrying out this section, the Administrator shall ensure that the additional private-sector application capabilities under subsections (b), (c), and (d) are undertaken in addition to any other related Transportation Security Administration program, initiative, or procurement, including the Universal Enrollment Services program.

(l) EXPENDITURE OF FUNDS.—Federal funds expended by the Administrator to expand PreCheck Program enrollment shall be expended in a manner that includes the requirements of this section.

§ 40930. PreCheck expedited screening

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Commerce, Science, and Transportation of the Senate;

(2) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(3) the Committee on Homeland Security of the House of Representatives.

(b) IN GENERAL.—The Administrator shall ensure that only a traveler who is a member of a trusted traveler program specified in subsection (c) is permitted to use a PreCheck security screening lane at a passenger screening checkpoint.

(c) TRUSTED TRAVELER PROGRAMS SPECIFIED.—A trusted traveler program specified in this subsection is any of the following:

(1) The PreCheck Program under section 40929 of this title.

(2) Any other program implemented by the Transportation Security Administration under section 11521(a)(3) of this title

(3) Any other United States Government program that issues a unique identifier, such as a known traveler number, that the Transportation Security Administration accepts as validating that the individual holding the identifier is a member of a known low-risk population.

(d) EXEMPTIONS.—Nothing in this section shall affect—

(1) the authority of the Administrator, under section 40938 of this title, to carry out expedited screening for members of the Armed Forces with disabilities or severe injuries or veterans with disabilities or severe injuries; or

(2) the Honor Flight program under section 40939 of this title.

(e) LOW-RISK TRAVELERS.—A traveler who is determined by the Administrator to be low risk based on the traveler's age and who is not a member of a trusted traveler program specified in subsection (c) shall be permitted to utilize PreCheck security screening lanes at Transportation Security Administration checkpoints when traveling on the same reservation as a member of the program.

(f) RISK-MODIFIED SCREENING.—-

(1) DEFINITION OF LOW-RISK PASSENGER.—In this subsection, the term ''low-risk passenger'' means a passenger who—

(A) meets a risk-based, intelligence-driven criterion prescribed by the Administrator; or

(B) undergoes a canine enhanced screening on arrival at the passenger screening checkpoint.

(2) PILOT PROGRAM.—Not later than 60 days after October 5, 2018, and subject to paragraph (3), the Administrator shall commence a pilot program regarding a risk-modified screening protocol for lanes other than designated PreCheck security screening lanes at passenger screen-

ing checkpoints, in airports of varying categories, to further segment passengers based on risk.

(3) ELIGIBILITY.—Only a low-risk passenger shall be eligible to participate in the risk-modified screening pilot program under paragraph (2).

(4) TERMINATION.—The pilot program shall terminate on the date that is 120 days after the date it commences under paragraph (2).

(5) BRIEFING.—Not later than 30 days after the termination date under paragraph (4), the Administrator shall brief the appropriate committees of Congress on the findings of the pilot program, including—

(A) information relating to the security effectiveness and passenger facilitation effectiveness of the risk-modified screening protocol;

(B) a determination regarding whether the risk-modified screening protocol was effective; and

(C) if the Administrator determined that the protocol was effective, a plan for the deployment of the protocol at as many Transportation Security Administration passenger screening checkpoints as practicable.

(6) IMPLEMENTATION.–In determining whether deployment of the protocol at a Transportation Security Administration passenger screening checkpoint at an airport is practicable, the Administrator shall consider—

(A) the level of risk at the airport;

(B) the available space at the airport;

(C) passenger throughput levels at the airport;

(D) the checkpoint configuration at the airport; and

(E) adequate resources to appropriately serve passengers in PreCheck security screening lanes at the passenger screening checkpoint.

(g) WORKING GROUP.—

(1) IN GENERAL.—In carrying out subsection (f), the Administrator shall establish a working group to advise the Administrator on the development of plans for the deployment of the protocol at Transportation Security Administration passenger screening checkpoints, other than designated PreCheck security screening lanes, in the most effective and efficient manner practicable.

(2) MEMBERS.—The working group shall be comprised of representatives of Category X, I, II, III, and IV airports and air carriers (as the term is defined in section 40102 of title 49).

(3) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—-CHAPTER 10 OF TITLE 5 SHALL NOT APPLY TO THE WORKING GROUP ESTABLISHED UNDER THIS SUBSECTION.

(h) BRIEFINGS.—-

(1) IN GENERAL.—The Administrator shall brief, on a biannual basis, the appropriate committees of Congress on the implementation of subsection (b) until the Administrator certifies that only travelers who are members of trusted traveler programs specified in subsection (c) are permitted to use PreCheck security screening lanes at passenger screening checkpoints.

(2) CERTIFICATION.—On a determination by the Administrator that only travelers who are members of a trusted traveler program specified in subsection (c) are permitted to use PreCheck security screening lanes at checkpoints in accordance with subsection (b), the Administrator shall submit to the appropriate committees of Congress a written certification relating to the determination.

(i) INSPECTOR GENERAL ASSESSMENTS.—The Inspector General of the Department shall assess and transmit to the appropriate committees of Congress the Administrator's implementation under subsection (b).

(j) EXPANSION OF PRECHECK PROGRAM ENROLLMENT.—

(1) LONG-TERM STRATEGY.—The Administrator shall develop and begin the implementation of a long-term strategy to increase enrollment in the PreCheck Program.

(2) CONSIDERATIONS.—In developing the strategy under paragraph (1), the Administrator shall consider the following:

(A) Partnering with air carriers (as the term is defined in section 40102 of title 49) to incorporate PreCheck Program promotion opportunities in the reservation process described in section 1560.101 of title 49, Code of Federal Regulations;

(B) Including in the PreCheck Program an individual who—

(i) holds a Secret, Top Secret, or Top Secret/Sensitive Compartmented Information clearance, unless the individual's clearance has been revoked or the individual did not pass a periodic reinvestigation; or

(ii) is a current, full-time Federal law enforcement officer.

(C) Providing PreCheck Program enrollment flexibility by offering secure mobile enrollment platforms that facilitate in-person identity verification and application data collection, such as through biometrics.

(D) Reducing travel time to PreCheck Program enrollment centers for applicants, including—-

(i) by adjusting the locations and schedules of existing PreCheck Program enrollment centers to accommodate demand;

(ii) by seeking to colocate the enrollment centers with existing facilities that support the issuance of—-

(I) United States passports; and

(II) Security Identification Display Area credentials (as the term is defined in section 1540.5 of title 49, Code of Federal Regulations) located in public, non-secure areas of airports if no systems of an airport operator are used in support of enrollment activities for the credentials; and

(iii) by increasing the availability of PreCheck Program enrollment platforms, such as kiosks, tablets, or staffed laptop stations.

(E) Assessing the feasibility of providing financial assistance or other incentives for PreCheck Program enrollment for—-

(i) children who are at least 12 years old but less than 18 years old;

(ii) families consisting of 5 or more immediate family members;

(iii) private-sector entities, including small businesses, to establish PreCheck Program enrollment centers in their respective facilities; and

(iv) private-sector entities, including small business concerns (as the term is described in section 3 of the Small Business Act (15 U.S.C. 632)), to reimburse an employee for the cost of the PreCheck Program application.

(k) EXTENDED ENROLLMENT FOR ERRONEOUS REVOCATION.—Notwithstanding any other provision of law, the Secretary shall, with respect to an individual whose enrollment in a trusted traveler program was revoked in error, extend by an amount of time equal to the period of revocation the period of active enrollment in the program on reenrollment in the program by the individual.

§ 40931. Screening partnership program

(a) IN GENERAL.—An airport operator may submit to the Administrator an application to carry out the screening of passengers and property at the airport under section 40911 of this title by personnel of a qualified private screening company pursuant to a contract entered into with the Transportation Security Administration.

(b) APPROVAL OF APPLICATIONS.—

(1) IN GENERAL.—Not later than 60 days after the date of receipt of an application submitted by an airport operator under subsection (a), the Administrator shall approve or deny the application.

(2) STANDARDS.—The Administrator shall approve an application submitted by an airport operator under subsection (a) if the Administrator determines that the approval would not compromise security or detrimentally affect the cost-efficiency or the effectiveness of the screening of passengers or property at the airport.

(3) REPORTS ON DENIALS OF APPLICATIONS.—

(A) IN GENERAL.—If the Administrator denies an application submitted by an airport operator under subsection (a), the Administrator shall provide to the airport operator, not later than 60 days following the date of the denial, a written report that sets forth—

(i) the findings that served as the basis for the denial;

(ii) the results of a cost or security analysis conducted in considering the application; and

(iii) recommendations on how the airport operator can address the reasons for the denial.

(B) SUBMISSION TO CONGRESS.—The Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives a copy of a report provided to an airport operator under subparagraph (A).

(c) QUALIFIED PRIVATE SCREENING COMPANY.—A private screening company is qualified to provide screening services at an airport under this section if the company will only employ individuals to provide the services who meet all the requirements of this chapter applicable to Federal Government personnel who perform screening services at airports under this chapter and will provide compensation and other benefits to the individuals that are not less than the level of compensation and other benefits provided to the Federal Government personnel in accordance with this chapter.

(d) SELECTION OF CONTRACTS AND STANDARDS FOR PRIVATE SCREENING COMPANIES.—

(1) IN GENERAL.—The Administrator shall, on approval of the application, provide the airport operator with a list of qualified private screening companies.

(2) CONTRACTS.—The Administrator shall, to the extent practicable, enter into a contract with a private screening company from the list provided under paragraph (1) for the provision of screening at the air-

port not later than 120 days after the date of approval of an application submitted by the airport operator under subsection (a) if—

(A) the level of screening services and protection provided at the airport under the contract will be equal to or greater than the level that would be provided at the airport by Federal Government personnel under this chapter;

(B) the private screening company is owned and controlled by a citizen of the United States, to the extent that the Administrator determines that there are private screening companies owned and controlled by citizens of the United States; and

(C) the selected qualified private screening company offered contract price is equal to or less than the cost to the Federal Government to provide screening services at the airport.

(3) WAIVERS.—The Administrator may waive the requirement of paragraph (2)(B) for a company that is a United States subsidiary with a parent company that has implemented a foreign ownership, control, or influence mitigation plan that has been approved by the Defense Security Service of the Department of Defense prior to the submission of the application. The Administrator has complete discretion to reject any application from a private screening company that requires a waiver under this paragraph to provide screening services at an airport.

(e) SUPERVISION OF SCREENING PERSONNEL.—The Administrator shall—

(1) provide Federal Government supervisors to oversee all screening at each airport at which screening services are provided under this section and provide Federal Government law enforcement officers at the airport pursuant to this chapter; and

(2) undertake covert testing and remedial training support for employees of private screening companies providing screening at airports.

(f) SUSPENSION OF TERMINATION OF CONTRACTS.—The Administrator may suspend or terminate, as appropriate, a contract entered into with a private screening company to provide screening services at an airport under this section if the Administrator finds that the company has failed repeatedly to comply with a standard, regulation, directive, order, law, or contract applicable to the hiring or training of personnel to provide services or to the provision of screening at the airport.

(g) OPERATOR NOT LIABLE.—Notwithstanding another law, an operator of an airport is not liable for a claim for damages filed in State or Federal court (including a claim for compensatory, punitive, contributory, or indemnity damages) relating to—

(1) the airport operator's decision—

(A) to submit an application to the Administrator under subsection (a); or

(B) not to submit an application; and

(2) an act of negligence, gross negligence, or intentional wrongdoing by—

(A) a qualified private screening company or its employees in a case in which the qualified private screening company is acting under a contract entered into with the Secretary or the Secretary's designee; or

(B) employees of the Federal Government providing passenger and property security screening services at the airport.

(h) EVALUATION OF SCREENING COMPANY PROPOSALS FOR AWARD.—

(1) IN GENERAL.—Except as provided in paragraph (2), notwithstanding another law, including title 48 of the Code of Federal Regulations and the Federal Advisory Committee Act (5 U.S.C. App.), an airport operator that has applied and been approved to have security screening services carried out by a qualified private screening company under contract with the Administrator may nominate to the head of the contracting activity an individual to participate in the evaluation of proposals for the award of the contract.

(2) PARTICIPATION ON A PROPOSAL EVALUATION COMMITTEE.—Participation on a proposal evaluation committee under paragraph (1) shall be conducted in accordance with chapter 21 of title 41.

(i) INNOVATIVE SCREENING APPROACHES AND TECHNOLOGIES.—The Administrator shall encourage an airport operator to whom screening services are provided under this section to recommend to the Administrator innovative screening approaches and technologies. On receipt of any recommendations, the Administrator shall review and, if appropriate, test, conduct a pilot project, and, if appropriate, deploy the approaches and technologies.

(j) OPERATOR LIABILITY.—Nothing in this section shall relieve an airport operator from liability for its own acts or omissions related to its security responsibilities. Except as may be provided by subchapter II of chapter 109 of this title, nothing in this section shall relieve a qualified private screening company or its employees from liability related to its own acts of negligence, gross negligence, or intentional wrongdoing.

§ 40932. Federal flight deck officer program

(a) DEFINITIONS.—In this section:

(1) AIR TRANSPORTATION.—The term ''air transportation'' includes all-cargo air transportation.

(2) FIREARMS TRAINING FACILITY.—The term ''firearms training facility'' means a private or government-owned gun range approved by the Administrator to provide recurrent or requalification training, as applicable for the program, using a Transportation Security Administration-approved contractor and a curriculum developed and approved by the Transportation Security Administration.

(3) PILOT.—The term ''pilot'' means an individual who has final authority and responsibility for the operation and safety of a flight or another flight deck crew member.

(b) NONAPPLICABILITY.—This section does not apply to air carriers operating under part 135 of title 14, Code of Federal Regulations, and to pilots employed by the carriers to the extent that the carriers and pilots are covered by section 135.119 of title 14, Code of Federal Regulations, or a successor to that section.

(c) ESTABLISHMENT.—The Administrator shall establish a program to deputize volunteer pilots of air carriers providing air transportation or intrastate air transportation as Federal law enforcement officers to defend the flight decks of aircraft of air carriers against acts of criminal violence or air piracy. The officers shall be known as ''Federal flight deck officers''.

(d) PROCEDURAL REQUIREMENTS.—

(1) IN GENERAL.—The Administrator shall establish procedural requirements to carry out the program under this section.

(2) COMMENCEMENT OF PROGRAM.—The Administrator shall train and deputize pilots who are qualified to be Federal flight deck officers as Federal flight deck officers under the program.

(3) ISSUES TO BE ADDRESSED.—The procedural requirements established under paragraph (1) shall address the following issues:

(A) The type of firearm to be used by a Federal flight deck officer.

(B) The type of ammunition to be used by a Federal flight deck officer.

(C) The standards and training needed to qualify and requalify as a Federal flight deck officer.

(D) The placement of the firearm of a Federal flight deck officer on board the aircraft to ensure both its security and its ease of retrieval in an emergency.

(E) An analysis of the risk of catastrophic failure of an aircraft as a result of the discharge (including an accidental discharge) of a firearm to be used in the program into the avionics, electrical systems, or other sensitive areas of the aircraft.

(F) The division of responsibility between pilots in the event of an act of criminal violence or air piracy if only one pilot is a Federal flight deck officer and if both pilots are Federal flight deck officers.

(G) Procedures for ensuring that the firearm of a Federal flight deck officer does not leave the cockpit if there is a disturbance in the passenger cabin of the aircraft or if the pilot leaves the cockpit for personal reasons.

(H) Interaction between a Federal flight deck officer and a Federal air marshal on board the aircraft.

(I) The process for selection of pilots to participate in the program based on their fitness to participate in the program, including whether an additional background check should be required beyond that required by section 40956(a)(1) of this title.

(J) Storage and transportation of firearms between flights, including international flights, to ensure the security of the firearms, focusing particularly on whether security would be enhanced by requiring storage of the firearm at the airport when the pilot leaves the airport to remain overnight away from the pilot's base airport.

(K) Methods for ensuring that security personnel will be able to identify whether a pilot may carry a firearm under the program.

(L) Methods for ensuring that pilots (including Federal flight deck officers) will be able to identify whether a passenger is a law enforcement officer who may carry a firearm aboard the aircraft.

(M) Other issues that the Administrator considers necessary.

(4) PREFERENCE.—In selecting pilots to participate in the program, the Administrator shall give preference to pilots who are former military or law enforcement personnel.

(5) CLASSIFIED INFORMATION.—Notwithstanding section 552 of title 5, information developed under paragraph (3)(E) shall not be disclosed.

(6) NOTICE TO CONGRESS.—The Administrator shall provide notice to the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate after completing the analysis required by paragraph (3)(E).

(7) MINIMIZATION OF RISK.—If the Administrator determines as a result of the analysis under paragraph (3)(E) that there is a significant risk of the catastrophic failure of an aircraft as a result of the discharge of a firearm, the Administrator shall take necessary actions to minimize that risk.

(8) REVIEW STANDARD.—The Administrator's decisions regarding the methods for implementing each of the procedural requirements specified in paragraph (3) shall be subject to review only for abuse of discretion.

(e) TRAINING, SUPERVISION, AND EQUIPMENT.—

(1) IN GENERAL.—The Administrator shall only be obligated to provide the training, supervision, and equipment necessary for a pilot to be a Federal flight deck officer under this section at no expense to the pilot or the air carrier employing the pilot.

(2) TRAINING.—

(A) IN GENERAL.—The Administrator shall base the requirements for the training of Federal flight deck officers under subsection (d) on the training standards applicable to Federal air marshals, except that the Administrator shall take into account the differing roles and responsibilities of Federal flight deck officers and Federal air marshals.

(B) ELEMENTS.—The training of a Federal flight deck officer shall include, at a minimum—

(i) training to ensure that the officer achieves the level of proficiency with a firearm required under subparagraph (C)(i);

(ii) training to ensure that the officer maintains exclusive control over the officer's firearm at all times, including training in defensive maneuvers; and

(iii) training to assist the officer in determining when it is appropriate to use the officer's firearm and when it is appropriate to use less than lethal force.

(C) TRAINING IN USE OF FIREARMS.—

(i) LEVEL OF PROFICIENCY.—To be deputized as a Federal flight deck officer, a pilot must achieve a level of proficiency with a firearm that is required by the Administrator. The level shall be comparable to the level of proficiency required of Federal air marshals.

(ii) TRAINING BY ADMINISTRATOR OR FIREARMS TRAINING FACILITY.—

(I) IN GENERAL.—The training of a Federal flight deck officer in the use of a firearm may be conducted by the Administrator or by a firearms training facility.

(II) ACCESS TO TRAINING FACILITIES.—The Administrator shall designate additional firearms training facilities located in various regions of the United States for

Federal flight deck officers for recurrent and requalifying training relative to the number of the facilities available on the day before October 5, 2018.

(iii) REQUALIFICATION.—

(I) IN GENERAL.—The Administrator shall require a Federal flight deck officer to requalify to carry a firearm under the program. The requalification shall occur at an interval required by the Administrator.

(II) USE OF FACILITIES FOR REQUALIFICATION.—The Administrator shall allow a Federal flight deck officer to requalify to carry a firearm under the program through training at a Transportation Security Administration-approved firearms training facility utilizing a Transportation Security Administration-approved contractor and a curriculum developed and approved by the Transportation Security Administration.

(iv) PERIODIC REVIEW.—The Administrator shall periodically review requalification training intervals and assess whether it is appropriate and sufficient to adjust the time between each requalification training to facilitate continued participation in the program under this section while still maintaining effectiveness of the training, and update the training requirements as appropriate.

(D) TRAINING REVIEW.—Not later than 2 years after October 5, 2018, and biennially thereafter, the Administrator shall review training facilities and training requirements for initial and recurrent training for Federal flight deck officers and evaluate how training requirements, including the length of training, could be streamlined while maintaining the effectiveness of the training, and update the training requirements as appropriate.

(f) DEPUTIZATION.—

(1) IN GENERAL.—The Administrator may deputize, as a Federal flight deck officer under this section, a pilot who submits to the Administrator a request to be such an officer and who the Administrator determines is qualified to be such an officer.

(2) QUALIFICATION.—

(A) IN GENERAL.—A pilot is qualified to be a Federal flight deck officer under this section if—

(i) the pilot is employed by an air carrier;

(ii) the Administrator determines that the pilot meets the standards established by the Administrator for being a Federal flight deck officer; and

(iii) the Administrator determines that the pilot has completed the training required by the Administrator.

(B) CONSISTENCY WITH REQUIREMENTS FOR CERTAIN MEDICAL CERTIFICATES.—In establishing standards under subparagraph (A)(ii), the Administrator may not establish medical or physical standards for a pilot to become a Federal flight deck officer that are inconsistent with or more stringent than the requirements of the Federal Aviation Administration for the issuance of the required airman medical certificate under part 67 of title 14, Code of Federal Regulations (or any corresponding similar regulation or ruling).

(3) DEPUTIZATION BY OTHER FEDERAL AGENCIES.—The Administrator may request another Federal agency to deputize, as Federal flight deck officers under this section, pilots that the Administrator determines are qualified to be Federal flight deck officers.

(4) REVOCATION.—The Administrator may revoke the deputization of a pilot as a Federal flight deck officer if the Administrator finds that the pilot is no longer qualified to be a Federal flight deck officer.

(5) TRANSFER FROM INACTIVE TO ACTIVE STATUS.—In accordance with any applicable Transportation Security Administration appeals processes, a pilot deputized as a Federal flight deck officer who moves to inactive status may return to active status on successful completion of a recurrent training program administered within program guidelines.

(g) COMPENSATION.—

(1) IN GENERAL.—Pilots participating in the program under this section shall not be eligible for compensation from the Federal Government for services provided as a Federal flight deck officer. The Federal Government and air carriers shall not be obligated to compensate a pilot for participating in the program or for the pilot's training or qualification and requalification to carry firearms under the program.

(2) FACILITATION OF TRAINING.—An air carrier shall permit a pilot seeking to be deputized as a Federal flight deck officer or a Federal flight deck officer to take a reasonable amount of leave to participate in initial, recurrent, or requalification training, as applicable, for the program. Leave required under this paragraph may be provided without compensation.

(h) AUTHORITY TO CARRY FIREARMS.—

(1) IN GENERAL.—The Administrator shall authorize a Federal flight deck officer to carry a firearm while engaged in providing air transportation or intrastate air transportation. Notwithstanding subsection (e)(1), the officer may purchase a firearm and carry that firearm aboard an aircraft of which the officer is the pilot under this section if the firearm is of a type that may be used under the program.

(2) PREEMPTION.—Notwithstanding another Federal or State law, a Federal flight deck officer, whenever necessary to participate in the program, may carry a firearm in a State and from one State to another State.

(3) CARRYING FIREARMS OUTSIDE UNITED STATES.—In consultation with the Secretary of State, the Administrator may take necessary action to ensure that a Federal flight deck officer may carry a firearm in a foreign country whenever necessary to participate in the program.

(4) CONSISTENCY WITH FEDERAL AIR MARSHAL PROGRAM.—The Administrator shall harmonize, to the extent practicable and in a manner that does not jeopardize existing Federal air marshal agreements, the policies relating to the carriage of firearms on international flights by Federal flight deck officers with the policies of the Federal air marshal program for carrying firearms on international flights and carrying out the duties of a Federal flight deck officer, notwithstanding Annex 17 of the International Civil Aviation Organization.

(i) AUTHORITY TO USE FORCE.—Notwithstanding section 40913(d) of this title, the Administrator shall prescribe the standards and circumstances under which a Federal flight deck officer may use, while the program under this section is in effect, force (including lethal force) against an individual in the defense of the flight deck of an aircraft in air transportation or intrastate air transportation.

(j) LIMITATION ON LIABILITY.—

(1) AIR CARRIERS.—An air carrier is not liable for damages in an action brought in a Federal or State court arising out of a Federal flight deck officer's use of or failure to use a firearm.

(2) FEDERAL FLIGHT DECK OFFICERS.—A Federal flight deck officer is not liable for damages in an action brought in a Federal or State court arising out of the acts or omissions of the officer in defending the flight deck of an aircraft against acts of criminal violence or air piracy unless the officer is guilty of gross negligence or willful misconduct.

(3) FEDERAL GOVERNMENT.—For purposes of an action against the United States with respect to an act or omission of a Federal flight deck officer in defending the flight deck of an aircraft, the officer shall

be treated as an employee of the Federal Government under chapter 171 of title 28, relating to tort claims procedure.

(k) PROCEDURES FOLLOWING ACCIDENTAL DISCHARGES.—If an accidental discharge of a firearm under the pilot program results in the injury or death of a passenger or crew member on an aircraft—

(1) the Administrator shall revoke the deputization of the Federal flight deck officer responsible for that firearm if the Administrator determines that the discharge was attributable to the negligence of the officer; and

(2) if the Administrator determines that a shortcoming in standards, training, or procedures was responsible for the accidental discharge, the Administrator may temporarily suspend the program until the shortcoming is corrected.

(l) LIMITATION ON AUTHORITY OF AIR CARRIERS.—An air carrier may not—

(1) prohibit a pilot employed by the air carrier from becoming a Federal flight deck officer under this section;

(2) threaten a retaliatory action against a pilot employed by the air carrier for becoming a Federal flight deck officer under this section;

(3) prohibit a Federal flight deck officer from piloting an aircraft operated by the air carrier; or

(4) terminate the employment of a Federal flight deck officer, solely on the basis of his or her volunteering for or participating in the program under this section.

(m) CLASSIFY INFORMATION AS SENSITIVE SECURITY INFORMATION.—Not later than 180 days after October 5, 2018—

(1) the Secretary of Transportation shall revise section 15.5(b)(11) of title 49, Code of Federal Regulations, to classify information about pilots deputized as Federal flight deck officers under this section as sensitive security information in a manner consistent with the classification of information about Federal air marshals; and

(2) the Administrator shall revise section 1520.5(b)(11) of title 49, Code of Federal Regulations, to classify information about pilots deputized as Federal flight deck officers under this section as sensitive security information in a manner consistent with the classification of information about Federal air marshals.

(n) REGULATIONS.—Not later than 180 days after October 5, 2018, the Administrator shall prescribe such regulations as may be necessary to carry out this section.

§ 40933. Deputization of State and local law enforcement officers

(a) DEPUTIZATION AUTHORITY.—The Administrator may deputize a State or local law enforcement officer to carry out Federal airport security duties under this chapter.

(b) FULFILLMENT OF REQUIREMENTS.—A State or local law enforcement officer who is deputized under this section shall be treated as a Federal law enforcement officer for purposes of meeting the requirements of this chapter and other provisions of law to provide Federal law enforcement officers to carry out Federal airport security duties.

(c) AGREEMENTS.—To deputize a State or local law enforcement officer under this section, the Administrator shall enter into a voluntary agreement with the appropriate State or local law enforcement agency that employs the State or local law enforcement officer.

(d) REIMBURSEMENT.—The Administrator shall reimburse a State or local law enforcement agency for all reasonable, allowable, and allocable costs incurred by the State or local law enforcement agency with respect to a law enforcement officer deputized under this section.

(e) FEDERAL TORT CLAIMS ACT.—A State or local law enforcement officer who is deputized under this section shall be treated as an ''employee of the Government'' for purposes of sections 1346(b) and 2401(b) and chapter 171 of title 28 while carrying out Federal airport security duties in the course and scope of the officer's employment, subject to Federal supervision and control, and under the terms of the deputization.

(f) STATIONING OF OFFICERS.—The Administrator may allow law enforcement personnel to be stationed other than at the airport security screening location if that would be preferable for law enforcement purposes and if the personnel would still be able to provide a prompt response to problems occurring at the screening location.

§ 40934. Airport security improvement projects

(a) DEFINITION OF SPONSOR.—In this section, the term ''sponsor'' has the meaning given the term in section 47102 of title 49.

(b) GRANT AUTHORITY.—Subject to the requirements of this section, the Administrator shall make grants to airport sponsors—

(1) for projects to replace baggage conveyer systems related to aviation security;

(2) for projects to reconfigure terminal baggage areas as needed to install explosive detection systems;

(3) for projects to enable the Administrator to deploy explosive detection systems behind the ticket counter, in the baggage sorting area, or in line with the baggage handling system; and

(4) for other airport security capital improvement projects.

(c) APPLICATIONS.—A sponsor seeking a grant under this section shall submit to the Administrator an application in the form, and containing the information, the Administrator prescribes.

(d) APPROVAL.—The Administrator, after consultation with the Secretary of Transportation, may approve an application of a sponsor for a grant under this section only if the Administrator determines that the project will improve security at an airport or improve the efficiency of the airport without lessening security.

(e) LETTERS OF INTENT.—

(1) ISSUANCE.—The Administrator shall issue a letter of intent to a sponsor committing to obligate from future budget authority an amount, not more than the Federal Government's share of the project's cost, for an airport security improvement project (including interest costs and costs of formulating the project).

(2) SCHEDULE.—A letter of intent under this subsection shall establish a schedule under which the Administrator will reimburse the sponsor for the Government's share of the project's costs, as amounts become available, if the sponsor, after the Administrator issues the letter, carries out the project without receiving amounts under this section.

(3) NOTICE TO ADMINISTRATOR.—A sponsor that has been issued a letter of intent under this subsection shall notify the Administrator of the sponsor's intent to carry out a project before the project begins.

(4) NOTICE TO CONGRESS.—The Administrator shall transmit to the Committee on Appropriations and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Appropriations and the Committee on Commerce, Science, and Transportation of the Senate a written notification at least 3 days before the issuance of a letter of intent under this section.

(5) LIMITATIONS.—A letter of intent issued under this subsection is not an obligation of the Government under section 1501 of title 31, and the letter is not deemed to be an administrative commitment for financing. An obligation or administrative commitment may be made only as amounts are provided in authorization and appropriations laws.

(6) STATUTORY CONSTRUCTION.—Nothing in this subsection shall be construed to prohibit the obligation of amounts pursuant to a letter of intent under this subsection in the same fiscal year as the letter of intent is issued.

(f) FEDERAL SHARE.—The Government's share of the cost of a project under this section shall be 90 percent for a project at a medium or large hub airport and 95 percent for a project at any other airport.

(g) APPLICABILITY OF CERTAIN REQUIREMENTS.—The requirements that apply to grants and letters of intent issued under chapter 471 of title 49 (other than section 47102(3)) shall apply to grants and letters of intent issued under this section.

(h) AVIATION SECURITY CAPITAL FUND.—

(1) IN GENERAL.—There is established in the Department the Aviation Security Capital Fund. The first $250,000,000 from fees received under section 40960(a) of this title in each of fiscal years 2004 through 2028 is available to be deposited in the Fund. The Administrator shall impose the fee authorized by section 40960(a) of this title so as to collect at least $250,000,000 in each of the fiscal years for deposit into the Fund. Amounts in the Fund are available to the Administrator to make grants under this section.

(2) ALLOCATION.—Of the amount made available under paragraph (1) for a fiscal year, not less than $200,000,000 shall be allocated to fulfill letters of intent issued under subsection (e).

(3) DISCRETIONARY GRANTS.—Of the amount made available under paragraph (1) for a fiscal year, up to $50,000,000 shall be used to make discretionary grants, including other transaction agreements for airport security improvement projects, with priority given to small hub airports and nonhub airports.

(i) LEVERAGED FUNDING.—For purposes of this section, a grant under subsection (b) to an airport sponsor to service an obligation issued by or on behalf of that sponsor to fund a project described in subsection (b) is considered to be a grant for that project.

§ 40935. Repair station security

(a) SECURITY REVIEW AND AUDIT.—To ensure the security of maintenance and repair work conducted on air carrier aircraft and components at foreign repair stations, the Administrator, in consultation with the Administrator of the Federal Aviation Administration, shall complete a security review and audit of foreign repair stations that are certified by the Administrator of the Federal Aviation Administration under part 145 of title 14, Code of Federal Regulations, and that work on air carrier aircraft and components. The review shall be completed no later than 6 months after the date on which the Administrator issues regulations under subsection (f).

(b) ADDRESSING SECURITY CONCERNS.—The Administrator shall require a foreign repair station to address the security issues and vulnerabilities identified in a security audit conducted under subsection (a) within 90 days of providing notice to the repair station of the security issues and vulnerabilities so identified and shall notify the Administrator of the Federal

Aviation Administration that a deficiency was identified in the security audit.

(c) SUSPENSIONS AND REVOCATIONS OF CERTIFICATES.—

(1) FAILURE TO CARRY OUT EFFECTIVE SECURITY MEASURES.—If, after the 90th day on which a notice is provided to a foreign repair station under subsection (b), the Administrator determines that the foreign repair station does not maintain and carry out effective security measures, the Administrator shall notify the Administrator of the Federal Aviation Administration of the determination. On receipt of the determination, the Administrator of the Federal Aviation Administration shall suspend the certification of the repair station until the Administrator determines that the repair station maintains and carries out effective security measures and transmits the determination to the Administrator of the Federal Aviation Administration.

(2) IMMEDIATE SECURITY RISK.—If the Administrator determines that a foreign repair station poses an immediate security risk, the Administrator shall notify the Administrator of the Federal Aviation Administration of the determination. On receipt of the determination, the Administrator of the Federal Aviation Administration shall revoke the certification of the repair station.

(3) PROCEDURES FOR APPEALS.—The Administrator, in consultation with the Administrator of the Federal Aviation Administration, shall establish procedures for appealing a revocation of a certificate under this subsection.

(d) FAILURE TO MEET AUDIT DEADLINE.—If the security audits required by subsection (a) are not completed on or before the date that is 6 months after the date on which the Administrator issues regulations under subsection (f), the Administrator of the Federal Aviation Administration shall be barred from certifying a foreign repair station (other than a station that was previously certified, or is in the process of certification, by the Administrator of the Federal Aviation Administration under part A of subtitle VII of title 49) until the audits are completed for existing stations.

(e) PRIORITY FOR AUDITS.—In conducting the audits described in subsection (a), the Administrator and the Administrator of the Federal Aviation Administration shall give priority to foreign repair stations located in countries identified by the Government as posing the most significant security risks.

(f) REGULATIONS.—The Administrator, in consultation with the Administrator of the Federal Aviation Administration, shall issue final regulations to ensure the security of foreign and domestic aircraft repair stations.

§ 40936. Deployment and use of detection equipment at airport screening checkpoints

(a) WEAPONS AND EXPLOSIVES.—The Secretary shall give a high priority to developing, testing, improving, and deploying, at airport screening checkpoints, equipment that detects nonmetallic, chemical, biological, and radiological weapons, and explosives, in all forms, on individuals and in their personal property. The Secretary shall ensure that the equipment alone, or as part of an integrated system, can detect under realistic operating conditions the types of weapons and explosives that terrorists would likely try to smuggle aboard an air carrier aircraft.

(b) STRATEGIC PLAN FOR DEPLOYMENT AND USE OF EXPLOSIVE DETECTION EQUIPMENT AT AIRPORT SCREENING CHECKPOINTS.—

(1) IN GENERAL.—The Administrator shall submit to the appropriate congressional committees a strategic plan to promote the optimal utilization and deployment of explosive detection equipment at airports to screen individuals and their personal property. Such equipment includes walk-through explosive detection portals, document scanners, shoe scanners, and backscatter x-ray scanners. The plan may be submitted in a classified format.

(2) CONTENT.—The strategic plan shall include, at minimum—

(A) a description of current efforts to detect explosives in all forms on individuals and in their personal property;

(B) a description of the operational applications of explosive detection equipment at airport screening checkpoints;

(C) a deployment schedule and a description of the quantities of equipment needed to implement the plan;

(D) a description of funding needs to implement the plan, including a financing plan that provides for leveraging of non-Federal funding;

(E) a description of the measures taken and anticipated to be taken in carrying out subsection (d); and

(F) a description of any recommended legislative actions.

(c) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Secretary for the use of the Transportation Security Administration $250,000,000, in addition to amounts otherwise authorized by law, for research, development, and installation of detection systems and other devices for the detection of biological, chemical, radiological, and explosive materials.

(d) INTERIM ACTION.—Until measures are implemented that enable the screening of all passengers for explosives, the Administrator shall provide, by means the Administrator considers appropriate, explosives detection

screening for all passengers identified for additional screening and their personal property that will be carried aboard a passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation.

§ 40937. Appeal and redress process for passengers wrongly delayed or prohibited from boarding a flight

(a) IN GENERAL.—The Secretary shall establish a timely and fair process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat under the regimes utilized by the Transportation Security Administration, U.S. Customs and Border Protection, or another office or component of the Department.

(b) OFFICE OF APPEALS AND REDRESS.—

(1) ESTABLISHMENT.—The Secretary shall establish in the Department an Office of Appeals and Redress to implement, coordinate, and execute the process established by the Secretary under subsection (a). The Office shall include representatives from the Transportation Security Administration, U.S. Customs and Border Protection, and other offices and components of the Department that the Secretary determines appropriate.

(2) RECORDS.—The process established by the Secretary under subsection (a) shall include the establishment of a method by which the Office, under the direction of the Secretary, will be able to maintain a record of air carrier passengers and other individuals who have been misidentified and have corrected erroneous information.

(3) INFORMATION.—To prevent repeated delays of a misidentified passenger or other individual, the Office of Appeals and Redress shall—

(A) ensure that the records maintained under this subsection contain information determined by the Secretary to authenticate the identity of the passenger or individual;

(B) furnish to the Transportation Security Administration, U.S. Customs and Border Protection, or another appropriate office or component of the Department, on request, information necessary to allow the office or component to assist air carriers in improving their administration of the advanced passenger prescreening system and reduce the number of false positives; and

(C) require that air carriers and foreign air carriers take action to identify passengers determined, under the process established under subsection (a), to have been wrongly identified.

(4) HANDLING OF PERSONALLY IDENTIFIABLE INFORMATION.—The Secretary, in conjunction with the Chief Privacy Officer of the Department, shall—

(A) require that Federal employees of the Department handling personally identifiable information of passengers (in this paragraph referred to as ''PII'') complete mandatory privacy and security training prior to being authorized to handle PII;

(B) ensure that the records maintained under this subsection are secured by encryption, one-way hashing, other data anonymization techniques, or other, equivalent security technical protections the Secretary determines necessary;

(C) limit the information collected from misidentified passengers or other individuals to the minimum amount necessary to resolve a redress request;

(D) require that the data generated under this subsection shall be shared or transferred via a secure data network that has been audited to ensure that the anti-hacking and other security related software functions properly and is updated as necessary;

(E) ensure that an employee of the Department receiving the data contained in the records handles the information under section 552a of title 5 and the Federal Information Security Management Act of 2002 (Public Law 107–296, 116 Stat. 2259);

(F) only retain the data for as long as needed to assist the individual traveler in the redress process; and

(G) conduct and publish a privacy impact assessment of the process described within this subsection and transmit the assessment to the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, and the Committee on Homeland Security and Governmental Affairs of the Senate.

(5) INITIATION OF REDRESS PROCESS AT AIRPORTS.—The Office of Appeals and Redress shall establish at each airport at which the Department has a significant presence a process to provide information to air carrier passengers to begin the redress process established under subsection (a).

§ 40938. Expedited screening for severely injured or disabled members of the armed forces and severely injured or disabled veterans

(a) PASSENGER SCREENING.—The Administrator, in consultation with the Secretary of Defense, the Secretary of Veterans Affairs, and organizations identified by the Secretaries of Defense and Veterans Affairs that ad-

vocate on behalf of severely injured or disabled members of the armed forces and severely injured or disabled veterans, shall develop and implement a process to support and facilitate the ease of travel and to the extent possible provide expedited passenger screening services through passenger screening for severely injured or disabled members of the armed forces and severely injured or disabled veterans. The process shall be designed to offer the individual private screening to the maximum extent practicable.

(b) OPERATIONS CENTER.—As part of the process under subsection (a), the Administrator shall maintain an operations center to provide support and facilitate the movement of severely injured or disabled members of the armed forces and severely injured or disabled veterans through passenger screening prior to boarding a passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation.

(c) PROTOCOLS.—The Administrator shall—

(1) establish and publish protocols, in consultation with the Secretary of Defense, the Secretary of Veterans Affairs, and the organizations identified under subsection (a), under which a severely injured or disabled member of the armed forces or severely injured or disabled veteran, or the family member or other representative of the member or veteran, may contact the operations center maintained under subsection (b) and request the expedited passenger screening services described in subsection (a) for that member or veteran; and

(2) on receipt of a request under paragraph (1), require the operations center to notify the appropriate Federal Security Director of the request for expedited passenger screening services, as described in subsection (a), for that member or veteran.

(d) TRAINING.—The Administrator shall integrate training on the protocols established under subsection (c) into the training provided to all employees who will regularly provide the passenger screening services described in subsection (a).

(e) RULE OF CONSTRUCTION.—Nothing in this section shall affect the authority of the Administrator to require additional screening of a severely injured or disabled member of the armed forces, a severely injured or disabled veteran, or their accompanying family members or nonmedical attendants, if intelligence, law enforcement, or other information indicates that additional screening is necessary.

(f) REPORT.—The Administrator each year shall submit to Congress a report on the implementation of this section. Each report shall include the following:

(1) Information on the training provided under subsection (d).

(2) Information on the consultations between the Administrator and the organizations identified under subsection (a).

(3) The number of people who accessed the operations center during the period covered by the report.

(4) Other information the Administrator determines is appropriate.

§ 40939. Honor Flight program

The Administrator shall establish, in collaboration with the Honor Flight Network or other not-for-profit organization that honors veterans, a process for providing expedited and dignified passenger screening services for veterans traveling on an Honor Flight Network private charter, or another not-for-profit organization that honors veterans, to visit war memorials built and dedicated to honor the service of those veterans.

§ 40940. Donation of screening equipment to protect the United States

(a) IN GENERAL.—Subject to subsection (b), the Administrator may donate security screening equipment to a foreign last point of departure airport operator if the equipment can be reasonably expected to mitigate a specific vulnerability to the security of the United States or United States citizens.

(b) CONDITIONS.—Before donating any security screening equipment to a foreign last point of departure airport operator, the Administrator shall—

(1) ensure that the screening equipment has been restored to commercially available settings;

(2) ensure that no Transportation Security Administration-specific security standards or algorithms exist on the screening equipment; and

(3) verify that the appropriate officials have an adequate system—

(A) to properly maintain and operate the screening equipment; and

(B) to document and track any removal or disposal of the screening equipment to ensure the screening equipment does not come into the possession of terrorists or otherwise pose a risk to security.

(c) REPORTS.—Not later than 30 days before a donation of security screening equipment under subsection (a), the Administrator shall provide to 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 of the House of Representatives a detailed written explanation of the following:

(1) The specific vulnerability to the United States or United States citizens that will be mitigated by the donation.

(2) An explanation as to why the recipient of the donation is unable or unwilling to purchase security screening equipment to mitigate the vulnerability.

(3) An evacuation plan for sensitive technologies in case of emergency or instability in the country to which the donation is being made.

(4) How the Administrator will ensure the security screening equipment that is being donated is used and maintained over the course of its life by the recipient.

(5) The total dollar value of the donation.

(6) How the appropriate officials will document and track removal or disposal of the screening equipment by the recipient to ensure the screening equipment does not come into the possession of terrorists or otherwise pose a risk to security.

Subchapter III—Administration and Personnel

§ 40951. Authority to exempt from regulations

The Secretary may grant an exemption from a regulation prescribed in carrying out sections 40911, 40913, 40919(c), and 40955 through 40957 of this title when the Secretary decides the exemption is in the public interest.

§ 40952. Administrative

(a) IN GENERAL.—The Secretary or the Administrator may take action the Administrator considers necessary to carry out sections 11522 through 11524(a) of this title, subchapters I and II of this chapter, sections 40951 through 40961 of this title, subchapter V of this chapter, and chapter 465 of title 49, including conducting investigations, prescribing regulations, standards, and procedures, and issuing orders.

(b) INDEMNIFICATION.—The Administrator may indemnify an officer or employee of the Transportation Security Administration against a claim or judgment arising out of an act that the Administrator decides was committed within the scope of the official duties of the officer or employee.

§ 40953. Federal Security Directors

(a) ESTABLISHMENT, DESIGNATION, AND STATIONING.—The Administrator shall establish the position of Federal Security Director at each airport in the United States described in section 40913(c) of this title. The Administrator shall designate individuals as Federal Security Directors for, and station those Federal Security Directors at, those airports.

(b) DUTIES AND POWERS.—The Federal Security Director at each airport shall—

(1) oversee the screening of passengers and property at the airport; and

(2) carry out other duties prescribed by the Administrator.

(c) INFORMATION SHARING.—Not later than 1 year after October 5, 2018, the Administrator shall—

(1) require each Federal Security Director of an airport to meet at least quarterly with the airport director, airport security coordinator, and law enforcement agencies serving the airport to discuss incident management protocols, including the resolution of screening anomalies at passenger screening checkpoints; and

(2) require each Federal Security Director at an airport to inform, consult, and coordinate, as appropriate, with the respective airport security coordinator in a timely manner on security matters impacting airport operations and to establish and maintain operational protocols with the airport operators to ensure coordinated responses to security matters.

§ 40954. Foreign Security Liaison Officers

(a) ESTABLISHMENT, DESIGNATION, AND STATIONING.—The Administrator shall establish the position of Foreign Security Liaison Officer for each airport outside the United States at which the Administrator decides an Officer is necessary for air transportation security. In coordination with the Secretary of State, the Administrator shall designate an Officer for each of those airports. In coordination with the Secretary of State, the Administrator shall designate an Officer for each of those airports where extraordinary security measures are in place. The Secretary of State shall give high priority to stationing those Officers.

(b) DUTIES AND POWERS.—Each Federal Security Liaison Officer reports directly to the Administrator. The Officer at each airport shall—

(1) serve as the liaison of the Administrator to foreign security authorities (including governments of foreign countries and foreign airport authorities) in carrying out United States Government security requirements at that airport; and

(2) to the extent practicable, carry out duties and powers referred to in section 40953(b) of this title.

(c) COORDINATION OF ACTIVITIES.—The activities of each Foreign Security Liaison Officer shall be coordinated with the chief of the diplomatic mission of the United States to which the Officer is assigned. Activities of an Officer under this section shall be consistent with the duties and powers of the Secretary of State and the chief of mission to a foreign country under section 103 of the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (22 U.S.C. 4802) and section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927).

§ 40955. Employment standards and training

(a) EMPLOYMENT STANDARDS.—The Administrator shall prescribe standards for the employment and continued employment of, and contracting for, air carrier personnel and, as appropriate, airport security personnel. The standards shall include—

(1) minimum training requirements for new employees;

(2) retraining requirements;

(3) minimum staffing levels;

(4) minimum language skills; and

(5) minimum education levels for employees, when appropriate.

(b) REVIEW AND RECOMMENDATIONS.—In coordination with air carriers, airport operators, and other interested persons, the Administrator shall review issues related to human performance in the aviation security system to maximize that performance. When the review is completed, the Administrator shall recommend guidelines and prescribe appropriate changes in existing procedures to improve that performance.

(c) SECURITY PROGRAM TRAINING, STANDARDS, AND QUALIFICATIONS.—

(1) IN GENERAL.—The Administrator—

(A) may train individuals employed to carry out a security program under section 40913(c) of this title; and

(B) shall prescribe uniform training standards and uniform minimum qualifications for individuals eligible for that training.

(2) REIMBURSEMENTS.—The Administrator may authorize reimbursement for travel, transportation, and subsistence expenses for security training of non-United States Government domestic and foreign individuals whose services will contribute significantly to carrying out civil aviation security programs. To the extent practicable, air travel reimbursed under this paragraph shall be on air carriers.

(d) EDUCATION AND TRAINING STANDARDS FOR SECURITY COORDINATORS, SUPERVISORY PERSONNEL, AND PILOTS.—

(1) IN GENERAL.—The Administrator shall prescribe standards for educating and training—

(A) ground security coordinators;

(B) security supervisory personnel; and

(C) airline pilots as in-flight security coordinators.

(2) ELEMENTS.—The standards shall include initial training, retraining, and continuing education requirements and methods. The requirements and methods shall be used annually to measure the performance of ground security coordinators and security supervisory personnel.

(e) SECURITY SCREENERS.—

(1) TRAINING PROGRAM.—The Administrator shall establish a program for the hiring and training of security screening personnel.

(2) HIRING.—

(A) QUALIFICATIONS.—The Administrator shall establish qualification standards for individuals to be hired by the United States as security screening personnel. Notwithstanding another law, the standards shall require, at a minimum, an individual—

(i) to have a satisfactory or better score on a Federal security screening personnel selection examination;

(ii) to be a citizen of the United States or a national of the United States, as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a));

(iii) to meet, at a minimum, the requirements set forth in subsection (f);

(iv) to meet other qualifications the Administrator may establish; and

(v) to have the ability to demonstrate daily a fitness for duty without an impairment due to illegal drugs, sleep deprivation, medication, or alcohol.

(B) BACKGROUND CHECKS.—The Administrator shall require that an individual to be hired as a security screener undergo an employment investigation (including a criminal history record check) under section 40956(a)(1) of this title.

(C) DISQUALIFICATION OF INDIVIDUALS WHO PRESENT NATIONAL SECURITY RISKS.—The Administrator, in consultation with the heads of other appropriate Federal agencies, shall establish procedures, in addition to any background check conducted under section 40956 of this title, to ensure that an individual who presents a threat to national security is not employed as a security screener.

(3) EXAMINATION.—The Administrator shall develop a security screening personnel examination for use in determining the qualification of individuals seeking employment as security screening personnel.

(4) REVIEW OF STANDARDS, RULES, AND REGULATIONS.—The Administrator shall review, and revise as necessary, a standard, rule, or regulation governing the employment of individuals as security screening personnel.

(f) EMPLOYMENT STANDARDS FOR SCREENING PERSONNEL.—

(1) SCREENER REQUIREMENTS.—Notwithstanding another law, an individual may not be deployed as a security screener unless that individual meets the following requirements:

(A) EDUCATION OR EXPERIENCE.—The individual possesses a high school diploma, a general equivalency diploma, or experience that the Administrator has determined to be sufficient for the individual to perform the duties of the position.

(B) BASIC APTITUDES AND PHYSICAL ABILITIES.—The individual possesses basic aptitudes and physical abilities, including color perception, visual and aural acuity, physical coordination, and motor skills, to the following standards:

(i) Screeners operating screening equipment are able to distinguish on the screening equipment monitor the appropriate imaging standard specified by the Administrator.

(ii) Screeners operating screening equipment are able to distinguish each color displayed on every type of screening equipment and explain what each color signifies.

(iii) Screeners are able to hear and respond to the spoken voice and to audible alarms generated by screening equipment in an active checkpoint environment.

(iv) Screeners performing physical searches or other related operations are able to efficiently and thoroughly manipulate and handle the baggage, containers, and other objects subject to security processing.

(v) Screeners performing pat-downs or hand-held metal detector searches of individuals have sufficient dexterity and capability to thoroughly conduct those procedures over an individual's entire body.

(C) READ, WRITE, AND SPEAK ENGLISH.—The individual is able to read, speak, and write English well enough to—

(i) carry out written and oral instructions regarding the proper performance of screening duties;

(ii) read English language identification media, credentials, airline tickets, and labels on items normally encountered in the screening process;

(iii) provide direction to and understand and answer questions from English-speaking individuals undergoing screening; and

(iv) write incident reports and statements and log entries into security records in the English language.

(D) TRAINING.—The individual has satisfactorily completed all initial, recurrent, and appropriate specialized training required by the security program, except as provided in paragraph (3).

(2) VETERANS PREFERENCE.—The Administrator shall provide a preference for the hiring of an individual as a security screener if the individual is a member or former member of the armed forces and if the individual is entitled, under statute, to retired, retirement, or retainer pay on account of service as a member of the armed forces.

(3) EXCEPTIONS.—An individual who has not completed the training required by this section may be deployed during the on-the-job portion of training to perform functions if that individual—

(A) is closely supervised; and

(B) does not make independent judgments as to whether individuals or property may enter a sterile area or aircraft without further inspection.

(4) REMEDIAL TRAINING.—No individual employed as a security screener may perform a screening function after that individual has failed an operational test related to that function until that individual has successfully completed the remedial training specified in the security program.

(5) ANNUAL PROFICIENCY REVIEW.—The Administrator shall provide that an annual evaluation of each individual assigned screening duties is conducted and documented. An individual employed as a security screener may not continue to be employed in that capacity unless the evaluation demonstrates that the individual—

(A) continues to meet all qualifications and standards required to perform a screening function;

(B) has a satisfactory record of performance and attention to duty based on the standards and requirements in the security program; and

(C) demonstrates the current knowledge and skills necessary to courteously, vigilantly, and effectively perform screening functions.

(6) OPERATIONAL TESTING.—In addition to the annual proficiency review conducted under paragraph (5), the Administrator shall provide for the operational testing of personnel.

(g) TRAINING.—

(1) USE OF OTHER AGENCIES.—The Administrator may enter into a memorandum of understanding or other arrangement with another Federal agency or department with appropriate law enforcement responsibilities, to provide personnel, resources, or other forms of assistance in the training of security screening personnel.

(2) TRAINING PLAN.—The Administrator shall develop a plan for the training of security screening personnel. The plan shall require, at a minimum, that a security screener—

(A) has completed 40 hours of classroom instruction or successfully completed a program that the Administrator determines will train individuals to a level of proficiency equivalent to the level that would be achieved by the classroom instruction;

(B) has completed 60 hours of on-the-job instructions; and

(C) has successfully completed an on-the-job training examination prescribed by the Administrator.

(3) EQUIPMENT-SPECIFIC TRAINING.—An individual employed as a security screener may not use a security screening device or equipment in the scope of that individual's employment unless the individual has been trained on that device or equipment and has successfully completed a test on the use of the device or equipment.

(h) TECHNOLOGICAL TRAINING.—

(1) DEFINITION OF DUAL-USE ITEM.—In this subsection, the term ''dual-use item'' means an item that may seem harmless but that may be used as a weapon.

(2) IN GENERAL.—The Administrator shall require training to ensure that screeners are proficient in using the most up-to-date new technology and to ensure their proficiency in recognizing new threats and weapons.

(3) PERIODIC ASSESSMENTS.—The Administrator shall make periodic assessments to determine if there are dual-use items and inform security screening personnel of the existence of the items.

(4) CURRENT LISTS OF DUAL-USE ITEMS.—Current lists of dual-use items shall be part of the ongoing training for screeners.

(i) LIMITATION ON RIGHT TO STRIKE.—An individual who screens passengers or property, or both, at an airport under this section may not participate in a strike, or assert the right to strike, against the person (including a governmental entity) employing the individual to perform the screening.

(j) UNIFORMS.—The Administrator shall require an individual who screens passengers and property under section 40911 of this title to be attired while on duty in a uniform approved by the Administrator.

(k) ACCESSIBILITY OF COMPUTER-BASED TRAINING FACILITIES.—The Administrator shall work with air carriers and airports to ensure that computer-based training facilities intended for use by security screeners at an airport regularly serving an air carrier holding a certificate issued by the

Secretary of Transportation are conveniently located for that airport and easily accessible.

(l) INITIAL AND RECURRING TRAINING.—

(1) INITIAL TRAINING.—The Administrator shall establish a training program for new security screening personnel located at the Transportation Security Administration Academy.

(2) RECURRING TRAINING.—

(A) IN GENERAL.—Not later than 180 days after October 5, 2018, the Administrator shall establish recurring training for security screening personnel regarding updates to screening procedures and technologies, including, in response to weaknesses identified in covert tests at airports—

(i) methods to identify the verification of false or fraudulent travel documents; and

(ii) training on emerging threats.

(B) CONTENTS.—The training under subparagraph (A) shall include—

(i) internal controls for monitoring and documenting compliance of transportation security officers with the training requirements; and

(ii) such other matters as are identified by the Administrator with regard to the training.

§ 40956. Employment investigations and restrictions

(a) EMPLOYMENT INVESTIGATION REQUIREMENT.—

(1) IN GENERAL.—

(A) EMPLOYEE COVERAGE.—The Administrator shall require by regulation that an employment investigation, including a criminal history record check and a review of available law enforcement data bases and records of other governmental and international agencies, to the extent determined practicable by the Administrator, shall be conducted of each individual employed in, or applying for, a position as a security screener under section 40955(e) of this title or a position in which the individual has unescorted access, or may permit other individuals to have unescorted access, to—

(i) aircraft of an air carrier or foreign air carrier; or

(ii) a secured area of an airport in the United States the Administrator designates that serves an air carrier or foreign air carrier.

(B) FURTHER COVERAGE.—The Administrator shall require by regulation that an employment investigation (including a criminal

history record check and a review of available law enforcement data bases and records of other governmental and international agencies, to the extent determined practicable by the Administrator) be conducted for—

(i) individuals who are responsible for screening passengers or property under section 40911 of this title;

(ii) supervisors of the individuals described in clause (i);

(iii) individuals who regularly have escorted access to aircraft of an air carrier or foreign air carrier or a secured area of an airport in the United States the Administrator designates that serves an air carrier or foreign air carrier; and

(iv) other individuals who exercise security functions associated with baggage or cargo that the Administrator determines is necessary to ensure air transportation security.

(C) EXEMPTION.—An employment investigation, including a criminal history record check, is not required under this subsection for an individual who is exempted under section 107.31(m)(1) or (2) of title 14, Code of Federal Regulations, as in effect on November 22, 2000. The Administrator shall work with the International Civil Aviation Organization and with appropriate authorities of foreign countries to ensure that individuals exempted under this subparagraph do not pose a threat to aviation or national security.

(2) EMPLOYER ROLE.—An air carrier, foreign air carrier, airport operator, or government that employs, or authorizes or makes a contract for the services of, an individual in a position described in paragraph (1) shall ensure that the investigation the Administrator requires is conducted.

(3) PERIODIC AUDITS.—The Administrator shall provide for the periodic audit of the effectiveness of criminal history record checks conducted under paragraph (1).

(b) PROHIBITED EMPLOYMENT.—

(1) IN GENERAL.—Except as provided in paragraph (3), an air carrier, foreign air carrier, airport operator, or government may not employ, or authorize or make a contract for the services of, an individual in a position described in subsection (a)(1) if—

(A) the investigation of the individual required under this section has not been conducted; or

(B) the results of that investigation establish that, in the 10-year period ending on the date of the investigation, the individual was convicted (or found not guilty by reason of insanity) of—

(i) a crime referred to in section 41044 of this title, section 32 of title 18, or section 46306, 46308, 46312, or 46315, or chapter 465, of title 49;

(ii) murder;

(iii) assault with intent to murder;

(iv) espionage;

(v) sedition;

(vi) treason;

(vii) rape;

(viii) kidnapping;

(ix) unlawful possession, sale, distribution, or manufacture of an explosive or weapon;

(x) extortion;

(xi) armed or felony unarmed robbery;

(xii) distribution of, or intent to distribute, a controlled substance;

(xiii) a felony involving a threat;

(xiv) a felony involving—

(I) willful destruction of property;

(II) importation or manufacture of a controlled substance;

(III) burglary;

(IV) theft;

(V) dishonesty, fraud, or misrepresentation;

(VI) possession or distribution of stolen property;

(VII) aggravated assault;

(VIII) bribery; and

(IX) illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year, or another crime classified as a felony that the Administrator determines indicates a propensity for placing contraband aboard an aircraft in return for money; or

(xv) conspiracy to commit any of the acts referred to in clauses (i) through (xiv).

(2) OTHER FACTORS.—The Administrator may specify other factors that are sufficient to prohibit the employment of an individual in a position described in subsection (a)(1).

(3) ALTERNATE SECURITY ARRANGEMENTS.—An air carrier, foreign air carrier, airport operator, or government may employ, or authorize or contract for the services of, an individual in a position described in

subsection (a)(1) without carrying out the investigation required under this section, if the Administrator approves a plan to employ the individual that provides alternate security arrangements.

(c) FINGERPRINTING AND RECORD CHECK INFORMATION.—

(1) IN GENERAL.—If the Administrator requires an identification and criminal history record check, to be conducted by the Attorney General, as part of an investigation under this section, the Administrator shall designate an individual to obtain fingerprints and submit those fingerprints to the Attorney General. The Attorney General may make the results of a check available to an individual the Administrator designates. Before designating an individual to obtain and submit fingerprints or receive results of a check, the Administrator shall consult with the Attorney General. All Federal agencies shall cooperate with the Administrator and the Administrator's designee in the process of collecting and submitting fingerprints.

(2) REGULATIONS.—The Administrator shall prescribe regulations on—

(A) procedures for taking fingerprints; and

(B) requirements for using information received from the Attorney General under paragraph (1)—

(i) to limit the dissemination of the information; and

(ii) to ensure that the information is used only to carry out this section.

(3) ACCESS TO INVESTIGATION.—If an identification and criminal history record check is conducted as part of an investigation of an individual under this section, the individual—

(A) shall receive a copy of a record received from the Attorney General; and

(B) may complete and correct the information contained in the check before a final employment decision is made based on the check.

(d) FEES AND CHARGES.—The Administrator and the Attorney General shall establish reasonable fees and charges to pay expenses incurred in carrying out this section. The employer of the individual being investigated shall pay the costs of a record check of the individual. Money collected under this section shall be credited to the account in the Treasury from which the expenses were incurred and shall be available to the Administrator and the Attorney General for those expenses.

(e) WHEN INVESTIGATION OR RECORD CHECK NOT REQUIRED.—This section does not require an investigation or record check when the investigation or record check is prohibited by a law of a foreign country.

§ 40957. Prohibition on transferring duties and powers

Except as specifically provided by law, the Administrator may not transfer a duty or power under section 40913(a), (b), (c), or (e), 40916, 40922(a) through (c), 40955, 40956, or 40958(b)(2) of this title.

§ 40958. Reports

(a) TRANSPORTATION SECURITY.—Not later than March 31 of each year, the Secretary shall submit to Congress a report on transportation security with recommendations the Secretary considers appropriate. The report shall be prepared in conjunction with the biennial report the Administrator submits under subsection (b) in each year the Administrator submits the biennial report, but may not duplicate the information submitted under subsection (b) or section 40917(a)(3) of this title. The Secretary may submit the report in classified and unclassified parts. The report shall include—

(1) an assessment of trends and developments in terrorist activities, methods, and other threats to transportation;

(2) an evaluation of deployment of explosive detection devices;

(3) recommendations for research, engineering, and development activities related to transportation security, except research engineering and development activities related to aviation security to the extent those activities are covered by the national aviation research plan required under section 44501(c) of title 49;

(4) identification and evaluation of cooperative efforts with other departments, agencies, and instrumentalities of the United States Government;

(5) an evaluation of cooperation with foreign transportation and security authorities;

(6) the status of the extent to which the recommendations of the President's Commission on Aviation Security and Terrorism have been carried out and the reasons for delay in carrying out those recommendations;

(7) an assessment of financial and staffing requirements, and the attainment of existing staffing goals, for carrying out the duties and powers of the Administrator relating to security; and

(8) appropriate legislative and regulatory recommendations.

(b) SCREENING AND FOREIGN AIR CARRIER AND AIRPORT SECURITY.—The Administrator shall submit biennially to Congress a report on the effectiveness of procedures under section 40911 (except subsection (e)) of this title that includes—

(1) a summary of the assessments conducted under section 40917(a)(1) and (2) of this title; and

(2) an assessment of the steps being taken, and the progress being made, in ensuring compliance with section 40916 of this title for each foreign air carrier security program at airports outside the United States—

(A) at which the Administrator decides that Foreign Security Liaison Officers are necessary for air transportation security; and

(B) for which extraordinary security measures are in place.

§ 40959. Training to operate certain aircraft

(a) WAITING PERIOD.—

(1) DEFINITION OF TRAINING.—In this subsection, the term ''training''—

(A) means training received from an instructor in an aircraft or aircraft simulator; but

(B) does not include recurrent training, ground training, or demonstration flights for marketing purposes.

(2) REQUIREMENTS.—A person operating as a flight instructor, pilot school, or aviation training center or subject to regulation under part A of subtitle VII of title 49 may provide training in the operation of an aircraft having a maximum certificated takeoff weight of more than 12,500 pounds to an alien (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a))) or to another individual specified by the Secretary only if—

(A) that person has first notified the Secretary that the alien or individual has requested training and submitted to the Secretary, in the form the Secretary prescribes, the following information about the alien or individual:

(i) Full name, including aliases used by the applicant or variations in spelling of the applicant's name.

(ii) Passport and visa information.

(iii) Country of citizenship.

(iv) Date of birth.

(v) Dates of training.

(vi) Fingerprints collected by, or under the supervision of, a Federal, State, or local law enforcement agency or by another entity approved by the Federal Bureau of Investigation or the Secretary, including fingerprints taken by United States Government personnel at a United States embassy or consulate; and

(B) the Secretary has not directed, within 30 days after being notified under subparagraph (A), that person not to provide the

requested training because the Secretary has determined that the individual presents a risk to aviation or national security.

(b) INTERRUPTION OF TRAINING.—If the Secretary, more than 30 days after receiving notification under subsection (a) from a person providing training described in subsection (a), determines that the individual presents a risk to aviation or national security, the Secretary shall immediately notify the person providing the training of the determination, and that person shall immediately terminate the training.

(c) NOTIFICATION.—A person operating as a flight instructor, pilot school, or aviation training center or subject to regulation under part A of subtitle VII of title 49 may provide training in the operation of an aircraft having a maximum certificated takeoff weight of 12,500 pounds or less to an alien (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)) or to another individual specified by the Secretary only if that person has notified the Secretary that the individual has requested the training and furnished the Secretary with that individual's identification in the form the Secretary requires.

(d) EXPEDITED PROCESSING.—The Secretary shall establish a process to ensure that the waiting period under subsection (a) shall not exceed 5 days for an alien (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a))) who—

(1) holds an airman's certification of a foreign country that is recognized by an agency of the United States, including a military agency, that permits an individual to operate a multi-engine aircraft that has a certificated takeoff weight of more than 12,500 pounds;

(2) is employed by a foreign air carrier that is certified under part 129 of title 14, Code of Federal Regulations, and that has a security program approved under part 1546 of title 49, Code of Federal Regulations;

(3) is an individual who has unescorted access to a secured area of an airport designated under section 40956(a)(1)(A)(ii) of this title; or

(4) is an individual who is part of a class of individuals that the Secretary has determined that providing aviation training to presents minimal risk to aviation or national security because of the aviation training already possessed by the class of individuals.

(e) NONAPPLICABILITY TO CERTAIN FOREIGN MILITARY PILOTS.—The procedures and processes required by subsections (a) through (d) do not apply to a foreign military pilot endorsed by the Department of Defense for flight training in the United States and seeking training described in subsection (a)(1) in the United States.

(f) FEE.—

(1) IN GENERAL.—The Secretary may assess a fee for an investigation under this section. The Secretary may adjust the maximum amount of the fee to reflect the costs of an investigation.

(2) OFFSET.—Notwithstanding section 3302 of title 31, a fee collected under this section—

(A) shall be credited to the account in the Treasury from which the expenses were incurred and shall be available to the Secretary for those expenses; and

(B) shall remain available until expended.

(g) INTERAGENCY COOPERATION.—The Attorney General, the Director of National Intelligence, and the Administrator of the Federal Aviation Administration shall cooperate with the Secretary in implementing this section.

(h) SECURITY AWARENESS TRAINING FOR EMPLOYEES.—The Secretary shall require flight schools to conduct a security awareness program for flight school employees to increase their awareness of suspicious circumstances and activities of individuals enrolling in or attending flight school.

§ 40960. Security service fee

(a) GENERAL AUTHORITY.—

(1) PASSENGER FEES.—The Administrator shall impose a uniform fee, on passengers of air carriers and foreign air carriers in air transportation and intrastate air transportation originating at airports in the United States, to pay for the following costs of providing civil aviation security services:

(A) Salary, benefits, overtime, retirement and other costs of screening personnel, their supervisors and managers, Federal law enforcement personnel, and State and local law enforcement officers deputized under section 40933 of this title, who are deployed at airport security screening locations under section 40911 (except subsection (e)) of this title.

(B) The costs of training personnel described in subparagraph (A), and the acquisition, operation, and maintenance of equipment used by the personnel.

(C) The costs of performing background investigations of personnel described in subparagraphs (A), (D), (F), and (G).

(D) The costs of the Federal air marshals program.

(E) The costs of performing civil aviation security research and development under this title.

(F) The costs of Federal Security Directors under section 40913 of this title.

(G) The costs of deploying Federal law enforcement personnel under section 40913(h) of this title.

(H) The costs of security-related capital improvements at airports.

(I) The costs of training pilots and flight attendants under sections 40928 and 40932 of this title.

(2) DETERMINATION OF COSTS.—The amount of the costs listed in paragraph (1) shall be determined by the Administrator and are not subject to judicial review

(b) SCHEDULE OF FEES.—In imposing fees under subsection (a), the Administrator shall ensure that the fees are reasonably related to the Transportation Security Administration's costs of providing services rendered.

(c) LIMITATION ON FEE.—

(1) DEFINITION OF ROUND TRIP.—In this subsection, ''round trip'' means a trip on an air travel itinerary that terminates or has a stopover at the origin point (or co-terminal).

(2) LIMITATION.—The fee imposed under subsection (a) is $5.60 per one-way trip in air transportation or intrastate air transportation that originates at an airport in the United States, except the fee imposed per round trip shall not exceed $11.20.

(3) OFFSETTING COLLECTIONS.—Beginning on October 21, 2027, fees collected under subsection (a)(1) for a fiscal year shall be credited as offsetting collections to appropriations made for aviation security measures carried out by the Transportation Security Administration and shall remain available until expended.

(d) IMPOSITION OF FEE.—

(1) IN GENERAL.—Notwithstanding section 9701 of title 31 and the procedural requirements of section 553 of title 5, the Administrator shall impose the fee under subsection (a) through the publication of notice of the fee in the Federal Register and begin collection of the fee as soon as possible.

(2) SPECIAL RULES FOR PASSENGER FEES.—A fee imposed under subsection (a) through the procedures under paragraph (1) shall apply only to tickets sold after the date on which the fee is imposed. If a fee imposed under subsection (a) through the procedures under paragraph (1) on transportation of a passenger of a carrier described in subsection (a) is not collected from the passenger, the amount of the fee shall be paid by the carrier.

(3) SUBSEQUENT MODIFICATION OF FEE.—After imposing a fee under paragraph (1), the Administrator may modify, from time to time

through publication of notice in the Federal Register, the imposition or collection of the fee, or both.

(4) LIMITATION ON COLLECTION.—A fee may be collected under this section, other than subsection (i), only to the extent that the expenditure of the fee to pay the costs of activities and services for which the fee is imposed is provided for in advance in an appropriations Act or in section 40934 of this title.

(e) ADMINISTRATION OF FEES.—

(1) FEES PAYABLE TO ADMINISTRATOR.—All fees imposed and amounts collected under this section are payable to the Administrator.

(2) FEES COLLECTED BY AIR CARRIER.—A fee imposed under subsection (a)(1) shall be collected by the air carrier or foreign air carrier that sells a ticket for transportation described in subsection (a).

(3) DUE DATE FOR REMITTANCE.—A fee collected under this section shall be remitted on the last day of each calendar month by the carrier collecting the fee. The amount to be remitted shall be for the calendar month preceding the calendar month in which the remittance is made.

(4) INFORMATION.—The Administrator may require the provision of information the Administrator decides is necessary to verify that fees have been collected and remitted at the proper times and in the proper amounts.

(5) FEE NOT SUBJECT TO TAX.—For purposes of section 4261 of the Internal Revenue Code of 1986 (26 U.S.C. 4261), a fee imposed under this section is not considered to be part of the amount paid for taxable transportation.

(6) COST OF COLLECTING FEE.—No portion of the fee collected under this section may be retained by the air carrier or foreign air carrier for the costs of collecting, handling, or remitting the fee, except for interest accruing to the carrier after collection and before remittance.

(f) RECEIPTS CREDITED AS OFFSETTING COLLECTIONS.—Notwithstanding section 3302 of title 31, a fee collected under this section—

(1) shall be credited as offsetting collections to the account that finances the activities and services for which the fee is imposed;

(2) shall be available for expenditure only to pay the costs of activities and services for which the fee is imposed; and

(3) shall remain available until expended.

(g) REFUNDS.—The Administrator may refund a fee paid by mistake or an amount paid in excess of that required.

(h) EXEMPTIONS.—The Administrator may exempt from the passenger fee imposed under subsection (a) a passenger enplaning at an airport in the

United States that does not receive screening services under section 40911 of this title for that segment of the trip for which the passenger does not receive screening.

(i) DEPOSIT OF RECEIPTS.—

(1) IN GENERAL.—Out of fees received in a fiscal year under subsection (a), after amounts are made available in the fiscal year under section 40934(h) of this title, the next funds derived from the fees in the fiscal year, in the amount specified for the fiscal year in paragraph (4), shall be credited as offsetting receipts and deposited in the general fund of the Treasury.

(2) FEE LEVELS.—The Secretary shall impose the fee authorized by subsection (a) so as to collect in a fiscal year at least the amount specified in paragraph (4) for the fiscal year for making deposits under paragraph (1).

(3) RELATIONSHIP TO OTHER PROVISIONS.—Subsections (b) and (f) do not apply to amounts to be used for making deposits under this subsection.

(4) FISCAL YEAR AMOUNTS.—For purposes of paragraphs (1) and (2), the fiscal year amounts are as follows:

(A) $1,520,000,000 for fiscal year 2023.

(B) $1,560,000,000 for fiscal year 2024.

(C) $1,600,000,000 for fiscal year 2025.

(D) $1,640,000,000 for fiscal year 2026.

(E) $1,680,000,000 for fiscal year 2027.

§ 40961. Immunity for reporting suspicious activities

(a) IN GENERAL.—An air carrier or foreign air carrier or an employee of an air carrier or foreign air carrier who makes a voluntary disclosure of a suspicious transaction relevant to a possible violation of law or regulation, relating to air piracy, a threat to aircraft or passenger safety, or terrorism, as defined in section 3077 of title 18, to an employee or agent of the Department, the Department of Transportation, the Department of Justice, a Federal, State, or local law enforcement officer, or an airport or airline security officer shall not be civilly liable to any person under a law or regulation of the United States, or a constitution, law, or regulation of a State or political subdivision of a State, for the disclosure.

(b) APPLICATION.—Subsection (a) does not apply to—

(1) a disclosure made with actual knowledge that the disclosure was false, inaccurate, or misleading; or

(2) a disclosure made with reckless disregard as to the truth or falsity of that disclosure.

§ 40962. Performance goals and objectives

(a) SHORT-TERM TRANSITION.—

(1) IN GENERAL.—The Administrator, in consultation with other relevant Federal agencies and Congress, may—

(A) establish acceptable levels of performance for aviation security, including screening operations and access control; and

(B) provide Congress with an action plan, containing measurable goals and milestones, that outlines how those levels of performance will be achieved.

(2) BASICS OF ACTION PLAN.—The action plan shall clarify the responsibilities of the Transportation Security Administration, the Federal Aviation Administration, and any other agency or organization that may have a role in ensuring the safety and security of the civil air transportation system.

(b) LONG-TERM RESULTS-BASED MANAGEMENT.—

(1) PERFORMANCE PLAN.—

(A) IN GENERAL.—Each year, consistent with the requirements of the Government Performance and Results Act of 1993 (in this section referred to as ''GPRA'') (Public Law 103–62, 107 Stat. 285), the Secretary and the Administrator shall agree on a performance plan for the succeeding 5 years that establishes measurable goals and objectives for aviation security. The plan shall identify action steps necessary to achieve the goals.

(B) CLARIFICATION OF RESPONSIBILITIES.—In addition to meeting the requirements of GPRA, the performance plan should clarify the responsibilities of the Secretary, the Administrator, and any other agency or organization that may have a role in ensuring the safety and security of the civil air transportation system.

(C) ANNUAL PERFORMANCE REPORT.—Each year, consistent with the requirements of GPRA, the Administrator shall prepare and submit to Congress an annual report, including an evaluation of the extent to which goals and objectives were met. The report shall include the results achieved during the year relative to the goals established in the performance plan.

§ 40963. Aviation Security Advisory Committee

(a) DEFINITIONS.—In this section:

(1) ADVISORY COMMITTEE.—The term ''Advisory Committee'' means the aviation security advisory committee established under subsection (b).

(2) PERIMETER SECURITY.—The term ''perimeter security''—

(A) means procedures or systems to monitor, secure, and prevent unauthorized access to an airport, including its airfield and terminal; and

(B) includes the fence area surrounding an airport, access gates, and access controls.

(b) ESTABLISHMENT.—The Administrator shall establish in the Transportation Security Administration an aviation security advisory committee.

(c) DUTIES.—

(1) IN GENERAL.—The Administrator shall consult the Advisory Committee, as appropriate, on aviation security matters, including on the development, refinement, and implementation of policies, programs, rulemaking, and security directives pertaining to aviation security, while adhering to sensitive security guidelines.

(2) RECOMMENDATIONS.—

(A) IN GENERAL.—At the request of the Administrator, the Advisory Committee shall develop recommendations for improvements to aviation security.

(B) RECOMMENDATIONS OF SUBCOMMITTEES.—Recommendations agreed on by the subcommittees established under this section shall be approved by the Advisory Committee before transmission to the Administrator.

(3) PERIODIC REPORTS.—The Advisory Committee shall periodically submit to the Administrator—

(A) reports on matters identified by the Administrator; and

(B) reports on other matters identified by a majority of the members of the Advisory Committee.

(4) ANNUAL REPORT.—The Advisory Committee shall submit to the Administrator an annual report providing information on the activities, findings, and recommendations of the Advisory Committee, including its subcommittees, for the preceding year. Not later than 6 months after the date that the Administrator receives the annual report, the Administrator shall publish a public version describing the Advisory Committee's activities and such related matters as would be informative to the public consistent with the policy of section 552(b) of title 5.

(5) FEEDBACK.—Not later than 90 days after receiving recommendations transmitted by the Advisory Committee under paragraph (4), the Administrator shall respond in writing to the Advisory Committee with feedback on each of the recommendations, an action plan to implement any of the recommendations with which the Admin-

istrator concurs, and a justification for why any of the recommendations have been rejected.

(6) CONGRESSIONAL NOTIFICATION.—Not later than 30 days after providing written feedback to the Advisory Committee under paragraph (5), the Administrator shall notify the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives on the feedback, and provide a briefing on request.

(7) REPORT TO CONGRESS.—Prior to briefing the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives under paragraph (6), the Administrator shall submit to the committees a report containing information relating to the recommendations transmitted by the Advisory Committee in accordance with paragraph (4).

(d) MEMBERSHIP.—

(1) IN GENERAL.—

(A) APPOINTMENT.—The Administrator shall appoint the members of the Advisory Committee.

(B) COMPOSITION.—The Advisory Committee consists of individuals representing not more than 34 member organizations. Each organization shall be represented by 1 individual (or the individual's designee).

(C) REPRESENTATION.—The membership of the Advisory Committee shall include representatives of—

(i) air carriers;

(ii) all-cargo air transportation;

(iii) indirect air carriers;

(iv) labor organizations representing air carrier employees;

(v) labor organizations representing transportation security officers;

(vi) aircraft manufacturers;

(vii) airport operators;

(viii) airport construction and maintenance contractors;

(ix) labor organizations representing employees of airport construction and maintenance contractors;

(x) general aviation;

(xi) privacy organizations;

(xii) the travel industry;

(xiii) airport-based businesses (including minority-owned small businesses);

(xiv) businesses that conduct security screening operations at airports;

(xv) aeronautical repair stations;

(xvi) passenger advocacy groups;

(xvii) the aviation security technology industry (including screening technology and biometrics);

(xviii) victims of terrorist acts against aviation; and

(xix) law enforcement and security experts.

(2) TERM OF OFFICE.—

(A) IN GENERAL.—The term of each member of the Advisory Committee shall be 2 years.

(B) REAPPOINTMENT.—A member of the Advisory Committee may be reappointed.

(C) REMOVAL.—The Administrator may review the participation of a member of the Advisory Committee and remove the member for cause at any time.

(3) PROHIBITION ON COMPENSATION.—The members of the Advisory Committee shall not receive pay, allowances, or benefits from the Government by reason of their service on the Advisory Committee.

(4) MEETINGS.—

(A) IN GENERAL.—The Administrator shall require the Advisory Committee to meet at least semiannually and may convene additional meetings as necessary.

(B) PUBLIC MEETINGS.—At least 1 of the meetings described in subparagraph (A) shall be open to the public.

(C) ATTENDANCE.—The Advisory Committee shall maintain a record of the individuals present at each meeting.

(5) MEMBER ACCESS TO SENSITIVE SECURITY INFORMATION.—Not later than 60 days after the date of a member's appointment, the Administrator shall determine if there is cause for the member to be restricted from possessing sensitive security information. Without that cause, and on the member's voluntarily signing a non-disclosure agreement, the member may be granted access to sensitive security information that is relevant to the member's advisory duties. The member shall protect the sensitive security information in accordance with part 1520 of title 49, Code of Federal Regulations.

(6) CHAIR.—A stakeholder representative on the Advisory Committee who is elected by the appointed membership of the Advisory Committee shall chair the Advisory Committee.

(e) SUBCOMMITTEES.—

(1) MEMBERSHIP.—The Advisory Committee chairperson, in coordination with the Administrator, may establish in the Advisory Committee any subcommittee that the Administrator and Advisory Committee determine to be necessary. The Administrator and the Advisory Committee shall create subcommittees to address aviation security issues, including the following:

(A) The implementation of the air cargo security programs established by the Transportation Security Administration to screen air cargo on passenger aircraft and all-cargo aircraft in accordance with established cargo screening mandates.

(B) General aviation facilities, general aviation aircraft, and helicopter operations at general aviation and commercial service airports.

(C) Recommendations on airport perimeter security, exit lane security, and technology at commercial service airports, and access control issues.

(D) Security technology standards and requirements, including their harmonization internationally, technology to screen passengers, passenger baggage, carry-on baggage, and cargo, and biometric technology.

(2) CONSIDERATION OF RISK-BASED SECURITY.—All subcommittees established by the Advisory Committee chairperson in coordination with the Administrator shall consider risk-based security approaches in the performance of their functions that weigh the optimum balance of costs and benefits in transportation security, including for passenger screening, baggage screening, air cargo security policies, and general aviation security matters.

(3) MEETINGS AND REPORTING.—Each subcommittee shall meet at least quarterly and submit to the Advisory Committee for inclusion in the annual report required under subsection (c)(4) information, including recommendations, regarding issues in the subcommittee.

(4) CO-CHAIRS.—Each subcommittee shall be co-chaired by a Government official and an industry official.

(5) SUBJECT MATTER EXPERTS.—Each subcommittee shall include subject matter experts with relevant expertise who are appointed by its co-chairs.

(f) NONAPPLICABILITY OF CHAPTER 10 OF TITLE 5.—Chapter 10 of title 5 shall not apply to the Advisory Committee and its subcommittees.

SEC. 4. CONFORMING AMENDMENTS.

(a) TITLE 6, UNITED STATES CODE.—Chapter 409 of title 6, United States Code, as enacted by section 3, is amended as follows:

(1) By inserting after section 40963 the following:

''§ 40964. General authority

''The Administrator may take action the Administrator considers necessary to carry out this chapter, including conducting investigations, prescribing regulations, standards, and procedures, and issuing orders.

''§ 40965. Withholding information

''(a) OBJECTIONS TO DISCLOSURE.—A person may object to the public disclosure of information in a record filed under this chapter. An objection must be in writing and must state the reasons for the objection.

''(b) WITHHOLDING INFORMATION FROM CONGRESS.—This section does not authorize information to be withheld from a committee of Congress authorized to have the information.

''Subchapter IV—Alcohol and Controlled Substances Testing

''§ 40981. Definition of controlled substance

''In this subchapter, the term ''controlled substance'' means a substance under section 102 of the Controlled Substances Act (21 U.S.C. 802) specified by the Administrator.

''§ 40982. Application

''This subchapter applies to—

''(1) programs relating to testing of airport security screening personnel; and

''(2) employees of the Transportation Security Administration whose duties include responsibility for security-sensitive functions.

''§ 40983. Alcohol and controlled substances testing programs

''(a) EMPLOYEES OF AIR CARRIERS AND FOREIGN AIR CARRIERS.—

''(1) IN GENERAL.—In the interest of aviation security, the Administrator shall prescribe regulations—

''(A) that establish a program requiring employers of airport security screening personnel to conduct preemployment, reasonable suspicion, random, and post-accident testing of their personnel responsible for security-sensitive functions (as decided by the Administrator) for the use of a controlled substance in violation of law or a United States Government regulation; and

''(B) that—

''(i) establish a program requiring employers of airport security screening personnel to conduct reasonable suspicion, random, and post-accident testing of their personnel responsible for security-sensitive functions (as decided by the Ad-

ministrator) for the use of alcohol in violation of law or a United States Government regulation; and

''(ii) permit the employers to conduct preemployment testing of airport security screening personnel responsible for safety-sensitive functions (as decided by the Administrator) for the use of alcohol.

''(2) RECURRING TESTING.—When the Administrator considers it appropriate in the interest of security, the Administrator may prescribe regulations for conducting periodic recurring testing of airport security screening personnel responsible for security-sensitive functions for the use of alcohol or a controlled substance in violation of law or a United States Government regulation.

''(b) EMPLOYEES OF TRANSPORTATION SECURITY ADMINISTRATION.—

''(1) IN GENERAL.—The Administrator—

''(A) shall establish for employees of the Transportation Security Administration whose duties include responsibility for security-sensitive functions a program—

''(i) of preemployment, reasonable suspicion, random, and post-accident testing for the use of a controlled substance in violation of law or a United States Government regulation; and

''(ii) of reasonable suspicion, random, and post-accident testing for the use of alcohol in violation of law or a United States Government regulation; and

''(B) may establish a program of preemployment testing for the use of alcohol for employees of the Transportation Security Administration whose duties include responsibility for security-sensitive functions.

''(2) RECURRING TESTING.—When the Administrator considers it appropriate in the interest of security, the Administrator may prescribe regulations for conducting periodic recurring testing of employees of the Transportation Security Administration responsible for security-sensitive functions for the use of alcohol or a controlled substance in violation of law or a United States Government regulation.

''(c) SANCTIONS.—In prescribing regulations under the programs required by this section, the Administrator shall require, as the Administrator considers appropriate, the disqualification or dismissal of an individual under this subchapter when a test conducted and confirmed under this subchapter indicates the individual has used alcohol or a controlled substance in violation of law or a United States Government regulation.

"**§ 40984. Prohibited service**

"(a) USE OF ALCOHOL OR A CONTROLLED SUBSTANCE.—An individual may not use alcohol or a controlled substance after October 28, 1991, in violation of law or a United States Government regulation and serve as an air carrier employee responsible for security-sensitive functions (as decided by the Administrator) or employee of the Transportation Security Administration with responsibility for security-sensitive functions.

"(b) REHABILITATION REQUIRED TO RESUME SERVICE.—Notwithstanding subsection (a), an individual found to have used alcohol or a controlled substance after October 28, 1991, in violation of law or a United States Government regulation may serve as an air carrier employee responsible for security-sensitive functions (as decided by the Administrator), or employee of the Transportation Security Administration with responsibility for security-sensitive functions only if the individual completes a rehabilitation program described in section 40986 of this title.

"(c) PERFORMANCE OF PRIOR DUTIES PROHIBITED.—An individual who served as an air carrier employee responsible for security-sensitive functions (as decided by the Administrator), or employee of the Transportation Security Administration with responsibility for security-sensitive functions and who was found by the Administrator to have used alcohol or a controlled substance after October 28, 1991, in violation of law or a United States Government regulation may not carry out the duties related to air transportation that the individual carried out before the finding of the Administrator if the individual—-

"(1) used the alcohol or controlled substance when on duty;

"(2) began or completed a rehabilitation program described in section 40986 of this title before using the alcohol or controlled substance; or

"(3) refuses to begin or complete a rehabilitation program described in section 40986 of this title after a finding by the Administrator under this section.

"**§ 40985. Testing and laboratory requirements**

"In carrying out section 40983 of this title, the Administrator shall develop requirements that—

"(1) promote, to the maximum extent practicable, individual privacy in the collection of specimens;

"(2) for laboratories and testing procedures for controlled substances, incorporate the Department of Health and Human Services scientific and technical guidelines dated April 11, 1988, and any amendments to those guidelines, including mandatory guidelines establishing—-

"(A) comprehensive standards for every aspect of laboratory controlled substances testing and laboratory procedures to be applied in carrying out this subchapter, including standards requiring the use of the best available technology to ensure the complete reliability and accuracy of controlled substances tests and strict procedures governing the chain of custody of specimens collected for controlled substances testing;

"(B) the minimum list of controlled substances for which individuals may be tested; and

"(C) appropriate standards and procedures for periodic review of laboratories and criteria for certification and revocation of certification of laboratories to perform controlled substances testing in carrying out this subchapter;

"(3) require that a laboratory involved in controlled substances testing under this subchapter have the capability and facility, at the laboratory, of performing screening and confirmation tests;

"(4) provide that all tests indicating the use of alcohol or a controlled substance in violation of law or a United States Government regulation be confirmed by a scientifically recognized method of testing capable of providing quantitative information about alcohol or a controlled substance;

"(5) provide that each specimen be subdivided, secured, and labeled in the presence of the tested individual and that a part of the specimen be retained in a secure manner to prevent the possibility of tampering, so that if the individual's confirmation test results are positive the individual has an opportunity to have the retained part tested by a 2d confirmation test done independently at another certified laboratory if the individual requests the 2d confirmation test not later than 3 days after being advised of the results of the 1st confirmation test;

"(6) ensure appropriate safeguards for testing to detect and quantify alcohol in breath and body fluid samples, including urine and blood, through the development of regulations that may be necessary and in consultation with the Secretary of Health and Human Services;

"(7) provide for the confidentiality of test results and medical information (except information about alcohol or a controlled substance) of employees, except that this paragraph does not prevent the use of test results for the orderly imposition of appropriate sanctions under this subchapter; and

"(8) ensure that employees are selected for tests by nondiscriminatory and impartial methods, so that no employee is harassed by being treated differently from other employees in similar circumstances.

"**§ 40986. Rehabilitation**

"(a) PROGRAM FOR EMPLOYEES OF AIR CARRIERS AND FOREIGN AIR CARRIERS.—The Administrator shall prescribe regulations establishing requirements for rehabilitation programs that at least provide for the identification and opportunity for treatment of employees of air carriers and foreign air carriers referred to in section 40983(a)(1) of this title who need assistance in resolving problems with the use of alcohol or a controlled substance in violation of law or a United States Government regulation. Each air carrier and foreign air carrier is encouraged to make the program available to all its employees in addition to the employees referred to in section 40983(a)(1). The Administrator shall decide on the circumstances under which employees shall be required to participate in a program. This subsection does not prevent an air carrier or foreign air carrier from establishing a program under this subsection in cooperation with another air carrier or foreign air carrier.

"(b) PROGRAM FOR EMPLOYEES OF THE TRANSPORTATION SECURITY ADMINISTRATION.—The Administrator shall establish and maintain a rehabilitation program that at least provides for the identification and opportunity for treatment of employees of the Transportation Security Administration whose duties include responsibility for security-sensitive functions who need assistance in resolving problems with the use of alcohol or a controlled substance.

"**§ 40987. Relationship to other laws, regulations, standards, and orders**

"(a) EFFECT ON STATE AND LOCAL GOVERNMENT LAWS, REGULATIONS, STANDARDS, OR ORDERS.—A State or local government may not prescribe, issue, or continue in effect a law, regulation, standard, or order that is inconsistent with regulations prescribed under this subchapter. However, a regulation prescribed under this subchapter does not preempt a State criminal law that imposes sanctions for reckless conduct leading to loss of life, injury, or damage to property.

"(b) INTERNATIONAL OBLIGATIONS AND FOREIGN LAWS.—

"(1) IN GENERAL.—In prescribing regulations under this subchapter, the Administrator—

"(A) shall establish only requirements applicable to foreign air carriers that are consistent with international obligations of the United States; and

"(B) shall consider applicable laws and regulations of foreign countries.

"(2) REQUEST TO STRENGTHEN AND ENFORCE EXISTING STANDARDS.—The Secretary and the Secretary of State jointly shall request

the governments of foreign countries that are members of the International Civil Aviation Organization to strengthen and enforce existing standards to prohibit crewmembers in international civil aviation from using alcohol or a controlled substance in violation of law or a United States Government regulation.

''(c) OTHER REGULATIONS ALLOWED.—This section does not prevent the Administrator from continuing in effect, amending, or further supplementing a regulation prescribed before October 28, 1991, governing the use of alcohol or a controlled substance by airport security screening employees, air carrier employees responsible for security-sensitive functions (as decided by the Administrator), or employees of the Transportation Security Administration with responsibility for security-sensitive functions.

''Subchapter V—Enforcement and Penalties

''Part A—Enforcement

''§ 41001. 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) a 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 com-

plaint, the Secretary of that department shall inform the Administrator of the action taken on the complaint, including any corrective or disciplinary action taken.

''§ 41002. 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 request of an interested party unless the Administrator decides that secrecy is required because of national defense.

''(d) CONFLICTS OF INTEREST.—The Administrator or an officer or employee of the Transportation Security Administration may not participate in a proceeding referred to in subsection (a) in which the individual has a pecuniary interest.

''§ 41003. Service of notice, process, and actions

''(a) DESIGNATING AGENTS.—

''(1) IN GENERAL.—Each air carrier and foreign air carrier shall designate an agent on whom service of notice and process in a proceeding before, and an action of, the Administrator, may be made.

''(2) FORM OF DESIGNATION; CHANGES.—The designation—

''(A) shall be in writing and filed with the Administrator; and

''(B) may be changed in the same way as originally made.

''(b) SERVICE.—

''(1) METHOD OF SERVICE.—Service may be made—

''(A) by personal service;

''(B) on a designated agent; or

''(C) by certified or registered mail to the person to be served or the designated agent of the person.

''(2) DATE OF SERVICE.—The date of service made by certified or registered mail is the date of mailing.

''(c) SERVING AGENTS.—Service on an agent designated under this section shall be made at the office or usual place of residence of the agent. If an air carrier or foreign air carrier does not have a designated agent, service may be made by posting the notice, process, or action in the office of the Administrator.

"**§ 41004. Evidence**

"(a) IN GENERAL.—In conducting a hearing or investigation under this chapter, the Administrator may—

"(1) subpoena witnesses and records related to a matter involved in the hearing or investigation from any place in the United States to the designated place of the hearing or investigation;

"(2) administer oaths;

"(3) examine witnesses; and

"(4) receive evidence at a place in the United States the Administrator designates.

"(b) COMPLIANCE WITH SUBPOENAS.—If a person disobeys a subpoena, the Administrator or a party to a proceeding before the Administrator may petition a court of the United States to enforce the subpoena. A judicial proceeding to enforce a subpoena under this section may be brought in the jurisdiction in which the proceeding or investigation is conducted. The court may punish a failure to obey an order of the court to comply with the subpoena as a contempt of court.

"(c) DEPOSITIONS.—

"(1) IN GENERAL.—In a proceeding or investigation, the Administrator may order an individual to give testimony by deposition and to produce records. If an individual fails to be deposed or to produce records, the order may be enforced in the same way a subpoena may be enforced under subsection (b).

"(2) TAKING OF DEPOSITION.—A deposition may be taken before an individual designated by the Administrator and having the power to administer oaths.

"(3) NOTICE REQUIREMENTS.—Before taking a deposition, the party or the attorney of the party proposing to take the deposition must give reasonable notice in writing to the opposing party or the attorney of record of that party. The notice shall state the name of the witness and the time and place of the taking of the deposition.

"(4) DEPOSITION PROCESS.—The testimony of an individual deposed under this subsection shall be under oath. The individual taking the deposition shall prepare, or cause to be prepared, a transcript of the testimony taken. The transcript shall be subscribed by the deponent. Each deposition shall be filed promptly with the Administrator.

"(5) DEPOSITIONS ABROAD.—If the laws of a foreign country allow, the testimony of a witness in that country may be taken by deposition—

"(A) by a consular officer or an individual commissioned by the Administrator or agreed on by the parties by written stipulation filed with the Administrator; or

"(B) under letters rogatory issued by a court of competent jurisdiction at the request of the Administrator.

"(d) WITNESS FEES AND MILEAGE AND CERTAIN FOREIGN COUNTRY EXPENSES.—A witness summoned before the Administrator or whose deposition is taken under this section and the individual taking the deposition are each entitled to the same fee and mileage that the witness and individual would have been paid for those services in a court of the United States. Under regulations of the Administrator, the Administrator shall pay the necessary expenses incident to executing, in another country, a commission or letter rogatory issued at the initiative of the Administrator.

"(e) DESIGNATING EMPLOYEES TO CONDUCT HEARINGS.—When designated by the Administrator, an employee appointed under section 3105 of title 5 may conduct a hearing, subpoena witnesses, administer oaths, examine witnesses, and receive evidence at a place in the United States the Administrator designates. On request of a party, the Administrator shall hear or receive argument.

"§ 41005. Regulations and orders

"(a) EFFECTIVENESS OF ORDERS.—Except as provided in this chapter, a regulation prescribed or order issued by the Administrator takes effect within a reasonable time prescribed by the Administrator. The regulation or order remains in effect under its own terms or until superseded. Except as provided in this chapter, the Administrator may amend, modify, or suspend an order in the way, and by giving the notice, that the Administrator decides.

"(b) CONTENTS AND SERVICE OF ORDERS.—An order of the Administrator shall include the findings of fact on which the order is based and shall be served on the parties to the proceeding and the persons affected by the order.

"§ 41006. Enforcement by the Department

"The Administrator may bring a civil action against a person in a district court of the United States to enforce this chapter or a requirement or regulation prescribed or order issued under this chapter. The action may be brought in the judicial district in which the person does business or the violation occurred.

"§ 41007. Enforcement by Attorney General

"(a) IN GENERAL.—On request of the Administrator, the Attorney General may bring a civil action in an appropriate court—

"(1) to enforce this chapter or a requirement or regulation prescribed or order issued under this chapter; and

"(2) to prosecute a person violating this chapter or a requirement or regulation prescribed or order issued under this chapter.

"(b) COSTS AND EXPENSES PAID OUT OF APPROPRIATIONS FOR COURT EXPENSES.—The costs and expenses of a civil action under this chapter shall be paid out of the appropriations for the expenses of the courts of the United States.

"(c) PARTICIPATION OF ADMINISTRATOR.—On request of the Attorney General, the Administrator may participate in a civil action under this chapter.

"§ 41008. Joinder and intervention

"A person interested in or affected by a matter under consideration in a proceeding before the Administrator, a civil action to enforce this chapter, or a requirement or regulation prescribed or order issued under this chapter may be joined as a party or permitted to intervene in the proceeding or civil action.

"§ 41009. Judicial review

"(a) FILING AND VENUE.—A person disclosing a substantial interest in an order issued by the Administrator, in whole or in part under this chapter or section 11507 or 11513 of this title, may apply for review of the order by filing a petition for review in the United States Court of Appeals for the District of Columbia Circuit or in the court of appeals of the United States for the circuit in which the person resides or has its principal place of business. The petition must be filed not later than 60 days after the order is issued. The court may allow the petition to be filed after the 60th day only if there are reasonable grounds for not filing by the 60th day.

"(b) JUDICIAL PROCEDURES.—When a petition is filed under subsection (a), the clerk of the court immediately shall send a copy of the petition to the Administrator. The Administrator shall file with the court a record of any proceeding in which the order was issued, as provided in section 2112 of title 28.

"(c) AUTHORITY OF COURT.—When the petition is sent to the Administrator, the court has exclusive jurisdiction to affirm, amend, modify, or set aside any part of the order and may order the Administrator to conduct further proceedings. After reasonable notice to the Administrator, the court may grant interim relief by staying the order or taking other appropriate action when good cause for its action exists. Findings of fact by the Administrator, if supported by substantial evidence, are conclusive.

"(d) REQUIREMENT FOR PRIOR OBJECTION.—In reviewing an order under this section, the court may consider an objection to an order of the

Administrator only if the objection was made in the proceeding conducted by the Administrator or if there was a reasonable ground for not making the objection in the proceeding.

''(e) SUPREME COURT REVIEW.—A decision by a court under this section may be reviewed only by the Supreme Court under section 1254 of title 28.

''Part B—Penalties

''Subpart 1—Civil Penalties

''§ 41021. General penalties

''(a) DEFINITION OF SMALL BUSINESS CONCERN.—In this section, the term ''small business concern'' has the meaning given the term in section 3 of the Small Business Act (15 U.S.C. 632).

''(b) IN GENERAL.—

''(1) CIVIL PENALTY.—Except as provided in paragraph (2), a person is liable to the United States Government for a civil penalty of not more than $10,000, and not more $25,000 in the case of a person operating an aircraft for the transportation of passengers or property for compensation (except an individual serving as an airman), for violating this chapter.

''(2) PENALTIES APPLICABLE TO INDIVIDUALS AND SMALL BUSINESS CONCERNS.—An individual (except an airman serving as an airman) or small business concern is liable to the United States Government for a civil penalty of not more than $10,000 for violating—

''(A) this chapter (except sections 40912, 40913(d), 40914, and 40917 through 40919); or

''(B) a regulation prescribed or order issued under a provision to which subparagraph (A) applies.

''(3) SEPARATE VIOLATIONS.—A separate violation occurs under this subsection for each day the violation continues or, if applicable, for each flight involving the violation.

''(4) FAILURE TO COLLECT AIRPORT SECURITY BADGES.—Notwithstanding paragraph (1), an employer (other than a governmental entity or airport operator) who employs an employee to whom an airport security badge or other identifier used to obtain access to a secure area of an airport is issued and who does not collect or make reasonable efforts to collect the badge from the employee on the date that the employment of the employee is terminated and does not notify the operator of the airport of the termination within 24 hours of the date of the termination is liable to the Government for a civil penalty not to exceed $10,000.

''(c) ADMINISTRATIVE IMPOSITION OF PENALTIES.—

"(1) IN GENERAL.—The Secretary may impose a civil penalty for a violation of this chapter (except sections 40912, 40913(d), 40917 (a) through (d)(1)(A) and (1)(C) through (f), 40918, and 40919).

"(2) WRITTEN NOTICE.—The Secretary shall give written notice of the finding of a violation and the penalty.

"(3) LIMIT ON REEXAMINATION.—In a civil action to collect a civil penalty imposed by the Secretary under this subsection, the issues of liability and the amount of the penalty may not be reexamined.

"(4) DISTRICT COURT JURISDICTION.—Notwithstanding paragraph (1), the district courts of the United States have exclusive jurisdiction of a civil action involving a penalty the Secretary initiates if—

"(A) the amount in controversy is more than—

"(i) $50,000 if the violation was committed by a person before December 12, 2003;

"(ii) $400,000 if the violation was committed by a person other than an individual or small business concern on or after that date; or

"(iii) $50,000 if the violation was committed by an individual or small business concern on or after that date;

"(B) the action is in rem or another action in rem based on the same violation has been brought;

"(C) the action involves an aircraft subject to a lien that has been seized by the Government; or

"(D) another action has been brought for an injunction based on the same violation.

"(5) MAXIMUM PENALTY.—The maximum civil penalty the Administrator may impose under this subsection is—

"(A) $50,000 if the violation was committed by a person before December 12, 2003;

"(B) $400,000 if the violation was committed by a person other than an individual or small business concern on or after that date; or

"(C) $50,000 if the violation was committed by an individual or small business concern on or after that date.

"(d) COMPROMISE AND SETOFF.—

"(1) COMPROMISE.—The Secretary may compromise the amount of a civil penalty imposed for violating—

"(A) this chapter (except sections 40912, 40913(d), 40914, 40917(a) through (d)(1)(A) and (1)(C) through (f), 40918, and 40919); or

"(B) a regulation prescribed or order issued under a provision to which subparagraph (A) applies.

"(2) SETOFF.—The United States Government may deduct the amount of a civil penalty imposed or compromised under this subsection from amounts it owes the person liable for the penalty.

"(e) JUDICIAL REVIEW.—An order of the Secretary imposing a civil penalty may be reviewed judicially only under section 41009 of this title.

"(f) NONAPPLICATION.—

"(1) IN GENERAL.—This section does not apply to the following when performing official duties:

"(A) A member of the armed forces of the United States.

"(B) A civilian employee of the Department of Defense subject to the Uniform Code of Military Justice.

"(2) REPORT ON ACTION TAKEN.—The appropriate military authority is responsible for taking necessary disciplinary action and submitting to the Administrator a timely report on any action taken.

"**§ 41022. False information**

"(a) CIVIL PENALTY.—A person that, knowing the information to be false, gives, or causes to be given, under circumstances in which the information reasonably may be believed, false information about an alleged attempt being made or to be made to do an act that would violate section 41062(a), 41064, 41065, or 41066 of this title is liable to the United States Government for a civil penalty of not more than $10,000 for each violation.

"(b) COMPROMISE AND SETOFF.—

"(1) COMPROMISE.—The Secretary may compromise the amount of a civil penalty imposed under subsection (a).

"(2) SETOFF.—The United States Government may deduct the amount of a civil penalty imposed or compromised under this section from amounts it owes the person liable for the penalty.

"**§ 41023. Carrying a weapon**

"(a) CIVIL PENALTY.—An individual who, when on, or attempting to board, an aircraft in, or intended for operation in, air transportation or intrastate air transportation, has on or about the individual or the property of the individual a concealed dangerous weapon that is or would be accessible to the individual in flight is liable to the United States Government for a civil penalty of not more than $10,000 for each violation.

"(b) COMPROMISE AND SETOFF.—

"(1) COMPROMISE.—The Secretary may compromise the amount of a civil penalty imposed under subsection (a).

"(2) SETOFF.—The United States Government may deduct the amount of a civil penalty imposed or compromised under this section from amounts it owes the individual liable for the penalty.

"(c) NONAPPLICATION.—This section does not apply to—

"(1) a law enforcement officer of a State or political subdivision of a State, or an officer or employee of the United States Government, authorized to carry arms in an official capacity; or

"(2) another individual the Secretary by regulation authorizes to carry arms in an official capacity.

"§ 41024. Liens on aircraft

"When an aircraft is involved in a violation of this chapter (except sections 40912, 40913(d), 40914, 40917(a) through (d)(1)(A) and (1)(C) through (f), and 40918) and the violation is by the owner of, or individual commanding, the aircraft, the aircraft is subject to a lien for the civil penalty as provided in section 46304 of title 49.

"§ 41025. Actions to recover civil penalties

"A civil penalty under this subpart may be collected by bringing a civil action against the person subject to the penalty, a civil action in rem against an aircraft subject to a lien for a penalty, or both. The action shall conform as nearly as practicable to a civil action in admiralty, regardless of the place an aircraft in a civil action in rem is seized. However, a party may demand a jury trial of an issue of fact in an action involving a civil penalty under this chapter if the value of the matter in controversy is more than $20. Issues of fact tried by a jury may be reexamined only under common law rules.

"Subpart 2—Criminal Penalties

"§ 41041. Reporting and recordkeeping violations.

"An air carrier or an officer, agent, or employee of an air carrier shall be fined under title 18 for intentionally—

"(1) failing to make a report or keep a record under this chapter;

"(2) falsifying, mutilating, or altering a report or record under this chapter; or

"(3) filing a false report or record under this chapter.

"§ 41042. Unlawful disclosure of information

"(a) CRIMINAL PENALTY.—The Administrator, or an officer or employee of the Transportation Security Administration, shall be fined under title 18, imprisoned for not more than 2 years, or both, if the Administrator, officer, or employee knowingly and willfully discloses information that—

"(1) the Administrator, officer, or employee acquires when inspecting the records of an air carrier; or

"(2) is withheld from public disclosure under section 40963 of this title.

"(b) NONAPPLICATION.—Subsection (a) does not apply if—

"(1) the officer or employee is directed by the Administrator to disclose information that the Administrator had ordered withheld; or

"(2) the Administrator, officer, or employee is directed by a court of competent jurisdiction to disclose the information.

"(c) WITHHOLDING INFORMATION FROM CONGRESS.—This section does not authorize the Administrator to withhold information from a committee of Congress authorized to have the information.

"§ 41043. Refusing to appear or produce records

"A person not obeying a subpoena or requirement of the Administrator to appear and testify or produce records shall be fined under title 18, imprisoned for not more than 1 year, or both.

"§ 41044. Entering aircraft or airport area in violation of security requirements

"(a) PROHIBITION.—A person may not knowingly and willfully enter, in violation of security requirements prescribed under section 40911, 40913(b) or (c), or 40916 of this title, an aircraft or an airport area that serves an air carrier or foreign air carrier.

"(b) CRIMINAL PENALTY.—

"(1) IN GENERAL.—A person violating subsection (a) shall be fined under title 18, imprisoned for not more than 1 year, or both.

"(2) INCREASED PENALTY.—A person violating subsection (a) with intent to evade security procedures or restrictions or with intent to commit, in the aircraft or airport area, a felony under a law of the United States or a State shall be fined under title 18, imprisoned for not more than 10 years, or both.

"(c) NOTICE OF PENALTIES.—

"(1) SIGNS.—Each operator of an airport in the United States that is required to establish an air transportation security program under section 40913(c) of this title shall ensure that signs that meet requirements the Secretary may prescribe for providing notice of the penalties imposed under subsection (b) and section 41021(b)(2)(A) of this title are displayed near all screening locations, all locations where passengers exit the sterile area, and other locations at the airport that the Secretary determines appropriate.

"(2) EFFECT OF SIGNS ON PENALTIES.—An individual is subject to a penalty imposed under subsection (b) or section 41021(b)(2)(A) of this title without regard to whether signs are displayed at an airport as required by paragraph (1).

"**§ 41045. General criminal penalty when specific penalty not provided**

"When another criminal penalty is not provided under this chapter, a person that knowingly and willfully violates section 40912, 40913(d), 40914, 40917, 40918, or 40919 of this title, or a regulation prescribed or order issued by the Administrator under section 40912, 40913(d), 40914, 40917, 40918, or 40919 of this title, shall be fined under title 18. A separate violation occurs for each day the violation continues.

"Subchapter VI—Special Aircraft Jurisdiction of the United States

"**§ 41061. Definitions**

"In this subchapter:

"(1) AIRCRAFT IN FLIGHT.—The term 'aircraft in flight' means an aircraft from the moment all external doors are closed following boarding—

"(A) through the moment when one external door is opened to allow passengers to leave the aircraft; or

"(B) until, if a forced landing, competent authorities take over responsibility for the aircraft and individuals and property on the aircraft.

"(2) COMMIT AN OFFENSE.—The term 'commit an offense' means, in the case of an individual and for the purposes of the Convention for the Suppression of Unlawful Seizure of Aircraft, when the individual, when on an aircraft in flight—

"(A) by any form of intimidation, unlawfully seizes, exercises control of, or attempts to seize or exercise control of, the aircraft; or

"(B) is an accomplice of an individual referred to in subparagraph (A).

"(3) SPECIAL AIRCRAFT JURISDICTION OF THE UNITED STATES.—The term 'special aircraft jurisdiction of the United States' includes any of the following aircraft in flight:

"(A) A civil aircraft of the United States.

"(B) An aircraft of the armed forces of the United States.

"(C) Another aircraft in the United States.

"(D) Another aircraft outside the United States—

"(i) that has its next scheduled destination or last place of departure in the United States, if the aircraft next lands in the United States;

"(ii) on which an individual commits an offense (as specified in the Convention for the Suppression of Unlawful Sei-

zure of Aircraft) if the aircraft lands in the United States with the individual still on the aircraft; or

''(iii) against which an individual commits an offense (as specified in subsection (d) or (e) of article I, section I of the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation) if the aircraft lands in the United States with the individual still on the aircraft.

''(E) Any other aircraft leased without crew to a lessee whose principal place of business is in the United States or, if the lessee does not have a principal place of business, whose permanent residence is in the United States.

''**§ 41062. Aircraft piracy**

''(a) AIRCRAFT PIRACY IN SPECIAL AIRCRAFT JURISDICTION.—

''(1) DEFINITION OF AIRCRAFT PIRACY.—In this subsection, the term 'aircraft piracy' means seizing or exercising control of an aircraft in the special aircraft jurisdiction of the United States by force, violence, threat of force or violence, or any form of intimidation, and with wrongful intent.

''(2) WHEN ATTEMPT TO COMMIT AIRCRAFT PIRACY DEEMED TO BE IN SPECIAL AIRCRAFT JURISDICTION.—An attempt to commit aircraft piracy is deemed to be in the special aircraft jurisdiction of the United States, although the aircraft is not in flight at the time of the attempt, if the aircraft would have been in the special aircraft jurisdiction of the United States had the aircraft piracy been completed.

''(3) CRIMINAL PENALTY.—An individual committing or attempting or conspiring to commit aircraft piracy—

''(A) shall be imprisoned for at least 20 years; or

''(B) notwithstanding section 3559(b) of title 18, if the death of another individual results from the commission or attempt, shall be put to death or imprisoned for life.

''(b) AIRCRAFT PIRACY OUTSIDE SPECIAL AIRCRAFT JURISDICTION.—

''(1) DEFINITION OF NATIONAL OF THE UNITED STATES.—In this subsection, the term 'national of the United States' has the meaning given the term in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)).

''(2) CRIMINAL PENALTY.—An individual committing or conspiring to commit an offense (as specified in the Convention for the Suppression of Unlawful Seizure of Aircraft) on an aircraft in flight outside the special aircraft jurisdiction of the United States—

''(A) shall be imprisoned for at least 20 years; or

"(B) notwithstanding section 3559(b) of title 18, if the death of another individual results from the commission or attempt, shall be put to death or imprisoned for life.

"(3) JURISDICTION.—There is jurisdiction over the offense in paragraph (2) if—

"(A) a national of the United States was aboard the aircraft;

"(B) an offender is a national of the United States; or

"(C) an offender is afterwards found in the United States.

"§ 41063. Interference with security screening personnel

"An individual in an area in a commercial service airport in the United States who, by assaulting a Federal, airport, or air carrier employee who has security duties in the airport, interferes with the performance of the duties of the employee or lessens the ability of the employee to perform those duties shall be fined under title 18, imprisoned for not more than 10 years, or both. If the individual uses a dangerous weapon in committing the assault or interference, the individual may be imprisoned for any term of years or for life.

"§ 41064. Interference with flight crew members and attendants

"An individual on an aircraft in the special aircraft jurisdiction of the United States who, by assaulting or intimidating a flight crew member or flight attendant of the aircraft, interferes with the performance of the duties of the member or attendant or lessens the ability of the member or attendant to perform those duties, or attempts or conspires to do such an act, shall be fined under title 18, imprisoned for not more than 20 years, or both. If a dangerous weapon is used in assaulting or intimidating the member or attendant, the individual shall be imprisoned for any term of years or for life.

"§ 41065. Carrying a weapon or explosive on an aircraft

"(a) DEFINITION OF LOADED FIREARM.—In this section, the term 'loaded firearm' means a starter gun or a weapon designed or converted to expel a projectile through an explosive, that has a cartridge, a detonator, or powder in the chamber, magazine, cylinder, or clip.

"(b) GENERAL CRIMINAL PENALTY.—An individual shall be fined under title 18, imprisoned for not more than 10 years, or both, if the individual—

"(1) when on, or attempting to get on, an aircraft in, or intended for operation in, air transportation or intrastate air transportation, has on or about the individual or the property of the individual a concealed dangerous weapon that is or would be accessible to the individual in flight;

"(2) has placed, attempted to place, or attempted to have placed a loaded firearm on that aircraft in property not accessible to passengers in flight; or

"(3) has on or about the individual, or has placed, attempted to place, or attempted to have placed on that aircraft, an explosive or incendiary device.

"(c) CRIMINAL PENALTY INVOLVING DISREGARD FOR HUMAN LIFE.—An individual who willfully and without regard for the safety of human life, or with reckless disregard for the safety of human life, violates subsection (b) shall be fined under title 18, imprisoned for not more than 20 years, or both, and, if death results to any person, shall be imprisoned for any term of years or for life.

"(d) NONAPPLICATION.—Subsection (b)(1) does not apply to—

"(1) a law enforcement officer of a State or political subdivision of a State, or an officer or employee of the United States Government, authorized to carry arms in an official capacity;

"(2) another individual the Administrator of the Federal Aviation Administration or the Administrator of the Transportation Security Administration by regulation authorizes to carry a dangerous weapon in air transportation or intrastate air transportation; or

"(3) an individual transporting a weapon (except a loaded firearm) in baggage not accessible to a passenger in flight if the air carrier was informed of the presence of the weapon.

"(e) CONSPIRACY.—If 2 or more individuals conspire to violate subsection (b) or (c), and any of the individuals does any act to effect the object of the conspiracy, each of the parties to the conspiracy shall be punished as provided in subsection (b) or (c).

"**§ 41066. Application of certain criminal laws to acts on an aircraft**

"An individual on an aircraft in the special aircraft jurisdiction of the United States who commits an act that—

"(1) if committed in the special maritime and territorial jurisdiction of the United States (as defined in section 7 of title 18) would violate section 113, 114, 661, 662, 1111, 1112, 1113, or 2111 or chapter 109A of title 18, shall be fined under title 18, imprisoned under that section or chapter, or both; or

"(2) if committed in the District of Columbia would violate section 9 of the Act of July 29, 1892 (D.C. Code 22-1312), shall be fined under title 18, imprisoned under section 9 of the Act, or both.

"**§ 41067. False information and threats**

"An individual shall be fined under title 18, imprisoned for not more than 5 years, or both, if the individual—

"(1) knowing the information to be false, willfully and maliciously or with reckless disregard for the safety of human life, gives, or causes to be given, under circumstances in which the information reasonably may be believed, false information about an alleged attempt being made or to be made to do an act that would violate section 41062(a), 41064, 41065, or 41066 of this title; or

"(2) threatens to violate section 41062(a), 41064, 41065, or 41066 of this title, or causes a threat to violate any of those sections to be made, and has the apparent determination and will to carry out the threat.".

(2) In the table of contents for chapter 409, by inserting after the item relating to 40963 the following:

"41066. Application of certain criminal laws to acts on an aircraft.
"41067. False information and threats.".

(b) TITLE 49, UNITED STATES CODE.—Title 49, United States Code, is amended as follows:

(1) Chapter 51 is amended—

(A) by inserting after section 5110 the following:

"**§ 5111. Hazardous materials highway route plans**

"(a) ROUTE PLAN GUIDANCE.—The Secretary of Transportation, in consultation with the Secretary of Homeland Security, shall—

"(1) document existing and proposed routes for the transportation of radioactive and nonradioactive hazardous materials by motor carrier, and develop a framework for using a geographic information system-based approach to characterize routes in the national hazardous materials route registry;

"(2) assess and characterize existing and proposed routes for the transportation of radioactive and nonradioactive hazardous materials by motor carrier for the purpose of identifying measurable criteria for selecting routes based on safety and security concerns;

"(3) analyze current route-related hazardous materials regulations in the United States, Canada, and Mexico to identify cross-border differences and conflicting regulations;

"(4) document the safety and security concerns of the public, motor carriers, and State, local, territorial, and tribal governments about the highway routing of hazardous materials;

"(5) prepare guidance materials for State officials to assist them in identifying and reducing both safety concerns and security risks when designating highway routes for hazardous materials consistent with the 13 safety-based nonradioactive materials routing criteria and radioactive materials routing criteria in subparts C and D of part 397 of title 49, Code of Federal Regulations;

"(6) develop a tool that will enable State officials to examine potential routes for the highway transportation of hazardous materials, assess specific security risks associated with each route, and explore alternative mitigation measures; and

"(7) transmit to the appropriate congressional committees (as defined in section 10101 of title 6) a report on the actions taken to fulfill paragraphs (1) through (6) and any recommended changes to the routing requirements for the highway transportation of hazardous materials in part 397 of title 49, Code of Federal Regulations.

"(b) ROUTE PLANS.—

''(1) ASSESSMENT.—The Secretary of Transportation shall complete an assessment of the safety and national security benefits achieved under existing requirements for route plans, in written or electronic format, for explosives and radioactive materials. The assessment shall, at a minimum—

''(A) compare the percentage of Department of Transportation recordable incidents and the severity of the incidents for shipments of explosives and radioactive materials for which route plans are required with the percentage of recordable incidents and the severity of the incidents for shipments of explosives and radioactive materials not subject to route plans; and

''(B) quantify the security and safety benefits, feasibility, and costs of requiring each motor carrier that is required to have a hazardous materials safety permit under part 385 of title 49, Code of Federal Regulations, to maintain, follow, and carry a route plan that meets the requirements of section 397.101 of that title when transporting the type and quantity of hazardous materials described in section 385.403 of that title, taking into account the various segments of the motor carrier industry, including tank truck, truckload, and less-than-truckload carriers.

''(2) REPORT.—The Secretary of Transportation shall submit a report to the appropriate congressional committees containing the findings and conclusions of the assessment.

''(c) REQUIREMENT.—The Secretary shall require a motor carrier that has a hazardous materials safety permit under part 385 of title 49, Code of Federal Regulations, to maintain, follow, and carry a route plan, in written or electronic format, that meets the requirements of section 397.101 of that title when transporting the type and quantity of hazardous materials described in section 385.403 of that title if the Secretary determines, under the assessment required in subsection (b), that such a requirement would enhance security and safety without imposing unreasonable costs or burdens upon motor carriers.'';

(B) by inserting after section 5118 the following:

''§ 5118a. Hazardous materials security inspections and study

''(a) IN GENERAL.—The Secretary of Transportation shall consult with the Secretary of Homeland Security to limit, to the extent practicable, duplicative reviews of the hazardous materials security plans required under part 172, title 49, Code of Federal Regulations.

''(b) TRANSPORTATION COSTS STUDY.—The Secretary of Transportation, in conjunction with the Secretary of Homeland Security, shall study to what

extent the insurance, security, and safety costs borne by railroad carriers, motor carriers, pipeline carriers, air carriers, and maritime carriers associated with the transportation of hazardous materials are reflected in the rates paid by offerors of the commodities as compared to the costs and rates, respectively, for the transportation of nonhazardous materials.''; and

(C) in the table of contents—

(i) by inserting the following after the item relating to section 5110:

''5111. Hazardous materials highway route plans.'';

and

(ii) by inserting the following after the item relating to section 5118:

''5118a. Hazardous materials security inspections and study.''.

(2) Section 40113(a) is amended—

(A) by striking ''or the Administrator of the Transportation Security Administration with respect to security duties and powers designated to be carried out by that Administrator''; and

(B) by striking '', Administrator of the Transportation Security Administration,''.

(3) Chapter 461 is amended—

(A) in sections 46101(a)(1), 46102(a), 46103(a), 46104(a), 46105(a), 46106, 46107(b), 46109, and 46110(a), by striking ''or the Administrator of the Transportation Security Administration with respect to security duties and powers designated to be carried out by the Administrator of the Transportation Security Administration'' and

(B) in sections 46101, 46102, 46103, 46104, 46105, 46107, and 46110, by striking '', Administrator of the Transportation Security Administration,'' each place it appears;

(C) in section 46102—

(i) in subsection (b), by striking '', the Administrator of the Transportation Security Administration,''; and

(ii) in subsection (d), by striking ''the Administrator of the Transportation Security Administration,'';

(D) in section 46104(b), by striking ''the Administrator of the Transportation Security Administration,''.

(4) Chapter 463 is amended—

(A) in section 46301—

(i) in subsection (d)(2), by striking the last two sentences and inserting ''The Administrator of the Federal Aviation Ad-

ministration shall give written notice of the finding of a violation and the penalty.'';

(ii) in subsection (d)(3), by striking ''Secretary of Homeland Security or'';

(iii) in subsection (d)(4), by striking ''Secretary of Homeland Security or'';

(iv) in subsection (d)(8), by striking ''Administrator of the Transportation Security Administration, Administrator of the Federal Aviation Administration,'' and inserting ''Administrator of the Federal Aviation Administration''; and

(v) in subsection (h)(2), by striking ''or the Administrator of the Transportation Security Administration with respect to security duties and powers designated to be carried out by the Administrator of the Transportation Security Administration'';

(B) in section 46311—

(i) in subsection (a), by striking ''the Administrator of the Transportation Security Administration with respect to security duties and powers designated to be carried out by the Administrator of the Transportation Security Administration, or'';

(ii) by striking '', Administrator of the Transportation Security Administration, or'' each place it appears and inserting ''or''; and

(iii) by striking ''Administrator of the Transportation Security Administration, Administrator of the Federal Aviation Administration'' each place it appears and inserting ''Administrator of the Federal Aviation Administration''; and

(C) in section 46313, by striking ''or the Administrator of the Transportation Security Administration with respect to security duties and powers designated to be carried out by the Administrator of the Transportation Security Administration''.

(5) Section 367 of Public Law 108–7 (49 U.S.C. 47110 note) is amended—

(A) in subsection (a), by striking ''Under Secretary of Transportation for Security'' and inserting ''Administrator of the Transportation Security Administration''; and

(B) by striking ''Under Secretary'' each place it appears and inserting ''Administrator''.

(6) The table of contents for subtitle VII of title 49, United States Code, is amended as follows:

(A) After the item for chapter 448, by striking
"**449. Security** ..... **44901**".

(B) After the item for chapter 463, by striking
"**465. Special Aircraft Jurisdiction of the United States** ..... **46501**".

SEC. 5. CONFORMING CROSS REFERENCES.

(a) TITLE 5, UNITED STATES CODE.—Title 5, United States Code, is amended as follows:

(1) Section 9701(g) is amended by striking ''section 842 of the Homeland Security Act of 2002'' and inserting ''section 10362 of title 6''.

(2) Section 10101 is amended—

(A) in paragraph (3), by striking ''section 602 of the Post-Katrina Emergency Management Reform Act of 2006'' and inserting ''section 20101 of title 6''; and

(B) in paragraph (5), by striking ''section 624 of the Post-Katrina Emergency Management Reform Act of 2006'' and inserting ''section 20301 of title 6''.

(3) Section 10103(b) is amended by striking ''section 844 of the Homeland Security Act of 2002'' and inserting ''section 10366 of title 6''.

(b) TITLE 8, UNITED STATES CODE.—Section 7202(g)(2)(H) of the Intelligence Reform and Terrorism Prevention Act of 2004 (8 U.S.C. 1777(g)(2)(H)) is amended by striking ''section 1016(b)'' and inserting ''section 11908(b) of title 6, United States Code''.

(c) TITLE 10, UNITED STATES CODE.—Section 130d of title 10, United States Code, is amended by striking ''section 892 of the Homeland Security Act of 2002 (6 U.S.C. 482)'' and inserting ''section 11907 of title 6''.

(d) TITLE 16, UNITED STATES CODE.—Section 402(b)(1)(H) of the Magnuson-Stevens Fishery Conservation and Management Act (16 U.S.C. 1881a(b)(1)(H)) is amended by striking ''as defined in section 888(a)(2) of the Homeland Security Act of 2002 (6 U.S.C. 468(a)(2))''.

(e) TITLE 19, UNITED STATES CODE.—Title 19, United States Code, is amended as follows:

(1) Section 13031(f)(2) of Public Law 99–272 (19 U.S.C. 58c(f)(2)) is amended by striking ''section 415 of the Homeland Security Act of 2002 (other than functions performed by the Office of International Affairs referred to in section 415(8) of that Act),'' and inserting ''section 11131 of title 6, United States Code (other than functions performed by the Office of International Affairs referred to in section 11131(8) of that title),''.

(2) Section 301(h) of Public Law 99–272 (19 U.S.C. 2075(h)) is amended—

(A) in paragraph (1), by striking ''section 412(b)(2) of the Homeland Security Act of 2002 (6 U.S.C. 212(b)(2))'' and ''section 412(b)(1) of such Act'' and inserting ''section 11132(b)(2) of title 6, United States Code'' and ''section 11132(b)(1) of such title'', respectively; and

(B) in paragraph (2)(A), by striking ''section 412(b) of the Homeland Security Act of 2002 (6 U.S.C. 212(b))'' and inserting ''section 11132(b) of title 6, United States Code,''.

(f) TITLE 26, UNITED STATES CODE.—Section 4261(f) of the Internal Revenue Code of 1986 (26 U.S.C. 4261(f)) is amended by striking ''44509 or 44913(b)'' and inserting ''40923(b) of title 6, United States Code, or section 44509''.

(g) TITLE 31, UNITED STATES CODE.—Section 3516(f)(3)(A) of title 31, United States Code, is amended by striking ''section 874(b)(2) of the Homeland Security Act of 2002'' and inserting ''section 10396(b)(2) of title 6''.

(h) TITLE 33, UNITED STATES CODE.—Section 303(b)(4) of Public Law 105–384 (33 U.S.C. 892a(b)(4)) is amended by striking ''section 641 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 741)'' and inserting ''section 20501 of title 6, United States Code''.

(i) TITLE 38, UNITED STATES CODE.—Section 8117(a)(2)(C) of title 38, United States Code, is amended by striking ''section 502(6) of the Homeland Security Act of 2002'' and inserting ''section 11303(a)(6) of title 6''.

(j) TITLE 42, UNITED STATES CODE.—Title 42, United States Code, is amended as follows:

(1) Section 319F–1(a)(2)(A) of the Act of July 1, 1944 (42 U.S.C. 247d–6a(a)(2)(A)) is amended by striking ''sections 302(2) and 304(a) of the Homeland Security Act of 2002'' and inserting ''sections 10901(2) and 10903(a) of title 6, United States Code''.

(2) Section 319F–2(c) of the Act of July 1, 1944 (42 U.S.C. 247d–6b(c)) is amended—

(A) in paragraph (1)(B)(i)(I), by striking ''sections 302(2) and 304(a) of the Homeland Security Act of 2002'' and inserting ''sections 10901(2) and 10903(a) of title 6, United States Code''; and

(B) in paragraph (2)(D), by striking ''section 202 of the Homeland Security Act of 2002'' and inserting ''section 10502 of title 6, United States Code''.

(3) Section 2801(a) of the Act of July 1, 1944 (42 U.S.C. 300hh(a)) is amended by striking ''section 502(6) of the Homeland Security Act

of 2002'' and inserting ''section 11303(a)(6) of title 6, United States Code''.

(4) Section 2802(a)(1) of the Act of July 1, 1944 (42 U.S.C. 300hh–1(a)(1)) is amended—

(A) by striking ''section 504(a)(19) of the Homeland Security Act of 2002'' and inserting ''section 11303(a)(19) of title 6, United States Code'';

(B) by striking ''section 501(7) of such Act'' and inserting ''section 11301(7) of such title''; and

(C) by striking ''section 504 of such Act'' and inserting ''section 11303 of such title''.

(5) Section 1061(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(d)) is amended—

(A) in paragraph (1)(A), by striking ''subsections (d) and (f) of section 1016'' and inserting ''section 11908(c) and (d) of title 6, United States Code'';

(B) in paragraph (1)(B), by striking ''subsections (d) and (f) of section 1016'' and inserting ''section 11908(c) and (d) of title 6, United States Code''; and

(C) in paragraph (2)(B), by striking ''subsections (d) and (f) of section 1016'' and inserting ''section 11908(c) and (d) of title 6, United States Code,''.

(6) Section 303(b) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5144(b)) is amended—

(A) in paragraph (1)(B), by striking ''section 507 of the Homeland Security Act of 2002'' and inserting ''section 11307 of title 6, United States Code'';

(B) in paragraph (2), by striking ''section 646(a) of the Post-Katrina Emergency Management Reform Act of 2006'' and inserting ''section 20506(a) of title 6, United States Code''; and

(C) in paragraph (4), by striking ''section 652(a) of the Post-Katrina Emergency Management Reform Act of 2006'' and inserting ''section 20512(a) of title 6, United States Code''.

(k) TITLE 46, UNITED STATES CODE.—Section 70105(l) of title 46, United States Code, is amended by striking ''section 2(1) of the SAFE Port Act'' and inserting ''section 30101(1) of title 6''.

(l) TITLE 49, UNITED STATES CODE.—Title 49, United States Code, is amended as follows:

(1) Section 46110(a) is amended by striking ''this part, part B, or subsection (l) or (s) of section 114'' and inserting ''this part or part B''.

(2) Chapter 463 is amended—

(A) in section 46301—

(i) in subsection (a), by striking paragraph (4) and redesignating paragraphs (5) through (7) as paragraphs (4) through (6);

(ii) in subsection (a)(1)(A), by striking ''chapter 449 (except sections 44902, 44903(d), 44904, 44907(a)–(d)(1)(A) and (d)(1)(C)–(f), and 44908),'';

(iii) in subsection (a)(4)(A)(i) as redesignated by clause (i), by striking ''chapter 449 (except sections 44902, 44903(d), 44904, and 44907–44909),'';

(iv) in subsection (c)(1)(A), by striking ''chapter 423, or section 44909'' and inserting ''or chapter 423''; and

(v) in subsection (f)(1)(A)(i), by striking ''chapter 449 (except sections 44902, 44903(d), 44904, 44907(a)–(d)(1)(A) and (d)(1)(C)–(f), 44908, and 44909),'';

(B) in section 46302—

(i) in subsection (a), by striking ''section 46502(a), 46504, 46505, or 46506'' and inserting ''section 46504''; and

(ii) in subsection (b)(1), by striking ''The Secretary of Homeland Security and, for a violation relating to section 46504, the Secretary of Transportation,'' and inserting ''The Secretary of Transportation'';

(C) by striking section 46303;

(D) in section 46306(d)(1), by striking ''Commissioner of Customs'' and inserting ''Commissioner of U. S. Customs and Border Protection'';

(E) by striking section 46314;

(F) in section 46316(b), by striking ''chapter 447 (except section 44718(a)), and chapter 449 (except sections 44902, 44903(d), 44904, and 44907–44909)'' and inserting ''and chapter 447 (except section 44718(a))''; and

(G) in the table of contents, by striking the items relating to sections 46303 and 46314.

(m) TITLE 50, UNITED STATES CODE.—Title 50, United States Code, is amended as follows:

(1) Section 1414(b) of the National Defense Authorization Act for Fiscal Year 1997 (50 U.S.C. 2314(b)) is amended by striking ''section 502(6) of the Homeland Security Act of 2002 (6 U.S.C. 312(6))'' and inserting ''section 11303(a)(6) of title 6, United States Code''.

(2) Section 1415(a)(2) of the National Defense Authorization Act for Fiscal Year 1997 (50 U.S.C. 2315(a)(2)) is amended by striking ''sections 102(c) and 430(c)(1) of the Homeland Security Act of 2002 (6 U.S.C. 112(c), 238(c)(1))'' and inserting ''sections 10322(b)(1) and 10341(h) of title 6, United States Code''.

(3) Section 102A(f)(1)(B)(iii) of the Act of July 26, 1947 (50 U.S.C. 3024(f)(1)(B)(iii)) is amended by striking ''sections 201 and 892 of the Homeland Security Act of 2002 (6 U.S.C. 121, 482)'' and inserting ''sections 10501 and 11907 of title 6, United States Code''.

SEC. 6. TRANSITIONAL AND SAVINGS PROVISIONS.

(a) DEFINITIONS.—In this section:

(1) RESTATED PROVISION.—The term ''restated provision'' means a provision of title 6, United States Code, that is enacted by section 3 or 4.

(2) SOURCE PROVISION.—The term ''source provision'' means a provision of law that is replaced by a restated provision.

(b) CUTOFF DATE.—The restated provisions replace certain provisions of law enacted on or before June 14, 2023. If a law enacted after that date amends or repeals a source provision, that law is deemed to amend or repeal, as the case may be, the corresponding restated provision. If a law enacted after that date is otherwise inconsistent with a restated provision or a provision of this Act, that law supersedes the restated provision or provision of this Act to the extent of the inconsistency.

(c) ORIGINAL DATE OF ENACTMENT UNCHANGED.—A restated provision is deemed to have been enacted on the date of enactment of the corresponding source provision.

(d) REFERENCE TO RESTATED PROVISION.—A reference to a restated provision is deemed to refer to the corresponding source provision.

(e) REFERENCE TO SOURCE PROVISION.—A reference to a source provision, including a reference in a regulation, order, or other law, is deemed to refer to the corresponding restated provision.

(f) REGULATIONS, ORDERS, AND OTHER ADMINISTRATIVE ACTIONS.—A regulation, order, or other administrative action in effect under a source provision continues in effect under the corresponding restated provision.

(g) ACTIONS TAKEN AND OFFENSES COMMITTED.—An action taken or an offense committed under a source provision is deemed to have been taken or committed under the corresponding restated provision.

SEC. 7. REPEALS.

The following provisions of law are repealed, except with respect to the rights and duties that matured, penalties that were incurred, or proceedings that were begun before the date of enactment of this Act:

Schedule of Laws Repealed

Statutes at Large

Act	Section	United States Code Former Classification
Act of March 3, 1927 (ch. 348)	1	19 U.S.C. 2071.
	3(b)	19 U.S.C. 2073(b).
	4	19 U.S.C. 2084.
Act of August 10, 1956 (ch. 1041)	43	6 U.S.C. 765.
Federal Fire Prevention and Control Act of 1974 (Public Law 93–498)	3	15 U.S.C. 2202.
	4	15 U.S.C. 2203.
	5	15 U.S.C. 2204.
	6	15 U.S.C. 2205.
	7	15 U.S.C. 2206.
	8	15 U.S.C. 2207.
	9	15 U.S.C. 2208.
	10	15 U.S.C. 2209.
	11	15 U.S.C. 2210.
	12	15 U.S.C. 2211.
	13	15 U.S.C. 2212.
	14	15 U.S.C. 2213.
	15	15 U.S.C. 2214.
	16	15 U.S.C. 2215.
	17	15 U.S.C. 2216.
	20	15 U.S.C. 2217.
	21	15 U.S.C. 2218.
	22	15 U.S.C. 2219.
	24	15 U.S.C. 2220.
	25	15 U.S.C. 2221.
	28	15 U.S.C. 2224.
	29	15 U.S.C. 2225.
	30	15 U.S.C. 2226.
	31	15 U.S.C. 2227.
	32	15 U.S.C. 2228.
	33	15 U.S.C. 2229.
	34	15 U.S.C. 2229a.
	35	15 U.S.C. 2230.
	36	15 U.S.C. 2231.
	37	15 U.S.C. 2234.
	38	15 U.S.C. 2235.
Customs and Trade Act of 1990 (Public Law 101–382)	113	19 U.S.C. 2082.
Hotel and Motel Fire Safety Act of 1990 (Public Law 101–391)	6	15 U.S.C. 2225a.
Firefighters' Safety Study Act (Public Law 101–446)	2	15 U.S.C. 2223a.
	3	15 U.S.C. 2223b.
	4	15 U.S.C. 2223c.
	5	15 U.S.C. 2223d.
	6	15 U.S.C. 2223e.
United States Fire Administration Authorization Act for Fiscal Years 1998 and 1999 (Public Law 105–108)	7(a), (b)(2)	15 U.S.C. 2218 note.
Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Public Law 106–398)	§ 1 [div. A, title XVII, § 1703]	15 U.S.C. 2232.
Aviation and Transportation Security Act (Public Law 107–71)	109	49 U.S.C. 114 note.
Homeland Security Act of 2002 (Public Law 107–296)	2	6 U.S.C. 101.
	3	6 U.S.C. 102.
	101	6 U.S.C. 111.
	102	6 U.S.C. 112.
	103	6 U.S.C. 113.
	201	6 U.S.C. 121.
	202	6 U.S.C. 122.
	203	6 U.S.C. 124.
	204	6 U.S.C. 124a.
	205	6 U.S.C. 124b.
	206	6 U.S.C. 124c.
	207	6 U.S.C. 124d.
	208	6 U.S.C. 124e.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	209	6 U.S.C. 124f.
	210	6 U.S.C. 124g.
	210A	6 U.S.C. 124h.
	210B	6 U.S.C. 124i.
	210C	6 U.S.C. 124j.
	210D	6 U.S.C. 124k.
	210E	6 U.S.C. 124m.
	210F	6 U.S.C. 124m–1.
	210G	6 U.S.C. 124n.
	221	6 U.S.C. 141.
	222	6 U.S.C. 142.
	301	6 U.S.C. 181.
	302	6 U.S.C. 182.
	303	6 U.S.C. 183.
	304	6 U.S.C. 184.
	305	6 U.S.C. 185.
	306	6 U.S.C. 186.
	307	6 U.S.C. 187.
	308	6 U.S.C. 188.
	309	6 U.S.C. 189.
	310	6 U.S.C. 190.
	311	6 U.S.C. 191.
	312	6 U.S.C. 192.
	313	6 U.S.C. 193.
	314	6 U.S.C. 195.
	315	6 U.S.C. 195a.
	316	6 U.S.C. 195b.
	317	6 U.S.C. 195c.
	318	6 U.S.C. 195d.
	319	6 U.S.C. 195e.
	320	6 U.S.C. 195f.
	321	6 U.S.C. 195g.
	322	6 U.S.C. 195h.
	323	6 U.S.C. 195i.
	402	6 U.S.C. 202.
	403	6 U.S.C. 203.
	404	6 U.S.C. 204.
	404	6 U.S.C. 205.
	411	6 U.S.C. 211.
	412	6 U.S.C. 212.
	413	6 U.S.C. 213.
	414	6 U.S.C. 214.
	415	6 U.S.C. 215.
	417	6 U.S.C. 217.
	418	6 U.S.C. 218.
	421	6 U.S.C. 231.
	422	6 U.S.C. 232.
	423	6 U.S.C. 233.
	424	6 U.S.C. 234.
	427	6 U.S.C. 235.
	428	6 U.S.C. 236.
	429	6 U.S.C. 237.
	430	6 U.S.C. 238.
	431	6 U.S.C. 239.
	432	6 U.S.C. 240.
	433	6 U.S.C. 241.
	434	6 U.S.C. 242.
	435	6 U.S.C. 243.
	436	6 U.S.C. 244.
	441	6 U.S.C. 251.
	442	6 U.S.C. 252.
	443	6 U.S.C. 253.
	444	6 U.S.C. 254.
	445	6 U.S.C. 255.
	451	6 U.S.C. 271.
	452	6 U.S.C. 272.
	453	6 U.S.C. 273.
	454	6 U.S.C. 274.
	456	6 U.S.C. 275.
	459	6 U.S.C. 276.
	460	6 U.S.C. 277.
	461	6 U.S.C. 278.
	471	6 U.S.C. 291.
	472	6 U.S.C. 292.
	473	6 U.S.C. 293.
	475	6 U.S.C. 295.
	476	6 U.S.C. 296.
	477	6 U.S.C. 297.
	478(a)	6 U.S.C. 298(a).
	481	6 U.S.C. 301.
	482	6 U.S.C. 301a.
	483	6 U.S.C. 301b.
	484	6 U.S.C. 301c.
	501	6 U.S.C. 311.
	502	6 U.S.C. 312.
	503	6 U.S.C. 313.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	504	6 U.S.C. 314.
	505	6 U.S.C. 315.
	506	6 U.S.C. 316.
	507	6 U.S.C. 317.
	508	6 U.S.C. 318.
	509	6 U.S.C. 319.
	510	6 U.S.C. 320.
	511	6 U.S.C. 321.
	512	6 U.S.C. 321a.
	513	6 U.S.C. 321b.
	514	6 U.S.C. 321c.
	515	6 U.S.C. 321d.
	517	6 U.S.C. 321f.
	518	6 U.S.C. 321g.
	519	6 U.S.C. 321h.
	521	6 U.S.C. 321j.
	522	6 U.S.C. 321k.
	523	6 U.S.C. 321l.
	524	6 U.S.C. 321m.
	525	6 U.S.C. 321n.
	526	6 U.S.C. 321o.
	527	6 U.S.C. 321p.
	528	6 U.S.C. 321q.
	529	6 U.S.C. 321r.
	701	6 U.S.C. 341.
	702	6 U.S.C. 342.
	703	6 U.S.C. 343.
	704	6 U.S.C. 344.
	705	6 U.S.C. 345.
	706	6 U.S.C. 346.
	707	6 U.S.C. 347.
	708	6 U.S.C. 348.
	709	6 U.S.C. 349.
	710	6 U.S.C. 350.
	711	6 U.S.C. 351.
	712	6 U.S.C. 352.
	713	6 U.S.C. 353.
	801	6 U.S.C. 361.
	821	6 U.S.C. 381.
	822	6 U.S.C. 383.
	831	6 U.S.C. 391.
	832	6 U.S.C. 392.
	833	6 U.S.C. 393.
	834	6 U.S.C. 394.
	835	6 U.S.C. 395.
	836	6 U.S.C. 397.
	841(b)	6 U.S.C. 411(b).
	842	6 U.S.C. 412.
	843	6 U.S.C. 413.
	844	6 U.S.C. 414.
	845	6 U.S.C. 415.
	846	6 U.S.C. 417.
	851	6 U.S.C. 421.
	852	6 U.S.C. 422.
	853	6 U.S.C. 423.
	854	6 U.S.C. 424.
	855	6 U.S.C. 425.
	856	6 U.S.C. 426.
	857	6 U.S.C. 427.
	862	6 U.S.C. 441.
	863	6 U.S.C. 442.
	864	6 U.S.C. 443.
	865	6 U.S.C. 444.
	871	6 U.S.C. 451.
	872	6 U.S.C. 452.
	873	6 U.S.C. 453.
	874	6 U.S.C. 454.
	875	6 U.S.C. 455.
	876	6 U.S.C. 456.
	877	6 U.S.C. 457.
	878	6 U.S.C. 458.
	879	6 U.S.C. 459.
	880	6 U.S.C. 460.
	881	6 U.S.C. 461.
	882	6 U.S.C. 462.
	883	6 U.S.C. 463.
	884	6 U.S.C. 464.
	885(a)	6 U.S.C. 465(a).
	887	6 U.S.C. 467.
	888	6 U.S.C. 468.
	890A	6 U.S.C. 473.
	890B	6 U.S.C. 474.
	890C	6 U.S.C. 475.
	890D	6 U.S.C. 475a.
	892(a) through (c)(1), (c)(3) through (g).	6 U.S.C. 482(a) through (c)(1), (c)(3) through (g).

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	893	6 U.S.C. 483.
	894	6 U.S.C. 484.
	895	6 U.S.C. 484a.
	899A	6 U.S.C. 488.
	899B	6 U.S.C. 488a.
	899C	6 U.S.C. 488b.
	899D	6 U.S.C. 488c.
	899E	6 U.S.C. 488d.
	899F	6 U.S.C. 488e.
	899G	6 U.S.C. 488f.
	899H	6 U.S.C. 488g.
	899I	6 U.S.C. 488h.
	899J	6 U.S.C. 488i.
	901	6 U.S.C. 491.
	902	6 U.S.C. 492.
	903	6 U.S.C. 493.
	904	6 U.S.C. 494.
	905	6 U.S.C. 495.
	906	6 U.S.C. 496.
	1001(c)(1)(A), (2)	6 U.S.C. 511(1)(A), (2).
	1006	6 U.S.C. 512.
	1333	6 U.S.C. 665a.
	1502	6 U.S.C. 542.
	1503	6 U.S.C. 543.
	1511	6 U.S.C. 551.
	1513	6 U.S.C. 553.
	1514	6 U.S.C. 554.
	1515	6 U.S.C. 555.
	1601	6 U.S.C. 561.
	1611	6 U.S.C. 563.
	1612	6 U.S.C. 563a.
	1613	6 U.S.C. 563b.
	1614	6 U.S.C. 563c.
	1615	6 U.S.C. 563d.
	1616	6 U.S.C. 563e.
	1617	6 U.S.C. 563f.
	1621	6 U.S.C. 565.
	1714	6 U.S.C. 103.
	1801	6 U.S.C. 571.
	1802	6 U.S.C. 572.
	1803	6 U.S.C. 573.
	1804	6 U.S.C. 574.
	1805	6 U.S.C. 575.
	1806	6 U.S.C. 576.
	1807	6 U.S.C. 577.
	1808	6 U.S.C. 578.
	1809	6 U.S.C. 579.
	1810	6 U.S.C. 580.
	1900	6 U.S.C. 590.
	1901	6 U.S.C. 591.
	1921	6 U.S.C. 591g.
	1922	6 U.S.C. 591h.
	1923	6 U.S.C. 592.
	1924	6 U.S.C. 593.
	1925	6 U.S.C. 594.
	1926	6 U.S.C. 596.
	1927	6 U.S.C. 596a.
	1928	6 U.S.C. 596b.
	1931	6 U.S.C. 597.
	1932	6 U.S.C. 597a.
	2001	6 U.S.C. 601.
	2002	6 U.S.C. 603.
	2003	6 U.S.C. 604.
	2004	6 U.S.C. 605.
	2005	6 U.S.C. 606.
	2006	6 U.S.C. 607.
	2007	6 U.S.C. 608.
	2008	6 U.S.C. 609.
	2009	6 U.S.C. 609a.
	2021(a), (b)	6 U.S.C. 611(a), (b).
	2022	6 U.S.C. 612.
	2023	6 U.S.C. 613.
	2101	6 U.S.C. 621.
	2102	6 U.S.C. 622.
	2103	6 U.S.C. 623.
	2104	6 U.S.C. 624.
	2105	6 U.S.C. 625.
	2106	6 U.S.C. 626.
	2107	6 U.S.C. 627.
	2108	6 U.S.C. 628.
	2109	6 U.S.C. 629.
	2200	6 U.S.C. 650.
	2201	6 U.S.C. 651.
	2202	6 U.S.C. 652.
	2203	6 U.S.C. 653.
	2204	6 U.S.C. 654.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	2205	6 U.S.C. 655.
	2206	6 U.S.C. 656.
	2207(b), (c)	6 U.S.C. 657(b), (c).
	2207(d)(2)	6 U.S.C. 657(d)(2).
	2208	6 U.S.C. 658.
	2209	6 U.S.C. 659.
	2210	6 U.S.C. 660.
	2211	6 U.S.C. 661.
	2212	6 U.S.C. 662.
	2213	6 U.S.C. 663.
	2214	6 U.S.C. 664.
	2215	6 U.S.C. 665.
	2216	6 U.S.C. 665b.
	2217	6 U.S.C. 665c.
	2218	6 U.S.C. 665d.
	2219	6 U.S.C. 665e.
	2220	6 U.S.C. 665f.
	2220A	6 U.S.C. 665g.
	2220B	6 U.S.C. 665h.
	2220C	6 U.S.C. 665i.
	2220D	6 U.S.C. 665k.
	2220E	6 U.S.C. 665n.
	2222	6 U.S.C. 671.
	2223	6 U.S.C. 672.
	2224	6 U.S.C. 673.
	2225	6 U.S.C. 674.
	2232	6 U.S.C. 677a.
	2233	6 U.S.C. 677b.
	2234	6 U.S.C. 677c.
	2235	6 U.S.C. 677d.
	2236	6 U.S.C. 677e.
	2237	6 U.S.C. 677f.
	2238	6 U.S.C. 677g.
	2240	6 U.S.C. 681.
	2241	6 U.S.C. 681a.
	2242	6 U.S.C. 681b.
	2243	6 U.S.C. 681c.
	2244	6 U.S.C. 681d.
	2245	6 U.S.C. 681e.
	2246	6 U.S.C. 681f.
Department of Homeland Security Appropriations Act, 2004 (Public Law 108–90)	(2d proviso under heading "SALARIES AND EXPENSES" under heading "FEDERAL LAW ENFORCEMENT TRAINING CENTER", 117 Stat. 1150).	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. 464c.
	(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.
	505	6 U.S.C. 453a.
	520	6 U.S.C. 469.
Firefighting Research and Coordination Act (Public Law 108—169)	204(b)	15 U.S.C. 2206 note.
	204(c)	15 U.S.C. 2206 note.
Department of Homeland Security Appropriations Act, 2005 (Public Law 108–334)	515(b)	49 U.S.C. 44945 note.
Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458)	1016	6 U.S.C. 485.
	4016(a)	49 U.S.C. 44917 note.
	4016(c)	49 U.S.C. 44917 note.
	7215	6 U.S.C. 123.
	7303(a) through (g)	6 U.S.C. 194(a) through (g).
	7405	6 U.S.C. 112 note.

Schedule of Laws Repealed—Continued

Statutes at Large

Act	Section	United States Code Former Classification
	8306	6 U.S.C. 112 note.
Department of Homeland Security Appropriations Act, 2006 (Public Law 109–90)	503(e)	6 U.S.C. 103 note.
	514	49 U.S.C. 114 note.
	537	6 U.S.C. 114.
	540	49 U.S.C. 114 note.
	541	6 U.S.C. 486.
USA PATRIOT Improvement and Reauthorization Act of 2005 (Public Law 109–177)	125	15 U.S.C. 2233.
Department of Homeland Security Appropriations 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.
	689i	6 U.S.C. 776.
	689j	6 U.S.C. 777.
	691	6 U.S.C. 791.
	693	6 U.S.C. 793.
	695	6 U.S.C. 794.
	696(a), (b)	6 U.S.C. 795.
	697	6 U.S.C. 796.
	698	6 U.S.C. 797.
	699	6 U.S.C. 811.
Security and Accountability for Every Port Act of 2006 (Public Law 109–347)	2	6 U.S.C. 901.
	114	6 U.S.C. 912.
	115	6 U.S.C. 913.
	121	6 U.S.C. 921.
	123	6 U.S.C. 923.
	125	6 U.S.C. 924.
	126	6 U.S.C. 925.
	128	6 U.S.C. 926.
	201	6 U.S.C. 941.
	202	6 U.S.C. 942.
	203	6 U.S.C. 943.
	204	6 U.S.C. 944.
	205	6 U.S.C. 945.
	211	6 U.S.C. 961.
	212	6 U.S.C. 962.
	213	6 U.S.C. 963.
	214	6 U.S.C. 964.
	215	6 U.S.C. 965.

Schedule of Laws Repealed—Continued
Statutes at Large

Act	Section	United States Code Former Classification
	216	6 U.S.C. 966.
	217	6 U.S.C. 967.
	218	6 U.S.C. 968.
	219	6 U.S.C. 969.
	220	6 U.S.C. 970.
	221	6 U.S.C. 971.
	222	6 U.S.C. 972.
	223	6 U.S.C. 973.
	231	6 U.S.C. 981.
	232	6 U.S.C. 982.
	233(a)	6 U.S.C. 983.
	236	6 U.S.C. 985.
	301(b)	6 U.S.C. 1001.
	301(e)	6 U.S.C. 239 note.
	302(e)	6 U.S.C. 1002.
	303	6 U.S.C. 1003.
	401	6 U.S.C. 115.
	502	6 U.S.C. 592a.
	612	6 U.S.C. 314a.
	702	6 U.S.C. 470.
	707	6 U.S.C. 220.
U.S. Troop Readiness, Veterans' Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007 (Public Law 110–28)	6405	6 U.S.C. 396.
Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53)	502(b)	6 U.S.C. 124a note.
	1104	6 U.S.C. 921a.
	1201	6 U.S.C. 1101.
	1203(b)	49 U.S.C. 114 note.
	1204	6 U.S.C. 1102.
	1205	6 U.S.C. 1103.
	1206	6 U.S.C. 1104.
	1301	6 U.S.C. 1111.
	1303	6 U.S.C. 1112.
	1304	6 U.S.C. 1113.
	1305	6 U.S.C. 1114.
	1306	6 U.S.C. 1115.
	1307	6 U.S.C. 1116.
	1310	6 U.S.C. 1117.
	1402	6 U.S.C. 1131.
	1404	6 U.S.C. 1133.
	1405	6 U.S.C. 1134.
	1406	6 U.S.C. 1135.
	1407	6 U.S.C. 1136.
	1408	6 U.S.C. 1137.
	1409	6 U.S.C. 1138.
	1410	6 U.S.C. 1139.
	1411	6 U.S.C. 1140.
	1412	6 U.S.C. 1141.
	1413	6 U.S.C. 1142.
	1414	6 U.S.C. 1143.
	1415	6 U.S.C. 1144.
	1501	6 U.S.C. 1151.
	1502	6 U.S.C. 1152.
	1503(b)	6 U.S.C. 1153.
	1504	6 U.S.C. 1154.
	1511	6 U.S.C. 1161.
	1512	6 U.S.C. 1162.
	1513	6 U.S.C. 1163.
	1514	6 U.S.C. 1164.
	1515	6 U.S.C. 1165.
	1516	6 U.S.C. 1166.
	1517	6 U.S.C. 1167.
	1518	6 U.S.C. 1168.
	1519	6 U.S.C. 1169.
	1522	6 U.S.C. 1170.
	1524	6 U.S.C. 1171.
	1526(b)	6 U.S.C. 1172.
	1531	6 U.S.C. 1181.
	1532	6 U.S.C. 1182.
	1533	6 U.S.C. 1183.
	1534	6 U.S.C. 1184.
	1535	6 U.S.C. 1185.
	1541	6 U.S.C. 1186.
	1551	6 U.S.C. 1201.
	1552	6 U.S.C. 1202.
	1553	6 U.S.C. 1203.
	1554	6 U.S.C. 1204.
	1555	6 U.S.C. 1205.
	1556(b)	6 U.S.C. 1206.

Schedule of Laws Repealed—Continued

Statutes at Large

Act	Section	United States Code Former Classification
	1557	6 U.S.C. 1207.
	1558	6 U.S.C. 1208.
	2205	6 U.S.C. 194 note.
	2403	6 U.S.C. 121 note.
Border Infrastructure and Technology Modernization Act of 2007 (Public Law 110–161)	602	6 U.S.C. 1401.
	606	6 U.S.C. 1405.
American Recovery and Reinvestment Act of 2009 (Public Law 111–5)	604	6 U.S.C. 453b.
Department of Homeland Security Appropriations Act, 2010 (Public Law 111–83)	554	6 U.S.C. 469a.
Coast Guard Authorization Act of 2010 (Public Law 111–281)	825	6 U.S.C. 945 note.
Anti-Border Corruption Act of 2010 (Public Law 111–376)	3	6 U.S.C. 221.
Consolidated Appropriations Act, 2012 (Public Law 112–74)	div. D, title II, (1st proviso in paragraph under heading "CONSTRUCTION AND FACILITIES MANAGEMENT", 125 Stat. 949).	6 U.S.C. 214 note.
	div. D, title V, § 526	6 U.S.C. 453c.
	div. D, title V, § 538	6 U.S.C. 190 note.
	div. D, title V, § 546	6 U.S.C. 124j note.
	div. D, title V, § 557	6 U.S.C. 222.
Border Tunnel Prevention Act of 2012 (Public Law 112–127)	8	6 U.S.C. 257.
Intelligence Authorization Act for Fiscal Year 2013 (Public Law 112–277)	501	6 U.S.C. 121a.
Department of Homeland Security Appropriations Act, 2013 (Public Law 113–6)	div. D, title III, 2d proviso on p. 357.	6 U.S.C. 462 note.
	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 Appropriations 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. 659 note.
Intelligence Authorization Act for Fiscal Year 2015 (Public Law 113–293)	324	6 U.S.C. 125.

Schedule of Laws Repealed—Continued

Statutes at Large

Act	Section	United States Code Former Classification
Department of Homeland Security Appropriations Act, 2015 (Public Law 114–4)	562	6 U.S.C. 472.
Justice for Victims of Trafficking Act of 2015 (Public Law 114–22)	901	6 U.S.C. 641.
	902	6 U.S.C. 642.
	903	6 U.S.C. 643.
	904	6 U.S.C. 644.
	906	6 U.S.C. 645.
Department of Homeland Security Interoperable Communications Act (Public Law 114–29)	2 through 6	6 U.S.C. 194 note.
Border Jobs for Veterans Act of 2015 (Public Law 114–68)	3 through 6	6 U.S.C. 211 note.
Federal Cybersecurity Enhancement Act of 2015 (Public Law 114–113)	div. N, title I, § 102	6 U.S.C. 1501.
	div. N, title I, § 103	6 U.S.C. 1502.
	div. N, title I, § 104	6 U.S.C. 1503.
	div. N, title I, § 105	6 U.S.C. 1504.
	div. N, title I, § 106	6 U.S.C. 1505.
	div. N, title I, § 107	6 U.S.C. 1506.
	div. N, title I, § 108	6 U.S.C. 1507.
	div. N, title I, § 109	6 U.S.C. 1508.
	div. N, title I, § 110	6 U.S.C. 1509.
	div. N, title I, § 111	6 U.S.C. 1510.
	div. N, title II, § 222	6 U.S.C. 1521.
	div. N, title II, § 223(b)	6 U.S.C. 663 note.
	div. N, title II, § 224	6 U.S.C. 1522.
	div. N, title II, § 225	6 U.S.C. 1523.
	div. N, title II, § 226	6 U.S.C. 1524.
	div. N, title II, § 227	6 U.S.C. 1525.
	div. N, title IV, § 403	6 U.S.C. 1531.
	div. N, title IV, § 404	6 U.S.C. 1532.
	div. N, title IV, § 405	6 U.S.C. 1533.
U.S. Customs and Border Protection Authorization Act (Public Law 114–125)	title VIII, § 802(j)	8 U.S.C. 1185 note.
National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328)	div. A, title X, § 1086	6 U.S.C. 104.
	div. A, title X, § 1092	6 U.S.C. 223.
United States Fire Administration, AFG, and SAFER Program Reauthorization Act of 2017 (Public Law 115—98)	5	15 U.S.C. 2229 note.
	6	15 U.S.C. 2229 note.
Disaster Recovery Reform Act of 2018 (Public Law 115–254)	div. D, § 1208	6 U.S.C. 748a.
	div. D, § 1209	6 U.S.C. 721 note.
Maritime Security Improvement Act of 2018 (Public Law 115–254)	div. J, § 1803	46 U.S.C. 70102 note.
	div. J, § 1805(a)	46 U.S.C. 70112 note.
	div. J, § 1805(c)(2)	46 U.S.C. 70112 note.
TSA Modernization Act (Public Law 115–254)	div. K, § 1910	49 U.S.C. 114 note.
	div. K, § 1911	49 U.S.C. 114 note.
	div. K, § 1912	49 U.S.C. 114 note.
	div. K, § 1919	6 U.S.C. 1118.
	div. K, §§ 1926 through 1929	6 U.S.C. 1116 note.
	div. K, § 1930(a)	6 U.S.C. 1112 note.
	div. K, § 1931	49 U.S.C. 114 note.
	div. K, § 1932	49 U.S.C. 114 note.
	div. K, § 1938	49 U.S.C. 44919 note.
	div. K, § 1959(a) through (c)(4).	49 U.S.C. 44917 note.
	div. K, § 1963(i)	49 U.S.C. 44921 note.

Schedule of Laws Repealed—Continued

Statutes at Large

Act	Section	United States Code Former Classification
	div. K, § 1963(j)	49 U.S.C. 44921 note.
	div. K, § 1964	49 U.S.C. 114 note.
	div. K, § 1965	49 U.S.C. 114 note.
	div. K, § 1967	49 U.S.C. 114 note.
	div. K, § 1968(a)	49 U.S.C. 114 note.
	div. K, § 1971	6 U.S.C. 1116 note.
	div. K, § 1974	6 U.S.C. 1164 note.
	div. K, § 1976	6 U.S.C. 1155.
	div. K, § 1977	6 U.S.C. 1119.
	div. K, § 1979	6 U.S.C. 982 note.
	div. K, § 1982	49 U.S.C. 114 note.
	div. K, § 1984	6 U.S.C. 1156.
	div. K, § 1986	49 U.S.C. 114 note.
	div. K, § 1987	49 U.S.C. 114 note.
	div. K, § 1988(d)	49 U.S.C. 44948 note.
Department of Homeland Security Data Framework Act of 2018 (Public Law 115–331)	2	6 U.S.C. 126.
Countering Weapons of Mass Destruction Act of 2018 (Public Law 115–387)	2(g)	6 U.S.C. 591 note.
Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (Public Law 115–390)	101	6 U.S.C. 663 note.
	102	6 U.S.C. 663 note.
Trafficking Victims Protection Act of 2017 (Public Law 115–393)	403	6 U.S.C. 645a.
National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92)	div. A, title XVII, § 1756	6 U.S.C. 321o–1.
Protecting America's Food and Agriculture Act of 2019 (Public Law 116–122)	3(2), 4	6 U.S.C. 211 note.
DHS Opioid Detection Resilience Act of 2019 (Public Law 116–254)	2, 3	6 U.S.C. 211 note.
DOTGOV Online Trust in Government Act of 2020 (Public Law 116–260)	903, 904(a), (b)(1)(B), (2)(B), 907.	6 U.S.C. 665 notes.
Missing Persons and Unidentified Remains Act of 2019 (Public Law 116–277)	5	6 U.S.C. 224.
William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116283)	div. A, title III, § 363	6 U.S.C. 105.
	div. A, title III, § 364	6 U.S.C. 106.
	div. A, title XVII, § 1716(b)	6 U.S.C. 659 note.
	div. A, title XVII, § 1717(a)(2)	6 U.S.C. 665c note.
	div. A, title XVII, § 1717(a)(3)	not classified.
	div. A, title XVII, § 1717(a)(4)	6 U.S.C. 665c note.
	div. A, title XVII, § 1752	6 U.S.C. 1500.
	div. H, title XC, § 9002	6 U.S.C. 652a.
	div. H, title XCVI, § 9603	6 U.S.C. 322.
Securing America's Ports Act (Public Law 116–299)	§ 2	6 U.S.C. 211 note.
k–12 Cybersecurity Act of 2021 (Public Law 11747)	§ 3	6 U.S.C. 652 note.
National Defense Authorization Act for Fiscal Year 2022 (Public Law 11781)	div. A, title XV, § 1544	6 U.S.C. 663 note.
	div. A, title XV, § 1550	6 U.S.C. 652 note.
	div. F, title LXIV, § 6413	49 U.S.C. 114 note.

Schedule of Laws Repealed—Continued

Statutes at Large

Act	Section	United States Code Former Classification
	div. F, title LXIV, § 6417	49 U.S.C. 44919 note.
	div. F, title LXIV, § 6418	6 U.S.C. 124h–1.
	div. F, title LXIV, § 6419	6 U.S.C. 1137a.
	div. F, title LXIV, § 6423(b)	49 U.S.C. 114 note.
Department of Homeland Security Appropriations Act, 2022 (Public Law 117103)	div. F, title V, § 538	6 U.S.C. 103a.
Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Public Law 117103)	div. Y, § 102	6 U.S.C. 665j note.
	div. Y, § 104	6 U.S.C. 681g.
	div. Y, § 105	6 U.S.C. 652 note.
	div. Y, § 106	6 U.S.C. 665j.
National Cybersecurity Preparedness Consortium Act of 2021 (Public Law 117122)	§ 2	6 U.S.C. 652 note.
Luke and Alex School Safety Act of 2022 (Public Law 117159)	div. A, title III, §§ 13303 through 13305.	6 U.S.C. 665k note.
Protecting Firefighters from Adverse Substances Act (Public Law 117248)	§ 2	6 U.S.C. 323.
Quantum Computing Cybersecurity Preparedness Act (Public Law 117260	§ 3	6 U.S.C. 1526 note.
	§ 4	6 U.S.C. 1526.
James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263)	div. G, title LXXI, § 7103	6 U.S.C. 665l.
	div. G, title LXXI, § 7113	6 U.S.C. 112 note.
	div. G, title LXXI, § 7116(a)	6 U.S.C. 451 note.
	div. G, title LXXI, § 7121	6 U.S.C. 665m.
	div. G, title LXXI, § 7132	49 U.S.C. 44901 note.
	div. G, title LXXI, § 7134	6 U.S.C. 257 note.
	div. G, title LXXI, § 7135(c)	6 U.S.C. 216 note.
	div. G, title LXXI, § 7136	6 U.S.C. 225.
	div. G, title LXXIII, § 7302	6 U.S.C. 821.
	div. G, title LXXIII, § 7303	6 U.S.C. 822.
	div. G, title LXXIII, § 7304	6 U.S.C. 823.
	div. G, title LXXIII, § 7305	6 U.S.C. 824.
	div. G, title LXXIII, § 7309	6 U.S.C. 825.
	div. K, title CXII, § 11264	6 U.S.C. 245.
Countering Human Trafficking Act of 2021 (Public Law 117–322)	§ 5	6 U.S.C. 242b.
	§ 6	6 U.S.C. 242 note.
Abolish Trafficking Reauthorization Act of 2022 (Public Law 117–347)	title IV, § 401	6 U.S.C. 1534.
	title IV, § 406(b)	6 U.S.C. 242a note.

United States Code

Title	Section
49	114
	115
	44901
	44902
	44903
	44904
	44905
	44906
	44907
	44908
	44909
	44910
	44911
	44912

Title	Section
	44913
	44914
	44915
	44916
	44917
	44918
	44919
	44920
	44921
	44922
	44923
	44924
	44925
	44926
	44927
	44928
	44929
	44931
	44932
	44933
	44934
	44935
	44936
	44937
	44938
	44939
	44940
	44941
	44942
	44943
	44944
	44945
	44946
	44947
	44948
	46501
	46502
	46503
	46504
	46505
	46506
	46507