HOMELAND SECURITY ACT OF 2002

[Public Law 107–296; Approved November 25, 2002]

[As Amended Through P.L. 118–41, Enacted March 8, 2024]

[Currency: This publication is a compilation of the text of Public Law 107-296. It was last amended by the public law listed in the As Amended Through note above and below at the bottom of each page of the pdf version and reflects current law through the date of the enactment of the public law listed at https://www.govinfo.gov/app/collection/comps/]

[Note: While this publication does not represent an official version of any Federal statute, substantial efforts have been made to ensure the accuracy of its contents. The official version of Federal law is found in the United States Statutes at Large and in the United States Code. The legal effect to be given to the Statutes at Large and the United States Code is established by statute (1 U.S.C. 112, 204).]

AN ACT To establish the Department of Homeland Security, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) [6 U.S.C. 101 note] SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

[1] Section 104(c)(1) public law 108-7 repealed section 811 of the Homeland Security Act of 2002. Such law did not strike the item relating to such section in the table of contents.

SEC. 2. [6 U.S.C. 101] DEFINITIONS.

In this Act, the following definitions apply:

(1) Each of the terms "American homeland" and "homeland" means the United States.

(2) The term "appropriate congressional committee" means any 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) The term "assets" includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).

(4) The term "critical infrastructure" has the meaning given that term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(5) The term "Department" means the Department of Homeland Security.

(6) 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) The term "EMP" means an electromagnetic pulse caused by a nuclear device or nonnuclear device, including such a pulse caused by an act of terrorism.

(8) The term "executive agency" means an executive agency and a military department, as defined, respectively, in sections 105 and 102 of title 5, United States Code.

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

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

(11) The term "intelligence component of the Department" means any 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(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)), 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 pursuant to section 3 of title 14, United States Code, 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(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

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

(13) 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) The term "major disaster" has the meaning given in section 102(2) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(15) The term "personnel" means officers and employees.

(16) The term "Secretary" means the Secretary of Homeland Security.

(17) The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

(18) The term "terrorism" means any 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 any 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)(A) The term "United States", when used in a geographic sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, any possession of the United States, and any waters within the jurisdiction of the United States.

(B) Nothing in this paragraph or any other provision of this Act shall be construed to modify the definition of "United States" for the purposes of the Immigration and Nationality Act or any other immigration or nationality law.

(20) 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 Disaster/Emergency Management and Business Continuity Programs (ANSI/NFPA 1600).

SEC. 3. [6 U.S.C. 102] CONSTRUCTION; SEVERABILITY.

Any provision of this Act held to be invalid or unenforceable by its terms, or as applied to any person or circumstance, shall be construed so as to give it the maximum effect permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which event such provision shall be deemed severable from this Act and shall not affect the remainder thereof, or the application of such provision to other persons not similarly situated or to other, dissimilar circumstances.

SEC. 4. [6 U.S.C. 101 note] EFFECTIVE DATE.

This Act shall take effect 60 days after the date of enactment.

TITLE I—DEPARTMENT OF HOMELAND SECURITY

SEC. 101. [6 U.S.C. 111] EXECUTIVE DEPARTMENT; MISSION.

(a) ESTABLISHMENT.—There is established a Department of Homeland Security, as an executive department of the United States within the meaning of title 5, United States Code.

(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 within 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 such 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 Act, 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.

SEC. 102. [6 U.S.C. 112] SECRETARY; FUNCTIONS.

(a) SECRETARY.—

(1) IN GENERAL.—There is a Secretary of Homeland Security, appointed by the President, by and with the advice and consent of the Senate.

(2) HEAD OF DEPARTMENT.—The Secretary is the head of the Department and shall have direction, authority, and control over it.

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

(b) FUNCTIONS.—The Secretary—

(1) except as otherwise provided by this Act, may delegate any of the Secretary's functions to any 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 Act or otherwise provided by law; and

(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.

(c) COORDINATION WITH NON-FEDERAL ENTITIES.—With respect to homeland security, the Secretary shall coordinate through the Office of State and Local Coordination (established under section 801) (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.

(d) 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.

(e) ISSUANCE OF REGULATIONS.—The issuance of regulations by the Secretary shall be governed by the provisions of chapter 5 of title 5, United States Code, except as specifically provided in this Act, in laws granting regulatory authorities that are transferred by this Act, and in laws enacted after the date of enactment of this Act.

(f) SPECIAL ASSISTANT TO THE SECRETARY.—The Secretary shall appoint a Special Assistant to the Secretary who shall be 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 of Homeland Security, 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 and Preparedness on all matters of concern to the private sector, including the tourism industry.

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

(h) 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 within under-served communities, in mission planning and mission execution. In furtherance of this subsection, the Secretary shall require each such head to seek, to the extent practicable, advice and feedback from organizations representing the needs of children. The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply whenever such advice or feedback is sought in accordance with this subsection.

SEC. 103. [6 U.S.C. 113] OTHER OFFICERS.

(a) DEPUTY SECRETARY; UNDER SECRETARIES.—

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

(A) 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, United States Code.

(B) An Under Secretary for Science and Technology.

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

(D) An Administrator of the Federal Emergency Management Agency.

(E) A Director of the Bureau of Citizenship and Immigration Services.

(F) An Under Secretary for Management, who shall be first assistant to the Deputy Secretary of Homeland Security for purposes of subchapter III of chapter 33 of title 5, United States Code.

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

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

(I) Not more than 12 Assistant Secretaries.

(J) A General Counsel, who shall be the chief legal officer of the Department.

(K) An 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 Health Affairs, 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.

(b) INSPECTOR GENERAL.—There shall be in the Department an Office of Inspector General and an Inspector General at the head of such office, as provided in chapter 4 of title 5, United States Code.

(c) 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 44 of title 14, United States Code, and who shall report directly to the Secretary. In addition to such duties as may be provided in this Act and as assigned to the Commandant by the Secretary, the duties of the Commandant shall include those required by section 2 of title 14, United States Code.

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

(1) A Director of the Secret Service.

(2) A Chief Information Officer.

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

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

(5) Any Director of a Joint Task Force under section 708.

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

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

(g) VACANCIES.—

(1) ABSENCE, DISABILITY, OR VACANCY OF SECRETARY OR DEPUTY SECRETARY.—Notwithstanding chapter 33 of title 5, United States Code, 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 Deputy Secretary is available to exercise the duties of the Office of the Secretary.

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

(3) 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, United States Code (commonly known as the "Federal Vacancies Reform Act of 1998").

TITLE II—INFORMATION ANALYSIS

Subtitle A—Information and Analysis; Access to Information

SEC. 201. [6 U.S.C. 121] INFORMATION AND ANALYSIS.

(a) INTELLIGENCE AND ANALYSIS.—There shall be in the Department an Office of Intelligence and Analysis.

(b) UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS.—

(1) OFFICE OF INTELLIGENCE AND ANALYSIS.—The Office of Intelligence and Analysis shall be headed by an Under Secretary for Intelligence and Analysis, who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) CHIEF INTELLIGENCE OFFICER.—The Under Secretary for Intelligence and Analysis shall serve as the Chief Intelligence Officer of the Department.

(c) DISCHARGE OF RESPONSIBILITIES.—The Secretary shall ensure that the responsibilities of the Department relating to information analysis, including those described in subsection (d), are carried out through the Under Secretary for Intelligence and Analysis.

(d) RESPONSIBILITIES OF SECRETARY RELATING TO INTELLIGENCE AND ANALYSIS.—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 such 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. 404o), in order 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 such 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 such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

(3) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether such 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, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such 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 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), including homeland security information, terrorism information, and weapons of mass destruction information, and any 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 such 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 such 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) any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties; and

(B) any intelligence information under this Act 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. 401 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 such 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 any 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 such 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 such 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 any 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 such 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 such component; and

(B) to present to the Secretary a recommendation for a consolidated budget for the intelligence components of the Department, together with any comments from the heads of such components.

(22) To perform such other duties relating to such responsibilities as the Secretary may provide.

(23)(A) Not later than six months after the date of the enactment of this paragraph, 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—

(i) a recommended strategy to protect and prepare the critical infrastructure of the homeland against threats of EMP and GMD; and

(ii) not less frequently than every two years thereafter for the next six years, updates of the recommended strategy.

(B) The recommended strategy under subparagraph (A) shall—

(i) be based on findings of the research and development conducted under section 320;

(ii) be developed in consultation with the relevant Federal sector-specific 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 conducted under subparagraph (A); and

(v) be submitted in unclassified form, but may include a classified annex.

(C) The Secretary may, if appropriate, incorporate the recommended strategy into a broader recommendation developed by the Department to help protect and prepare critical infrastructure from terrorism, cyber attacks, and other threats if, as incorporated, the recommended strategy complies with subparagraph (B).

(e) 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 such 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.

(f) DETAIL OF PERSONNEL.—

(1) IN GENERAL.—In order to assist the Office of Intelligence and Analysis in discharging responsibilities under this section, personnel of the agencies referred to 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 this paragraph 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 agree-

ments 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.

(g) FUNCTIONS TRANSFERRED.—In accordance with title XV, there shall be transferred to the Secretary, for assignment to the Office of Intelligence and Analysis and the Office of Infrastructure Protection under this section, the functions, personnel, assets, and liabilities of the following:

(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, 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.

* * * * * * *

SEC. 202. [6 U.S.C. 122] ACCESS TO INFORMATION.

(a) IN GENERAL.—

(1) THREAT AND VULNERABILITY INFORMATION.—Except as otherwise directed by the President, the Secretary shall have such access as 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 such information has been analyzed, that may be collected, possessed, or prepared by any agency of the Federal Government.

(2) OTHER INFORMATION.—The Secretary shall also 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 pursuant to this section—

(1) the Secretary may obtain such material upon request, and may enter into cooperative arrangements with other executive agencies to provide such material or provide Department officials with access to it on a regular or routine basis, includ-

ing requests or arrangements involving broad categories of material, access to electronic databases, or both; and

(2) regardless of whether the Secretary has made any request or entered into any cooperative arrangement pursuant to 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 such information has been analyzed;

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

(D) such 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 of 2001 (Public Law 107–56).

(2) Section 2517(6) of title 18, United States Code.

(3) Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure.

(d) ACCESS TO INTELLIGENCE AND OTHER INFORMATION.—

(1) ACCESS BY ELEMENTS OF FEDERAL GOVERNMENT.—Nothing in this title shall preclude any element of the intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)), or any other element of the Federal Government with responsibility for analyzing terrorist threat information, from receiving any 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 Department 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.

SEC. 203. [6 U.S.C. 124] HOMELAND SECURITY ADVISORY SYSTEM.

(a) REQUIREMENT.—The Secretary shall administer the Homeland Security Advisory System in accordance with 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 such 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 such advisories or warnings;

(2) develop a methodology, relying on the criteria established under paragraph (1), for the issuance and revocation of such advisories or warnings;

(3) provide, in each such 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 such advisory or warning to a specific region, locality, or economic sector believed to be under threat or at risk; and

(5) not, in issuing any 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.

SEC. 204. [6 U.S.C. 124a] HOMELAND SECURITY INFORMATION SHARING.

(a) INFORMATION SHARING.—Consistent with section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), 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(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))) except for any internal security protocols or personnel information of such 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 regarding coordinating the different systems used in the Department to gather and disseminate homeland security information or national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))).

(c) STATE, LOCAL, AND PRIVATE-SECTOR SOURCES OF INFORMATION.—

(1) ESTABLISHMENT OF BUSINESS PROCESSES.—The Secretary, acting through the Under Secretary for Intelligence and Analysis or 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 such information into the information gathered by the Department and other departments and agencies of the Federal Government; and

(C) make available such 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 any entity of State, local, or tribal government or the private sector that provides such 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(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))); and

(B) how information available to such 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 national intelligence, sharing information within the Department, as described in this title, and participating in the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485); and

(B) provide to the appropriate component heads regular reports regarding the evaluations under subparagraph (A).

SEC. 205. [6 U.S.C. 124b] COMPREHENSIVE INFORMATION TECHNOLOGY NETWORK ARCHITECTURE.

(a) ESTABLISHMENT.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall establish, consistent with the policies and procedures developed under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), 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.

(b) COMPREHENSIVE INFORMATION TECHNOLOGY NETWORK ARCHITECTURE DEFINED.—The term "comprehensive information tech-

nology 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.

SEC. 206. [6 U.S.C. 124c] COORDINATION WITH INFORMATION SHARING ENVIRONMENT.

(a) GUIDANCE.—All activities to comply with sections 203, 204, and 205 shall be—

(1) consistent with any policies, guidelines, procedures, instructions, or standards established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

(2) implemented in coordination with, as appropriate, the program manager for the information sharing environment established under that section;

(3) consistent with any applicable guidance issued by the Director of National Intelligence; and

(4) consistent with any 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 subtitle, the Under Secretary for Intelligence and Analysis shall take into account the views of the heads of the intelligence components of the Department.

SEC. 207. [6 U.S.C. 124d] INTELLIGENCE COMPONENTS.

Subject to the direction and control of the Secretary, and consistent with any 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(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))), 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 restruc-

ture 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 such employees comply with all applicable laws and regulations.

(7) To perform such other activities relating to such responsibilities as the Secretary may provide.

SEC. 208. [6 U.S.C. 124e] 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 defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))).

SEC. 209. [6 U.S.C. 124f] 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 such entities do not have the capacity, resources, or capabilities to conduct such training, the Secretary may approve another entity to conduct such 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.

SEC. 210. [6 U.S.C. 124g] INFORMATION SHARING INCENTIVES.

(a) AWARDS.—In making cash awards under chapter 45 of title 5, United States Code, the President or the head of an agency, in consultation with the program manager designated under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), 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(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)), in a manner consistent with any 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 1016(h) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485(h)), in consultation with the program manager designated under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), 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) publicizing information sharing accomplishments by individual employees and, where appropriate, the tangible end benefits that resulted.

SEC. 210A. [6 U.S.C. 124h] DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL, AND REGIONAL FUSION CENTER INITIATIVE.

(a) ESTABLISHMENT.—The Secretary, in consultation with the program manager of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), 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 (5 U.S.C. 601 note), shall establish a Department of Homeland Security State, Local, and Regional Fusion Center Initiative to establish partnerships with State, local, and regional fusion centers.

(b) 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 into 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 such 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 information, and weapons of mass destruction information, that is gathered by State, local, and regional fusion centers, and to incorporate such information, as appropriate, into the Department's own such 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 such fusion centers to participate in terrorism threat-related exercises conducted by the Department; and

(12) carry out such other duties as the Secretary determines are appropriate.

(c) 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) United States Customs and Border Protection.

(E) United States Immigration and Customs Enforcement.

(F) United States 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 as-

signing of Department officers or intelligence analysts under this section.

(B) CRITERIA.—Any 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 222 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 (5 U.S.C. 601 note); and

(iii) such 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 such officer or intelligence analyst and may use available funds for such purpose.

(6) FURTHER 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.

(d) 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 such information and other homeland security-relevant information provided by the Department; and

(4) assist in the dissemination of such 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.

(e) BORDER INTELLIGENCE PRIORITY.—

(1) IN GENERAL.—The Secretary shall make it a priority to assign officers and intelligence analysts under this section from United States Customs and Border Protection, United States 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 such 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 (d), officers and in-

telligence 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.

(f) DATABASE ACCESS.—In order to fulfill the objectives described under subsection (d), 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 any 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.

(g) CONSUMER FEEDBACK.—

(1) IN GENERAL.—The Secretary shall create a voluntary mechanism for any State, local, or tribal law enforcement officer or other emergency response provider who is a consumer of the intelligence or other information products referred to in subsection (d) to provide feedback to the Department on the quality and utility of such intelligence products.

(2) REPORT.—Not later than one year after the date of the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, and annually 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 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.

(h) RULE OF CONSTRUCTION.—

(1) IN GENERAL.—The authorities granted under this section shall supplement the authorities granted under section 201(d) and nothing in this section shall be construed to abrogate the authorities granted under section 201(d).

(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.

(i) 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 any such 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 any 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.

(j) FUSION CENTER INFORMATION SHARING STRATEGY.—Not later than 1 year after the date of the enactment of the DHS Field Engagement Accountability Act, and not less frequently than once every 5 years thereafter, the Secretary shall develop or update a strategy for Department engagement with fusion centers. Such 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. Such strategy shall include the following:

(1) Specific goals and objectives for sharing information and engaging with fusion centers—

(A) through the direct deployment of personnel from intelligence components of the Department;

(B) through 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) through 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.

(k) DEFINITIONS.—In this section—

(1) the term "fusion center" means a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity;

(2) the term "information sharing environment" means the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

(3) 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) 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; and

(5) the term "terrorism information" has the meaning given that term in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485).

(l) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $10,000,000 for each of fiscal years 2008 through 2012, to carry out this section, except for subsection (i), including for hiring officers and intelligence analysts to replace officers and intelligence analysts who are assigned to fusion centers under this section.

SEC. 210B. [6 U.S.C. 124i] HOMELAND SECURITY INFORMATION SHARING FELLOWS PROGRAM.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, and in consultation with the Chief Human Capital Officer, shall establish a fellowship program in accordance with this section for the purpose of—

(A) 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, United States Code, to participate in the work of the Office

of Intelligence and Analysis in order to become familiar with—

(i) the relevant missions and capabilities of the Department and other Federal agencies; and

(ii) the role, programs, products, and personnel of the Office of Intelligence and Analysis; and

(B) promoting information sharing between the Department and State, local, and tribal law enforcement officers and intelligence analysts by assigning such officers and analysts to—

(i) serve as a point of contact in the Department to assist in the representation of State, local, and tribal information requirements;

(ii) 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;

(iii) 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

(iv) 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 such products through appropriate Department channels.

(2) PROGRAM NAME.—The program under this section shall be known as the "Homeland Security Information Sharing Fellows Program".

(b) ELIGIBILITY.—

(1) IN GENERAL.—In order to be eligible for selection as an Information Sharing Fellow under the program under this section, an individual shall—

(A) have homeland security-related responsibilities;

(B) be eligible for an appropriate security clearance;

(C) possess a valid need for access to classified information, as determined by the Under Secretary for Intelligence and Analysis;

(D) be an employee of an eligible entity; and

(E) 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 Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note).

(2) ELIGIBLE ENTITIES.—In this subsection, the term "eligible entity" means—

(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) such other entity as the Secretary determines is appropriate.

(c) OPTIONAL PARTICIPATION.—No State, local, or tribal law enforcement or other government entity shall 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.

SEC. 210C. [6 U.S.C. 124j] RURAL POLICING INSTITUTE.

(a) 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 such programs.

(b) CURRICULA.—The training at the Rural Policing Institute established under subsection (a) shall—

(1) be configured in a manner so as not to duplicate or displace any law enforcement or emergency response program of the Federal Law Enforcement Training Center or a local or tribal government entity in existence on the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 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.

(c) DEFINITION.—In this section, the term "rural" means an area that is not located in a metropolitan statistical area, as defined by the Office of Management and Budget.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section (including for contracts, staff, and equipment)—

(1) $10,000,000 for fiscal year 2008; and

(2) $5,000,000 for each of fiscal years 2009 through 2013.

SEC. 210D. [6 U.S.C. 124k] 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 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485) 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 (referred to in this section as the "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 the 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 of Homeland Security 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, within 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 1016(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485(f)), 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 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), 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.—Beginning not later than 90 days after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, 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)(E) of the National Security Act of 1947 (50 U.S.C. 404o(f)(E)), the Director of the National Counterterrorism Center, acting through the senior intelligence official from the Department of Homeland Security detailed pursuant to subsection (d)(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 such 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)(E) of the National Security Act of 1947 (50 U.S.C. 402 et seq.), 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 (d)(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 that paragraph;

(D) all detailees under subsection (d)(5) have the appropriate security clearances and are trained in the proce-

dures 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 (d)(5) complete appropriate privacy and civil liberties training.

(g)[2] INAPPLICABILITY OF THE FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.)[2] shall not apply to the ITACG or any subsidiary groups thereof.

(h)[2] AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary for each of fiscal years 2008 through 2012 to carry out this section, including to obtain security clearances for the State, local, and tribal participants in the ITACG.

SEC. 210E. [6 U.S.C. 124m] CLASSIFIED INFORMATION ADVISORY OFFICER.

(a) REQUIREMENT TO ESTABLISH.—The Secretary shall identify and designate within the Department a Classified Information Advisory Officer, as described in this section.

(b) RESPONSIBILITIES.—The responsibilities of the Classified Information Advisory Officer shall be 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 such information to individuals who lack appropriate security clearances;

(B) regarding the appropriate procedures for challenging classification designations of information received by personnel of such entities; and

(C) on the means by which such 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 such personnel, as appropriate.

(c) INITIAL DESIGNATION.—Not later than 90 days after the date of the enactment of the Reducing Over-Classification Act, the Secretary shall—

(1) designate the initial Classified Information Advisory Officer; and

(2) submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on

[2] Section 4(a)(12)(A) of Public Law 117-286 provides for an amendment to strike "THE FEDERAL ADVISORY COMMITTEE ACT" and insert "CHAPTER 10 OF TITLE 5, UNITED STATES CODE" in the subsection heading of section 210D(h). Such amendment could not be carried out and probably should have been made to the subsection heading of section 210D(g). Section 4(a)(12)(B) of such Public Law also provides for an amendment to the section text of section 210D(h) to strike "The Federal Advisory Committee Act (5 U.S.C. App.)" and insert "Chapter 10 of title 5, United States Code,". Such amendment also could not be carried out and probably should have been made to subsection (g) of section 210D.

Homeland Security of the House of Representatives a written notification of the designation.

SEC. 210F. [6 U.S.C. 124m-1] DEPARTMENTAL COORDINATION ON COUNTER THREATS.

(a) ESTABLISHMENT.—There is authorized in the Department, for a period of 2 years beginning after the date of enactment of this section, a Counter Threats Advisory Board (in this section referred to as the "Board") which 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, which 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) 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 203.

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

SEC. 210G. [6 U.S.C. 124n] PROTECTION OF CERTAIN FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT.

(a) AUTHORITY.—Notwithstanding section 46502 of title 49, United States Code, or sections 32, 1030, 1367 and chapters 119 and 206 of title 18, United States Code, the Secretary and the Attorney General may, for their respective Departments, take, and may authorize personnel with assigned duties that include the security or protection of people, facilities, or assets, to take such actions as are described in subsection (b)(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.

(b) ACTIONS DESCRIBED.—

(1) IN GENERAL.—The actions authorized in subsection (a) 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) REQUIRED COORDINATION.—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, training on, and evaluation of any equipment, including any electronic equipment, to determine its capability and utility prior to the use of any such technology for any action described in subsection (b)(1).

(4) COORDINATION.—The Secretary and the Attorney General shall coordinate with the Administrator of the Federal Aviation Administration when any action authorized by this section might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace.

(c) FORFEITURE.—Any unmanned aircraft system or unmanned aircraft described in subsection (a) that is seized by the Secretary or the Attorney General is subject to forfeiture to the United States.

(d) REGULATIONS AND GUIDANCE.—

(1) IN GENERAL.—The Secretary, the Attorney General, and the Secretary of Transportation may prescribe regulations and shall issue guidance in the respective areas of each Secretary or the Attorney General to carry out this section.

(2) COORDINATION.—

(A) COORDINATION WITH DEPARTMENT 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) EFFECT ON AVIATION SAFETY.—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 such guidance or implementation might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of airspace.

(e) PRIVACY PROTECTION.—The regulations or guidance issued to carry out actions authorized under subsection (b) by each Secretary 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 First and Fourth Amendments to the Constitution of the United States 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 (b)(1);

(3) records of such communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Secretary of Homeland Security or the Attorney General determine that maintenance of such records is necessary to investigate or prosecute a violation of law, directly support an ongoing security operation, is required under Federal law, or for the purpose of any litigation;

(4) such communications are not disclosed outside the Department of Homeland Security 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 any regulatory, statutory, or other enforcement action relating to an action described in subsection (b)(1);

(C) is between the Department of Homeland Security and the Department of Justice in the course of a security or protection operation of either agency or a joint operation of such agencies; or

(D) is otherwise required by law; and

(5) to the extent necessary, the Department of Homeland Security and the Department of Justice are authorized to share threat information, which shall not include communications referred to in subsection (b), with State, local, territorial, or tribal law enforcement agencies in the course of a security or protection operation.

(f) 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 after fiscal year 2019, a consolidated funding display that identifies the funding source for the actions described in subsection (b)(1) within the Department of Homeland Security or the Department of Justice. The funding display shall be in unclassified form, but may contain a classified annex.

(g) SEMIANNUAL BRIEFINGS AND NOTIFICATIONS.—

(1) IN GENERAL.—On a semiannual basis during the period beginning 6 months after the date of enactment of this section and ending on the date specified in subsection (i), 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.

(2) REQUIREMENT.—Each briefing required under paragraph (1) shall be conducted jointly with the Secretary of Transportation.

(3) CONTENT.—Each briefing required under paragraph (1) shall include—

(A) policies, programs, and procedures to mitigate or eliminate impacts of such activities to the National Airspace System;

(B) a description of instances in which actions described in subsection (b)(1) have been taken, including all such instances that may have resulted in harm, damage, or loss to a person or to private property;

(C) 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;

(D) a description of options considered and steps taken to mitigate any identified impacts to the national airspace system related to the use of any system or technology, including the minimization of the use of any technology that

disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1);

(E) 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 of Justice or the Department of Homeland Security;

(F) 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;

(G) 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 such authorities.

(4) UNCLASSIFIED FORM.—Each briefing required under paragraph (1) shall be in unclassified form, but may be accompanied by an additional classified briefing.

(5) NOTIFICATION.—Within 30 days of deploying any new technology to carry out the actions described in subsection (b)(1), the Secretary and the Attorney General shall, respectively, submit a notification to the appropriate congressional committees. Such notification shall include a description of options considered to mitigate any identified impacts to the national airspace system related to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1).

(h) 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 of Homeland Security any authority of the Attorney General;

(4) vest in the Attorney General any authority of the Secretary of Homeland Security; or

(5) provide a new basis of liability for any 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 subsection (k)(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.

(i) TERMINATION.—The authority to carry out this section with respect to a covered facility or asset specified in subsection (k)(3) shall terminate on May 11, 2024.

(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) and (k)(3)(C)(iii).

(k) DEFINITIONS.—In this section:

(1) 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) 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) The term "covered facility or asset" means any 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 subparagraph (C)(i)(II) and (C)(iii)(I), such 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 one or more—

(i) missions authorized to be performed by the Department of Homeland Security, consistent with governing statutes, regulations, and orders issued by the Secretary, pertaining to—

(I) security or protection functions of the 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, United States Code, 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, United States Code;

(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, United States Code; and

(bb) the United States Marshals Service of Federal jurists, court officers, witnesses,

and other threatened persons in the interests of justice, as specified in section 566(e)(1)(A) of title 28, United States Code;

(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, United States Code;

(iii) missions authorized to be performed by the Department of Homeland Security or the Department of Justice, acting together or separately, consistent with governing statutes, regulations, and orders 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, upon 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 timeframe 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 timeframe and location; and

(iv) missions authorized to be performed by the United States Coast Guard, including those described in clause (iii) as directed by the Secretary, and as further set forth in section 104 of title 14, United States Code, and consistent with governing statutes, regulations, and orders issued by the Secretary of the Department in which the Coast Guard is operating.

(4) The terms "electronic communication", "intercept", "oral communication", and "wire communication" have the meaning given those terms in section 2510 of title 18, United States Code.

(5) 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) For purposes of subsection (a), the term "personnel" means officers and employees of the Department of Homeland Security or the Department of Justice.

(7) The terms "unmanned aircraft" and "unmanned aircraft system" have the meanings given those terms in section 44801, of title 49, United States Code.

(8) For purposes of this section, 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, 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 (b)(1).

(B) Options for mitigating any 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 which disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1).

(C) Potential consequences of the impacts of any actions taken under subsection (b)(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 any 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 persons or property.

(F) The setting, character, timeframe, and national airspace system impacts of National Special Security Event 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.

(l) DEPARTMENT OF HOMELAND SECURITY ASSESSMENT.—

(1) REPORT.—Not later than 1 year after the date of the enactment of this section, 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 this Act) and to domestic large hub airports (as defined in section 40102 of title 49, United States Code);

(B) an evaluation of current Federal and 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 en-

forcement 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 of Homeland Security 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 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) UNCLASSIFIED FORM.—The report required under paragraph (1) shall be submitted in unclassified form, but may contain a classified annex.

Subtitle B—Information Security

SEC. 221. [6 U.S.C. 141] PROCEDURES FOR SHARING INFORMATION.

The Secretary shall establish procedures on the use of information shared under this title that—

(1) limit the redissemination of such information to ensure that it is not used for an unauthorized purpose;

(2) ensure the security and confidentiality of such information;

(3) protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(4) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

SEC. 222. [6 U.S.C. 142] 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) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in 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 or that 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 such 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 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 such investigations and reports relating to the administration of the programs and operations of the Department as 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 performance of the responsibilities of the senior official under this section; and

(D) administer to or take from any person an oath, affirmation, or affidavit, whenever necessary to performance of the responsibilities of the senior official under this section.

(2) ENFORCEMENT OF SUBPOENAS.—Any subpoena issued under paragraph (1)(C) shall, in the case of contumacy or refusal to obey, be enforceable by order of any appropriate United States district court.

(3) EFFECT OF OATHS.—Any 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 THE INSPECTOR GENERAL.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the senior official appointed under subsection (a) may investigate any matter relating to possible violations or

abuse concerning the administration of any program or operation of the Department relevant to the purposes under this section.

(B) COORDINATION.—

(i) REFERRAL.—Before initiating any 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) DETERMINATIONS AND NOTIFICATIONS BY THE INSPECTOR GENERAL.—

(I) IN GENERAL.—Not later than 30 days after the receipt of a matter referred under clause (i), the Inspector General shall—

(aa) make a determination regarding whether the Inspector General intends to initiate an audit or investigation of the matter referred under clause (i); and

(bb) notify the senior official of that determination.

(II) INVESTIGATION NOT INITIATED.—If the Inspector General notifies the senior official under subclause (I)(bb) that the Inspector General intended 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 subclause shall be made not later than 3 days after the end of that 90-day period.

(iii) 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)(I)(bb) 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 (ii)(II) relating to that matter.

(iv) PRIVACY TRAINING.—Any employee of the Office of Inspector General who audits or investigates any 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 Houses of Congress; and

(2) include in any such 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 the Congress regarding performance of the responsibilities of the senior official under this section, without any prior comment or amendment by the Secretary, Deputy Secretary, 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 not either been approved or disapproved by the Secretary.

Subtitle C—Office of Science and Technology

SEC. 231. [6 U.S.C. 161] ESTABLISHMENT OF OFFICE; DIRECTOR.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—There is hereby established within the Department of Justice an Office of Science and Technology (hereinafter in this title referred to as the "Office").

(2) AUTHORITY.—The Office shall be under the general authority of the Assistant Attorney General, Office of Justice Programs, and shall be established within the National Institute of Justice.

(b) DIRECTOR.—The Office shall be headed by a Director, who shall be an individual appointed based on approval by the Office of Personnel Management of the executive qualifications of the individual.

SEC. 232. [6 U.S.C. 162] MISSION OF OFFICE; DUTIES.

(a) MISSION.—The mission of the Office shall be—

(1) to serve as the national focal point for work on law enforcement technology; and

(2) to carry out programs that, through the provision of equipment, training, and technical assistance, improve the safety and effectiveness of law enforcement technology and improve access to such technology by Federal, State, and local law enforcement agencies.

(b) DUTIES.—In carrying out its mission, the Office shall have the following duties:

(1) To provide recommendations and advice to the Attorney General.

(2) To establish and maintain advisory groups (which shall be exempt from the provisions of chapter 10 of title 5, United

States Code) to assess the law enforcement technology needs of Federal, State, and local law enforcement agencies.

(3) To establish and maintain performance standards in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113) for, and test and evaluate law enforcement technologies that may be used by, Federal, State, and local law enforcement agencies.

(4) To establish and maintain a program to certify, validate, and mark or otherwise recognize law enforcement technology products that conform to standards established and maintained by the Office in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113). The program may, at the discretion of the Office, allow for supplier's declaration of conformity with such standards.

(5) To work with other entities within the Department of Justice, other Federal agencies, and the executive office of the President to establish a coordinated Federal approach on issues related to law enforcement technology.

(6) To carry out research, development, testing, evaluation, and cost-benefit analyses in fields that would improve the safety, effectiveness, and efficiency of law enforcement technologies used by Federal, State, and local law enforcement agencies, including, but not limited to—

(A) weapons capable of preventing use by unauthorized persons, including personalized guns;

(B) protective apparel;

(C) bullet-resistant and explosion-resistant glass;

(D) monitoring systems and alarm systems capable of providing precise location information;

(E) wire and wireless interoperable communication technologies;

(F) tools and techniques that facilitate investigative and forensic work, including computer forensics;

(G) equipment for particular use in counterterrorism, including devices and technologies to disable terrorist devices;

(H) guides to assist State and local law enforcement agencies;

(I) DNA identification technologies; and

(J) tools and techniques that facilitate investigations of computer crime.

(7) To administer a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications.

(8) To serve on the Technical Support Working Group of the Department of Defense, and on other relevant interagency panels, as requested.

(9) To develop, and disseminate to State and local law enforcement agencies, technical assistance and training materials for law enforcement personnel, including prosecutors.

(10) To operate the regional National Law Enforcement and Corrections Technology Centers and, to the extent nec-

essary, establish additional centers through a competitive process.

(11) To administer a program of acquisition, research, development, and dissemination of advanced investigative analysis and forensic tools to assist State and local law enforcement agencies in combating cybercrime.

(12) To support research fellowships in support of its mission.

(13) To serve as a clearinghouse for information on law enforcement technologies.

(14) To represent the United States and State and local law enforcement agencies, as requested, in international activities concerning law enforcement technology.

(15) To enter into contracts and cooperative agreements and provide grants, which may require in-kind or cash matches from the recipient, as necessary to carry out its mission.

(16) To carry out other duties assigned by the Attorney General to accomplish the mission of the Office.

(c) COMPETITION REQUIRED.—Except as otherwise expressly provided by law, all research and development carried out by or through the Office shall be carried out on a competitive basis.

(d) INFORMATION FROM FEDERAL AGENCIES.—Federal agencies shall, upon request from the Office and in accordance with Federal law, provide the Office with any data, reports, or other information requested, unless compliance with such request is otherwise prohibited by law.

(e) PUBLICATIONS.—Decisions concerning publications issued by the Office shall rest solely with the Director of the Office.

(f) TRANSFER OF FUNDS.—The Office may transfer funds to other Federal agencies or provide funding to non-Federal entities through grants, cooperative agreements, or contracts to carry out its duties under this section: *Provided,* That any such transfer or provision of funding shall be carried out in accordance with section 605 of Public Law 107–77.

(g) ANNUAL REPORT.—The Director of the Office shall include with the budget justification materials submitted to Congress in support of the Department of Justice budget for each fiscal year (as submitted with the budget of the President under section 1105(a) of title 31, United States Code) a report on the activities of the Office. Each such report shall include the following:

(1) For the period of 5 fiscal years beginning with the fiscal year for which the budget is submitted—

(A) the Director's assessment of the needs of Federal, State, and local law enforcement agencies for assistance with respect to law enforcement technology and other matters consistent with the mission of the Office; and

(B) a strategic plan for meeting such needs of such law enforcement agencies.

(2) For the fiscal year preceding the fiscal year for which such budget is submitted, a description of the activities carried out by the Office and an evaluation of the extent to which those activities successfully meet the needs assessed under paragraph (1)(A) in previous reports.

SEC. 233. [6 U.S.C. 163] DEFINITION OF LAW ENFORCEMENT TECHNOLOGY.

For the purposes of this title, the term "law enforcement technology" includes investigative and forensic technologies, corrections technologies, and technologies that support the judicial process.

SEC. 234. [6 U.S.C. 164] ABOLISHMENT OF OFFICE OF SCIENCE AND TECHNOLOGY OF NATIONAL INSTITUTE OF JUSTICE; TRANSFER OF FUNCTIONS.

(a) AUTHORITY TO TRANSFER FUNCTIONS.—The Attorney General may transfer to the Office any other program or activity of the Department of Justice that the Attorney General, in consultation with the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives, determines to be consistent with the mission of the Office.

(b) TRANSFER OF PERSONNEL AND ASSETS.—With respect to any function, power, or duty, or any program or activity, that is established in the Office, those employees and assets of the element of the Department of Justice from which the transfer is made that the Attorney General determines are needed to perform that function, power, or duty, or for that program or activity, as the case may be, shall be transferred to the Office: *Provided,* That any such transfer shall be carried out in accordance with section 605 of Public Law 107–77.

(c) REPORT ON IMPLEMENTATION.—Not later than 1 year after the date of the enactment of this Act, the Attorney General shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report on the implementation of this title. The report shall—

(1) provide an accounting of the amounts and sources of funding available to the Office to carry out its mission under existing authorizations and appropriations, and set forth the future funding needs of the Office; and

(2) include such other information and recommendations as the Attorney General considers appropriate.

SEC. 235. [6 U.S.C. 165] NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTERS.

(a) IN GENERAL.—The Director of the Office shall operate and support National Law Enforcement and Corrections Technology Centers (hereinafter in this section referred to as "Centers") and, to the extent necessary, establish new centers through a merit-based, competitive process.

(b) PURPOSE OF CENTERS.—The purpose of the Centers shall be to—

(1) support research and development of law enforcement technology;

(2) support the transfer and implementation of technology;

(3) assist in the development and dissemination of guidelines and technological standards; and

(4) provide technology assistance, information, and support for law enforcement, corrections, and criminal justice purposes.

(c) ANNUAL MEETING.—Each year, the Director shall convene a meeting of the Centers in order to foster collaboration and communication between Center participants.

(d) REPORT.—Not later than 12 months after the date of the enactment of this Act, the Director shall transmit to the Congress a report assessing the effectiveness of the existing system of Centers and identify the number of Centers necessary to meet the technology needs of Federal, State, and local law enforcement in the United States.

[Sections 236 and 237 amend other laws and are not shown here.]

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

SEC. 301. [6 U.S.C. 181] UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.

There shall be in the Department a Directorate of Science and Technology headed by an Under Secretary for Science and Technology.

SEC. 302. [6 U.S.C. 182] RESPONSIBILITIES AND AUTHORITIES OF THE UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.

The Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility 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 comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such 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 such 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 any other agreements with the Department of Energy regarding the use of the national laboratories or sites and 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), as amended by section 1709(b);

(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.

SEC. 303. [6 U.S.C. 183] FUNCTIONS TRANSFERRED.

In accordance with title XV, there shall be transferred to the Secretary 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) Such life sciences activities of the biological and environmental research program related to microbial pathogens as may be 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.

SEC. 304. [6 U.S.C. 184] 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 such activities in collaboration with the Secretary of Homeland Security to ensure consistency with the national policy and strategic plan developed pursuant to section 302(2).

(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 such subsection.

* * * * * * *

SEC. 305. [6 U.S.C. 185] 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 1 or more federally funded research and development centers to provide independent analysis of homeland security issues, or to carry out other responsibilities under this Act, including coordinating and integrating both the extramural and intramural programs described in section 308.

SEC. 306. [6 U.S.C. 186] MISCELLANEOUS PROVISIONS.

(a) CLASSIFICATION.—To the greatest extent practicable, research conducted or supported by the Department shall be unclassified.

(b) CONSTRUCTION.—Nothing in this title shall be construed to preclude any Under Secretary of the Department from carrying out research, development, demonstration, or deployment activities, as long as such 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 such activities.

(d) NOTIFICATION OF PRESIDENTIAL LIFE SCIENCES DESIGNATIONS.—Not later than 60 days before effecting any transfer of Department of Energy life sciences activities pursuant to section 303(1)(D) of this Act, the President shall notify the appropriate congressional committees of the proposed transfer and shall include the reasons for the transfer and a description of the effect of the transfer on the activities of the Department of Energy.

SEC. 307. [6 U.S.C. 187] 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 established the Homeland Security Advanced Research Projects Agency.

(2) DIRECTOR.—HSARPA shall be headed by a Director, who shall be appointed by the Secretary. The Director shall report 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 persons, 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 shall have the hiring and management authorities described in section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note; Public Law 105–261). The term of appointments for employees under subsection (c)(1) of that section may not exceed 5 years before the granting of any extension under subsection (c)(2) of that section.

(7) DEMONSTRATIONS.—The Director, periodically, shall hold homeland security technology demonstrations to improve contact among technology developers, vendors and acquisition personnel.

(c) FUND.—

(1) ESTABLISHMENT.—There is established the Acceleration Fund for Research and Development of Homeland Security Technologies, which shall be administered by the Director of HSARPA.

(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $500,000,000 to the Fund for fiscal year 2003 and such sums as may be necessary thereafter.

(3) COAST GUARD.—Of the funds authorized to be appropriated under paragraph (2), not less than 10 percent of such funds for each fiscal year through fiscal year 2005 shall be authorized only for the Under Secretary, through joint agreement with the Commandant of the Coast Guard, to carry out research and development of improved ports, waterways and coastal security surveillance and perimeter protection capabilities for the purpose of minimizing the possibility that Coast Guard cutters, aircraft, helicopters, and personnel will be diverted from non-homeland security missions to the ports, waterways and coastal security mission.

SEC. 308. [6 U.S.C. 188] 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 302(4) 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 302(14); 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 establish 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 for homeland security, shall include, but are not limited to, demonstrated expertise in—

(i) The training of first responders.

(ii) Responding 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.

(xiv) The public policy implications and public dissemination of homeland security related research and development.

(C) DISCRETION OF SECRETARY.—To the extent that exercising such 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 section 308(b)(2)(B) and consider additional criteria beyond those specified in section 308(b)(2)(B). Upon 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, from the date of enactment, to Congress concerning the implementation of this section. That report shall indicate which center or centers have been des-

ignated and how the designation or designations enhance homeland security, as well as report any decisions to revoke or modify such designations.

(E) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out this paragraph.

(c) INTRAMURAL PROGRAMS.—

(1) CONSULTATION.—In carrying out the duties under section 302, 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 pursuant to paragraph (2), then 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.—No laboratory shall 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 such term is defined in section 4872(d) of title 10, United States Code; or

(ii) the Secretary determines is engaged in conduct that is detrimental to the national security of the United States.

(B) NONPROFIT ORGANIZATION; SMALL BUSINESS FIRM; SUBJECT INVENTION.—The terms "nonprofit organization", "small business firm", and "subject invention" have the meanings given such terms in section 201 of title 35, United States Code.

(C) MANUFACTURED SUBSTANTIALLY IN THE UNITED STATES.—The term "manufactured substantially in the United States" means an item is a domestic end product.

(D) DOMESTIC END PRODUCT.—The term "domestic end product" has the meaning given such term in section 25.003 of title 48, Code of Federal Regulations, or any successor thereto.

(3) WAIVERS.—

(A) IN GENERAL.—Subject to subparagraph (B), in individual cases, the requirements under section 204 of title 35, United States Code, may be waived by the Secretary upon 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 ON WAIVERS GRANTED BY DEPARTMENT.—

(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 (enacted as subtitle A of title IX of division G of Public Law 117–58).

(ii) PROHIBITION ON GRANTING CERTAIN WAIVERS.—The Secretary may not grant a waiver under subparagraph (A) if, as a result of such 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.

SEC. 309. [6 U.S.C. 189] 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 any 1 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) Any "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 any other law governing the administration, mission, use, or operations of any of the Department of Energy national laboratories and sites, such laboratories and sites are authorized to accept and perform work for the Secretary, consistent with resources provided, and perform such work on an

equal basis to other missions at the laboratory and not on a noninterference basis with other missions of such 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 1 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 such 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) FEDERAL ACQUISITION REGULATION.—Any 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 Regulations.

(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 such national laboratory under section 303(b)(1)(C) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 253(b)(1)(C)) or of such site to the extent such section applies to such 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 this Act from the Department of Energy to the Department of Homeland Security are being carried out through direct contracts with the operator of a national laboratory or site of the Department of Energy, the Secretary of Homeland Security and the Secretary of Energy shall ensure that direct contracts for such programs and activities between the Department of Homeland Security and such operator are separate from the direct contracts of the Department of Energy with such operator.

(d) AUTHORITY WITH RESPECT TO COOPERATIVE RESEARCH AND DEVELOPMENT AGREEMENTS AND LICENSING AGREEMENTS.—In connection with any utilization of the Department of Energy national laboratories and sites under this section, the Secretary may permit the director of any such 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 such an agreement consistent with the provisions of 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 any utilization of such laboratory or site under this section, the Department of Homeland Security shall reimburse the Department of Energy for costs of such activity through a method under which the Secretary of Energy waives any requirement for the Department of Homeland Security 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 such 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 any fiscal year may be obligated or expended for laboratory directed research and development activities carried out by the Department of Energy unless such activities support the missions of the Department of Homeland Security.

(g) OFFICE FOR NATIONAL LABORATORIES.—There is established within the Directorate of Science and Technology an Office for National Laboratories, which shall be 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 any research, development, test, and evaluation activities conducted within 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.

SEC. 310. [6 U.S.C. 190] TRANSFER OF PLUM ISLAND ANIMAL DISEASE CENTER, DEPARTMENT OF AGRICULTURE.

(a) IN GENERAL.—In accordance with title XV, the Secretary of Agriculture shall transfer to the Secretary of Homeland Security the Plum Island Animal Disease Center of the Department of Agriculture, including the assets and liabilities of the Center.

(b) CONTINUED DEPARTMENT OF AGRICULTURE ACCESS.—On completion of the transfer of the Plum Island Animal Disease Center under subsection (a), the Secretary of Homeland Security 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.

(c) 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 described in subsection (b).

(d) NOTIFICATION.—

(1) IN GENERAL.—At least 180 days before any change in the biosafety level at the Plum Island Animal Disease Center, the President shall notify Congress of the change and describe the reasons for the change.

(2) LIMITATION.—No change described in paragraph (1) may be made earlier than 180 days after the completion of the transition period (as defined in section 1501).

SEC. 311. [6 U.S.C. 191] HOMELAND SECURITY SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE.

(a) ESTABLISHMENT.—There is established within 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 shall consist of 20 members appointed by the Under Secretary for Science and Technology, which shall include emergency first-responders or representatives of organizations or associations of emergency first-responders. The Advisory Committee shall also 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 so selected as 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) ORIGINAL APPOINTMENTS.—The original members of the Advisory Committee shall be appointed to three classes. One class of six shall have a term of 1 year, one class of seven a term of 2 years, and one class of seven a term of 3 years.

(3) VACANCIES.—A member appointed to fill a vacancy occurring before the expiration of the term for which the mem-

ber's predecessor was appointed shall be appointed for the remainder of such term.

(d) ELIGIBILITY.—A person who has completed two consecutive full terms of service on the Advisory Committee shall thereafter be ineligible for appointment during the 1-year period following the expiration of the second such term.

(e) MEETINGS.—The Advisory Committee shall meet at least quarterly at the call of the Chair or whenever one-third of the members so request 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 shall constitute 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 render an annual report to the Under Secretary for Science and Technology for transmittal to Congress on or before January 31 of each year. Such report shall describe the activities and recommendations of the Advisory Committee during the previous year.

(2) ADDITIONAL REPORTS.—The Advisory Committee may render to the Under Secretary for transmittal to Congress such additional reports on specific policy matters as it considers appropriate.

(i) EXEMPTION FROM CHAPTER 10 OF TITLE 5, UNITED STATES CODE.—Section 1013 of title 5, United States Code, shall not apply to the Advisory Committee.

(j) TERMINATION.—The Department of Homeland Security Science and Technology Advisory Committee shall terminate on December 31, 2008.

SEC. 312. [6 U.S.C. 192] HOMELAND SECURITY INSTITUTE.

(a) ESTABLISHMENT.—The Secretary shall establish a federally funded research and development center to be known as the "Homeland Security Institute" (in this section referred to as the "Institute").

(b) ADMINISTRATION.—The Institute shall be administered as a separate entity by the Secretary.

(c) DUTIES.—The duties of the Institute shall be determined by the Secretary, and may include the following:

(1) Systems analysis, risk analysis, and simulation and modeling to determine the vulnerabilities of the Nation's critical infrastructures and the effectiveness of the systems deployed to reduce those vulnerabilities.

(2) Economic and policy analysis to assess the distributed costs and benefits of alternative approaches to enhancing security.

(3) Evaluation of the effectiveness of measures deployed to enhance the security of institutions, facilities, and infrastructure that may be terrorist targets.

(4) Identification of instances when common standards and protocols could improve the interoperability and effective utilization of tools developed for field operators and first responders.

(5) Assistance for Federal agencies and departments in establishing testbeds to evaluate the effectiveness of technologies under development and to assess the appropriateness of such technologies for deployment.

(6) Design of metrics and use of those metrics to evaluate the effectiveness of homeland security programs throughout the Federal Government, including all national laboratories.

(7) Design of and support for the conduct of homeland security-related exercises and simulations.

(8) Creation of strategic technology development plans to reduce vulnerabilities in the Nation's critical infrastructure and key resources.

(d) CONSULTATION ON INSTITUTE ACTIVITIES.—In carrying out the duties described in subsection (c), the Institute shall consult widely with representatives from private industry, institutions of higher education, nonprofit institutions, other Government agencies, and federally funded research and development centers.

(e) USE OF CENTERS.—The Institute shall utilize the capabilities of the National Infrastructure Simulation and Analysis Center.

(f) ANNUAL REPORTS.—The Institute shall transmit to the Secretary and Congress an annual report on the activities of the Institute under this section.

(g) TERMINATION.—The Homeland Security Institute shall terminate 5 years after its establishment.

SEC. 313. [6 U.S.C. 193] 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 101).

(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 such 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 paragraph (1) or (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, any other executive agency, any State or local government entity, or any 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).

SEC. 314. 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 7303(a)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(a)(1));

(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 such 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;

(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 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.

SEC. 315. EMERGENCY COMMUNICATIONS INTEROPERABILITY RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—The Under Secretary for Science and Technology, acting through 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 and 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.

(b) PURPOSES.—The purposes of the program established under subsection (a) 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.

(c) DEFINITIONS.—For purposes of this section, the term "interoperable", with respect to emergency communications, has the meaning given the term in section 1808.

SEC. 316. [6 U.S.C. 195b] NATIONAL BIOSURVEILLANCE INTEGRATION CENTER.

(a) 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 (referred to in this section as the "NBIC"), which shall be headed by a Directing Officer, under an office or directorate of the Department that is in existence as of the date of the enactment of this section.

(b) 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 such agencies to respond to a biological event of national concern; and

(2) oversee development and operation of the National Biosurveillance Integration System.

(c) 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 such 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 such 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 such 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 any incident that could develop into a biological event of national concern.

(d) RESPONSIBILITIES OF THE DIRECTING OFFICER OF THE NBIC.—

(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 bio-

logical 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, any affected regional, State, local, or tribal government, and any private sector entity considered appropriate that may enhance the mission of such 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 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485) and any 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 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485) 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.

(e) RESPONSIBILITIES OF THE NBIC MEMBER AGENCIES.—

(1) IN GENERAL.—Each Member Agency shall—

(A) 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;

(B) provide timely information to assist the NBIC in maintaining biological situational awareness for accurate detection and response purposes;

(C) enable the NBIC to receive and use biosurveillance information from member agencies to carry out its requirements under subsection (c);

(D) connect the biosurveillance data systems of that Member Agency to the NBIC data system under mutually agreed protocols that are consistent with subsection (c)(5);

(E) participate in the formation of strategy and policy for the operation of the NBIC and its information sharing;

(F) provide personnel to the NBIC under an interagency personnel agreement and consider the qualifications of such personnel necessary to provide human, animal, and environmental data analysis and interpretation support to the NBIC; and

(G) retain responsibility for the surveillance and intelligence systems of that department or agency, if applicable.

(f) 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.—Upon the request of the Directing Officer of the NBIC, the head of any Federal department or agency may detail, on a reimbursable basis, any of the personnel of that department or agency to the Department to assist the NBIC in carrying out this section.

(g) 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.

(h) RELATIONSHIP TO OTHER DEPARTMENTS AND AGENCIES.—The authority of the Directing Officer of the NBIC under this section shall not affect any authority or responsibility of any other department or agency of the Federal Government with respect to biosurveillance activities under any program administered by that department or agency.

(i) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as are necessary to carry out this section.

(j) DEFINITIONS.—In this section:

(1) The terms "biological agent" and "toxin" have the meanings given those terms in section 178 of title 18, United States Code.

(2) 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) The term "homeland security information" has the meaning given that term in section 892.

(4) The term "Member Agency" means any Federal department or agency that, at the discretion of the head of that department or agency, has entered a memorandum of understanding regarding participation in the NBIC.

(5) The term "Privacy Officer" means the Privacy Officer appointed under section 222.

SEC. 317. [6 U.S.C. 195c] PROMOTING ANTITERRORISM 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.—The Under Secretary shall establish the Science and Technology Homeland Security International Cooperative Programs Office.

(2) DIRECTOR.—The Office shall be headed by a Director, who—

(A) shall be selected, in consultation with the Assistant Secretary for International Affairs, by and shall report to the Under Secretary; and

(B) may be an officer of the Department serving in another position.

(3) RESPONSIBILITIES.—

(A) DEVELOPMENT OF MECHANISMS.—The Director shall be 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 shall be 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 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 those 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 entity 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 such amount at an appropriate rate, and such charges for administration of the grant as the Secretary determines appropriate.

(ii) MAXIMUM AMOUNT.—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 of Homeland Security 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, any 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.—Not later than one year after the date of enactment of this section, and every 5 years thereafter, the Under Secretary, acting through the Director, shall submit to Congress 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; and

(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, in coordination with the Assistant Secretary for the Countering Weapons of Mass Destruction 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, 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) Title V of the Foreign Relations Authorization Act, Fiscal Year 1979 (22 U.S.C. 2656a et seq.).

(2) Section 112b(c)[3] of title 1, United States Code.

(3) Section 1(e)(2) of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a(e)(2)).

(4) Sections 2 and 27 of the Arms Export Control Act (22 U.S.C. 2752 and 22 U.S.C. 2767).

(5) Section 622(c) of the Foreign Assistance Act of 1961 (22 U.S.C. 2382(c)).

(i) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section such sums as are necessary.

SEC. 318. [6 U.S.C. 195d] SOCIAL MEDIA WORKING GROUP.

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

(b) PURPOSE.—In order to enhance the dissemination of information through social media technologies between the Department

[3] Section 5947(a)(3) of Div. E of P.L. 117-263 calls for an amendment to strike "Section 112b(c)" and insert "Section 112b(g) ". This amendment is subject to a delayed effective date that shall take place 270 days after the date of enactment for this Act [9/19/23].

and appropriate stakeholders and to improve 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.—Membership of 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) CHAIRPERSON; CO-CHAIRPERSON.—

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

(B) 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.

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

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

(d) CONSULTATION WITH NON-MEMBERS.—To the extent practicable, the Group shall work with entities in the public and private sectors to carry out subsection (b).

(e) MEETINGS.—

(1) INITIAL MEETING.—Not later than 90 days after the date of enactment of this section, the Group shall hold its initial meeting.

(2) SUBSEQUENT MEETINGS.—After the initial meeting under paragraph (1), the Group shall meet—

(A) at the call of the chairperson; and

(B) not less frequently than twice each year.

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

(f) 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 the type of information disseminated through social media technologies, and how to access such information, during a natural disaster or an act of terrorism or other man-made disaster.

(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.

(g) DURATION OF GROUP.—

(1) IN GENERAL.—The Group shall terminate on the date that is 5 years after the date of enactment of this section unless the chairperson renews the Group for a successive 5-year period, prior to the date on which the Group would otherwise terminate, 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.

SEC. 319. [6 U.S.C. 195e] TRANSPARENCY IN RESEARCH AND DEVELOPMENT.

(a) REQUIREMENT TO LIST RESEARCH AND DEVELOPMENT PROGRAMS.—

(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 such project, including the component of the Department responsible for each such 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 (c).

(2) EXCEPTION FOR CERTAIN COMPLETED PROJECTS.—Paragraph (1) shall not apply to a project completed or otherwise terminated before the date of the enactment of this section.

(3) UPDATES.—The list required under paragraph (1) shall be updated as frequently as possible, but not less frequently than once per quarter.

(4) RESEARCH AND DEVELOPMENT DEFINED.—For purposes of the list required under paragraph (1), the Secretary shall provide a definition for the term "research and development".

(b) REQUIREMENT TO REPORT TO CONGRESS ON ALL PROJECTS.—Not later than January 1, 2017, 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 classified and unclassified report, as applicable, that lists each ongoing classified and unclassified project at the Department, including all appropriate details of each such project.

(c) INDICATORS OF SUCCESS OF 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) REQUIREMENT.—To the fullest extent possible, the tracking of a project required under paragraph (1) shall continue for the three-year period beginning on the date on which such project was transitioned to practice from research and development.

(d) 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 such project, including both classified and unclassified names if applicable;

(B) the name of the component of the Department carrying out such project;

(C) an abstract or summary of such project;

(D) funding levels for such project;

(E) project duration or timeline;

(F) the name of each contractor, grantee, or cooperative agreement partner involved in such project;

(G) expected objectives and milestones for such project; and

(H) to the maximum extent practicable, relevant literature and patents that are associated with such 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 11y. 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 (50 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.

(e) LIMITATION.—Nothing in this section overrides or otherwise affects the requirements specified in section 888.

SEC. 320. [6 U.S.C. 195f] 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—

(A) evaluating the risks to critical infrastructure from a range of threats of EMP and GMD; and

(B) which shall—

(i) be conducted in conjunction with the Office of Intelligence and Analysis; and

(ii) include a review and comparison of the range of threats and hazards facing critical infrastructure of the electrical grid.

(2) Determination of the critical utilities and national security assets and infrastructure that are at risk from threats of 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 one 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 differing levels of damage and disruption from various threats of EMP and GMD, as informed by the objective scientific analysis conducted under paragraph (1).

(6) An analysis of the feasibility of a real-time alert system to inform electrical grid operators and other stakeholders within milliseconds of a high-altitude nuclear explosion.

(c) EXEMPTION FROM DISCLOSURE.—

(1) INFORMATION SHARED WITH THE FEDERAL GOVERNMENT.—Section 2224, and any regulations issued pursuant to such section, shall apply to any information shared with the Federal Government under this section.

(2) INFORMATION SHARED BY THE FEDERAL GOVERNMENT.—Information shared by the Federal Government with a State, local, or tribal government under this section shall be 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) ROLES AND RESPONSIBILITIES.—

(A) DISTRIBUTION OF INFORMATION.—

(i) IN GENERAL.—Beginning not later than June 19, 2020, 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 ap-

propriate Sector-Specific 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) not later than June 19, 2020, 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-Specific 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.—Not later than March 26, 2020, and in coordination with the heads of relevant Sector-Specific 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 526, 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, in-

cluding the alerting capabilities of the integrated public alert and warning system authorized under section 526.

(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-Specific 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.

(2) 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-Specific 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 any 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-Specific 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.

(3) DEFINITIONS.—In this subsection:

(A) 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) 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) The term "Sector Risk Management Agency" has the meaning given that term in section 2200.

(e) RULE OF CONSTRUCTION.—Nothing in this section may be construe—

(1) to affect in any manner the authority of the executive branch to implement Executive Order 13865, dated March 26, 2019, and entitled "Coordinating National Resilience to Electromagnetic Pulses", or any other authority existing on the day before the date of enactment of this subsection 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 (6 U.S.C. 121 note), 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 the date of the enactment of this subsection.

SEC. 321. [6 U.S.C. 195g] COUNTERING UNMANNED AIRCRAFT SYSTEMS COORDINATOR.

(a) COORDINATOR.—

(1) IN GENERAL.—The Secretary shall designate an individual in a Senior Executive Service position (as defined in section 3132 of title 5, United States Code) of the Department

within the Office of Strategy, Policy, and Plans as the Countering Unmanned Aircraft Systems Coordinator (in this section referred to as the "Coordinator") and provide appropriate staff to carry out the responsibilities of the Coordinator.

(2) 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 unmanned aircraft systems (in this section referred to as "UAS") as described in section 210G;

(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 210G(g)(3); and

(F) carry out other related counter UAS authorities and activities under section 210G, as directed by the Secretary.

(b) 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.

(c) 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 to 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.

SEC. 322. [6 U.S.C. 195h] NATIONAL URBAN SECURITY TECHNOLOGY LABORATORY.

(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall designate the laboratory described in subsection (b) as an additional laboratory pursuant to the authority under section 308(c)(2) of this Act. Such 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.

(b) LABORATORY DESCRIBED.—The laboratory described in this subsection is the laboratory—

(1) known, as of the date of the enactment of this section, as the National Urban Security Technology Laboratory; and

(2) transferred to the Department pursuant to section 303(1)(E) of this Act.

(c) LABORATORY 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 such 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.

SEC. 323. [6 U.S.C. 195i] CHEMICAL SECURITY ANALYSIS CENTER.

(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall designate the laboratory described in subsection (b) as an additional laboratory pursuant to the authority under section 308(c)(2), which shall be used to conduct studies, analyses, and research to assess and address domestic chemical security events.

(b) LABORATORY DESCRIBED.—The laboratory described in this subsection is the laboratory known, as of the date of enactment of this section, as the Chemical Security Analysis Center.

(c) LABORATORY ACTIVITIES.—Pursuant to the authority under section 302(4), the Chemical Security Analysis 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 such 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, and respond to threats, hazards, and risks associated with domestic chemical security events; and

(6) carry out such other activities authorized under this section as the Secretary determines 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 within the Federal Government, including the activities and requirements of the Environmental Protection Agency under section 112(r) of the Clean 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 (commonly referred to as "Superfund"; 42 U.S.C. 9601 et seq.).

TITLE IV—BORDER, MARITIME, AND TRANSPORTATION SECURITY

Subtitle A—Border, Maritime, and Transportation Security Responsibilities and Functions

[Section 401 repealed by section 802(g)(2) of Public Law 114–125.]

SEC. 402. [6 U.S.C. 202] BORDER, MARITIME, AND TRANSPORTATION RESPONSIBILITIES.

The Secretary shall be 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 any officer, employee, or component of the Immigration and Naturalization Service) immediately before the date on which the transfer of functions specified under section 441 takes effect.

(4) Establishing and administering rules, in accordance with section 428, governing the granting of visas or other forms of permission, including parole, to enter the United States to individuals who are not a citizen or an alien lawfully admitted for permanent residence in the United States.

(5) Establishing national immigration enforcement policies and priorities.

(6) Except as provided in subtitle C, 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 of Homeland Security under section 421.

(8) In carrying out the foregoing responsibilities, ensuring the speedy, orderly, and efficient flow of lawful traffic and commerce.

SEC. 403. [6 U.S.C. 203] FUNCTIONS TRANSFERRED.

In accordance with title XV (relating to transition provisions), there shall be transferred to the Secretary the functions, personnel, assets, and liabilities of—

(1) the United States Customs Service of the Department of the Treasury, including the functions of the Secretary of the Treasury relating thereto;

(2) 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;

(3) the Federal Protective Service of the General Services Administration, including the functions of the Administrator of General Services relating thereto;

(4) the Federal Law Enforcement Training Center of the Department of the Treasury; and

(5) the Office for Domestic Preparedness of the Office of Justice Programs, including the functions of the Attorney General relating thereto.

SEC. 404. [6 U.S.C. 204] SURFACE TRANSPORTATION SECURITY ADVISORY COMMITTEE.

(a) ESTABLISHMENT.—The Administrator of the Transportation Security Administration (referred to in this section as "Administrator") shall establish within the Transportation Security Administration the Surface Transportation Security Advisory Committee (referred to in this section as the "Advisory Committee").

(b) DUTIES.—

(1) IN GENERAL.—The Advisory Committee 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.

(2) RISK-BASED SECURITY.—The Advisory Committee shall consider risk-based security approaches in the performance of its duties.

(c) MEMBERSHIP.—

(1) COMPOSITION.—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 such modes of surface transportation;

(B) labor organizations representing such modes of surface transportation;

(C) groups representing the users of such 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) CHAIRPERSON.—The Advisory Committee shall select a chairperson from among its voting members.

(4) TERM OF OFFICE.—

(A) TERMS.—

(i) 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.

(ii) REAPPOINTMENT.—A voting member of the Advisory Committee may be reappointed.

(B) REMOVAL.—

(i) IN GENERAL.—The Administrator may review the participation of a member of the Advisory Committee and remove such member for cause at any time.

(ii) ACCESS TO INFORMATION.—The Administrator may remove any member of the Advisory Committee that the Administrator determines should be restricted from reviewing, discussing, or possessing classified information or sensitive security information.

(5) PROHIBITION ON COMPENSATION.—The members of the Advisory Committee shall not receive any compensation from the Government by reason of their service on the Advisory Committee.

(6) MEETINGS.—

(A) IN GENERAL.—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 persons 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 (e)(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.

(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 any 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.

(8) 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) Aviation Security Advisory Committee established under section 44946 of title 49, United States Code.

(B) Maritime Security Advisory Committee established under section 70112 of title 46, United States Code.

(C) Railroad Safety Advisory Committee established by the Federal Railroad Administration.

(9) SUBJECT MATTER EXPERTS.—The Advisory Committee may request the assistance of subject matter experts with expertise related to the jurisdiction of the Advisory Committee.

(d) 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 REPORT.—

(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 that 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, United States Code.

(e) ADMINISTRATION RESPONSE.—

(1) CONSIDERATION.—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 that 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) NOTICES.—Not later than 30 days after the date 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 subparagraph (B) of that paragraph, as applicable; and

(B) provide the appropriate congressional committees with a briefing upon request.

(4) UPDATES.—Not later than 90 days after the date the Administrator receives a recommendation from the Advisory Committee under subsection (d)(2) that the Administrator agrees with, and quarterly 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.

(f) NONAPPLICABILITY OF FACA.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Advisory Committee or any subcommittee established under this section.

SEC. 405. [6 U.S.C. 205] OMBUDSMAN FOR IMMIGRATION DETENTION.

(a) IN GENERAL.—Within the Department, there shall be 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 any other action determined appropriate, for cases in which Department 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 any officer or employee of U.S. Customs and Border Protection or U.S. Immigration and Customs Enforcement, or any 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 of Homeland Security 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 within the Department of Homeland Security.

(c) ACCESS TO DETENTION FACILITIES.—The Ombudsman or designated personnel of the Ombudsman, shall be provided unfettered access to any location within each such detention facility and

shall be permitted confidential access to any detainee at the detainee's request and any departmental records concerning such detainee.

(d) COORDINATION WITH DEPARTMENT COMPONENTS.—

(1) IN GENERAL.—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 such officials by the Ombudsman within 60 days of receiving such 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 such information.

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

Subtitle B—U.S. Customs and Border Protection

SEC. 411. [6 U.S.C. 211] ESTABLISHMENT OF U.S. CUSTOMS AND BORDER PROTECTION; COMMISSIONER, DEPUTY COMMISSIONER, AND OPERATIONAL OFFICES.

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

(b) COMMISSIONER OF U.S. CUSTOMS AND BORDER PROTECTION.—

(1) IN GENERAL.—There shall be at the head of U.S. Customs and Border Protection a Commissioner of U.S. Customs and Border Protection (in this section referred to as the "Commissioner").

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

(c) DUTIES.—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 persons 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 persons who may undermine the security of the United States, in cases in which such persons 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 such term is defined in paragraph (17) of section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)), including—

(A) the inspection, processing, and admission of persons 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 persons 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 421;

(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 Department'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 205 of the Security and Accountability for Every Port Act of 2006 (6 U.S.C. 945); and

(B) the Customs–Trade Partnership Against Terrorism program under subtitle B of title II of such Act (6 U.S.C. 961 et seq.);

(15) conduct polygraph examinations in accordance with section 3(1) of the Anti-Border Corruption Act of 2010 (Public Law 111–376; 124 Stat. 4105);

(16) establish the standard operating procedures described in subsection (k);

(17) carry out the training required under subsection (l);

(18) carry out section 418, 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.

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

(e) U.S. BORDER PATROL.—

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

(2) CHIEF.—There shall be at the head of the U.S. Border Patrol a Chief, who shall—

(A) be at the level of Executive Assistant Commissioner within U.S. Customs and Border Protection; and

(B) report to the Commissioner.

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

(A) serve as the law enforcement office of U.S. Customs and Border Protection with primary responsibility for interdicting persons 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 the illegal entry of terrorists, terrorist weapons, persons, and contraband; and

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

(f) AIR AND MARINE OPERATIONS.—

(1) IN GENERAL.—There is established in U.S. Customs and Border Protection an office known as Air and Marine Operations.

(2) EXECUTIVE ASSISTANT COMMISSIONER.—There shall be at the head of Air and Marine Operations an Executive Assistant Commissioner, who shall report to the Commissioner.

(3) DUTIES.—Air and Marine Operations shall—

(A) serve as the law enforcement office within 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 established under paragraph (4); and

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

(4) AIR AND MARINE OPERATIONS CENTER.—

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

(B) EXECUTIVE DIRECTOR.—There shall be at the head of the Air and Marine Operations Center an Executive Director, who shall report to the Executive Assistant Commissioner 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, as directed by the Secretary;

(ii) monitor and coordinate the airspace for unmanned aerial systems operations of Air and Marine Operations in U.S. Customs and Border Protection;

(iii) detect, identify, and coordinate a response to threats to national security in the air domain, in coordination with other appropriate agencies, as determined by the Executive Assistant Commissioner;

(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 Executive Assistant Commissioner.

(g) OFFICE OF FIELD OPERATIONS.—

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

(2) EXECUTIVE ASSISTANT COMMISSIONER.—There shall be at the head of the Office of Field Operations an Executive Assistant Commissioner, who 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 such ports of entry;

(B) conduct inspections at such 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 established under paragraph (4);

(F) coordinate with the Executive Assistant Commissioner for the Office of Trade 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 prescribed by the Commissioner.

(4) NATIONAL TARGETING CENTER.—

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

(B) EXECUTIVE DIRECTOR.—There shall be at the head of the National Targeting Center an Executive Director, who 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 within U.S. Customs and Border Protection to collect and analyze traveler and cargo information in advance of arrival in the United States to identify and

address security risks and strengthen trade enforcement;

(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; and

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

(5) ANNUAL REPORT ON STAFFING.—

(A) IN GENERAL.—Not later than 30 days after the date of the enactment of the Trade Facilitation and Trade Enforcement Act of 2015, and annually thereafter, the Executive Assistant Commissioner shall 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 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 Assistant Commissioner determines that such 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 such.

(h) OFFICE OF INTELLIGENCE.—

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

(2) ASSISTANT COMMISSIONER.—There shall be at the head of the Office of Intelligence an Assistant Commissioner, who 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) manage the counterintelligence operations of U.S. Customs and Border Protection;

(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 prescribed by the Commissioner.

(i) OFFICE OF INTERNATIONAL AFFAIRS.—

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

(2) ASSISTANT COMMISSIONER.—There shall be at the head of the Office of International Affairs an Assistant Commissioner, who 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 organizations, and United States agencies in support of U.S. Customs and Border Protection's duties and responsibilities;

(D) provide necessary capacity building, training, and assistance to foreign customs and border control agencies to strengthen border, 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 as such matters relate 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 such agreements relate to the policies and regulations of U.S. Customs and Border Protection; and

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

(j) OFFICE OF PROFESSIONAL RESPONSIBILITY.—

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

(2) ASSISTANT COMMISSIONER.—There shall be at the head of the Office of Professional Responsibility an Assistant Commissioner, who 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 prescribed by the Commissioner.

(k) 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) uniform, standardized, and publicly-available procedures 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, United States Code (commonly referred to as the "Privacy Act" or 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 Executive 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 such a mission request;

(iii) a formal procedure to determine how such 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 subparagraph (A) of paragraph (1) 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 such search of the purpose and authority for such search, and how such individual may obtain information on reporting concerns about such search; and

(B) in the case of information collected by U.S. Customs and Border Protection through a search of an electronic device, if such information is transmitted to another Federal agency for subject matter assistance, translation, or decryption, the Commissioner to notify the individual subject to such search of such 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 such notifications would impair national security, law enforcement, or other operational interests.

(4) UPDATE AND REVIEW.—The Commissioner shall review and update every three years the standard operating procedures required under this subsection.

(5) AUDITS.—The Inspector General of the Department of Homeland Security shall develop and annually administer, during each of the three calendar years beginning in the calendar year that begins after the date of the enactment of the Trade Facilitation and Trade Enforcement Act of 2015, 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 subparagraph (A) of paragraph (1). Such 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 such searches.

(B) The number of such searches.

(C) The number of instances in which information contained in such devices that were subjected to such searches was retained, copied, shared, or entered in an electronic database.

(D) The number of such devices detained as the result of such searches.

(E) The number of instances in which information collected from such devices was subjected to such searches

and was transmitted to another Federal agency, including whether such transmissions resulted in a prosecution or conviction.

(6) REQUIREMENTS REGARDING OTHER NOTIFICATIONS.—The standard use of force procedures established pursuant to subparagraph (B) of paragraph (1) 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 such committees a copy of the evaluation pursuant to subparagraph (D) of such paragraph not later than 30 days after completion of such 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 an annual report, for each of the three calendar years beginning in the calendar year that begins after the date of the enactment of the Trade Facilitation and Trade Enforcement Act of 2015, that reviews whether the use of unmanned aerial systems is being conducted in conformity with the standard operating procedures required under subparagraph (E) of paragraph (1). Such reports—

(A) shall be submitted with the annual budget of the United States Government submitted by the President under section 1105 of title 31, United States Code;

(B) may be submitted in classified form if the Commissioner determines that such 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 such requests.

(l) 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.

(m) SHORT-TERM DETENTION STANDARDS.—

(1) 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 a United States port of entry or between ports of entry as soon as practicable following the time of such apprehension or during subsequent short-term detention.

(2) 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 such individual's rights, including the right to contact a representative of such individual's government for purposes of United States treaty obligations.

(B) FORM.—The information referred to in subparagraph (A) may be provided either verbally or in writing, and shall be posted in the detention holding cell in which such individual is being held. The information shall be provided in a language understandable to such individual.

(3) SHORT-TERM DETENTION DEFINED.—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.

(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 the date of the enactment of the Trade Facilitation and Trade Enforcement Act of 2015, the Comptroller General of the United States 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. Such report should also consider the operational efficiency of contracting the transportation and detention of such 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 such inspections, including information regarding the requirements under paragraphs (1) and (2) and, where appropriate, issue recommendations to improve the conditions of such facilities.

(n) WAIT TIMES TRANSPARENCY.—

(1) IN GENERAL.—The Commissioner shall—

(A) publish live wait times for travelers entering the United States 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 such 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 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, for each of the five calendar years beginning in the calendar year that begins after the date of the enactment of the Trade Facilitation and Trade Enforcement Act of 2015, a report that includes compilations of all such wait times and a ranking of such 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 such individual's clearance by a U.S. Customs and Border Protection officer.

(o) 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 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 not later than 30 days before exercising such authority.

(3) RESCUE BEACONS.—Beginning in fiscal year 2019, in carrying out subsection (c)(8), the Commissioner shall purchase, deploy, and maintain not more than 250 self-powering, 9–1–1 cellular relay rescue beacons along the southern border of the United States at locations determined appropriate by the Commissioner to mitigate migrant deaths.

(p) REPORTS TO CONGRESS.—The Commissioner shall, on and after the date of the enactment of the Trade Facilitation and Trade Enforcement Act of 2015, 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, on the day before such date of enactment, to be submitted under any provision of law.

(q) OTHER FEDERAL AGENCIES.—Nothing in this section may be construed as affecting in any manner the authority, existing on the day before the date of the enactment of the Trade Facilitation and Trade Enforcement Act of 2015, of any other Federal agency or component of the Department.

(r) 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 such

terms in section 2 of the Trade Facilitation and Trade Enforcement Act of 2015.

SEC. 412. [6 U.S.C. 212] 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 403(a)(1), authority related to Customs revenue functions that was vested in the Secretary of the Treasury by law before the effective date of this Act under those provisions of law set forth in paragraph (2) shall not be transferred to the Secretary by reason of this Act, and on and after the effective date of this Act, the Secretary of the Treasury may delegate any such 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 any such authority not delegated to the Secretary.

(2) STATUTES.—The provisions of law referred to in paragraph (1) are the following: the Tariff Act of 1930; section 249 of the Revised Statutes of the United States (19 U.S.C. 3); section 2 of the Act of March 4, 1923 (19 U.S.C. 6); section 13031 of the Consolidated Omnibus Budget Reconciliation Act of 1985 (19 U.S.C. 58c); section 251 of the Revised Statutes of the United States (19 U.S.C. 66); section 1 of the Act of June 26, 1930 (19 U.S.C. 68); the Foreign Trade Zones Act (19 U.S.C. 81a et seq.); section 1 of the Act of March 2, 1911 (19 U.S.C. 198); the Trade Act of 1974; the Trade Agreements Act of 1979; the North American Free Trade Area Implementation Act; the Uruguay Round Agreements Act; the Caribbean Basin Economic Recovery Act; the Andean Trade Preference Act; the African Growth and Opportunity Act; and 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 any other provision of this Act, the Secretary may not consolidate, discontinue, or diminish those functions described in paragraph (2) performed by U.S. Customs and Border Protection (as established under section 411) on or after the effective date of this Act, reduce the staffing level, or reduce the resources attributable to such functions, and the Secretary shall ensure that an appropriate management structure is implemented to carry out such 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 the day before the effective date of this Act: Import Specialists, Entry Specialists, Drawback Specialists, National Import Specialist, Fines and Penalties Specialists, attorneys of the Office of Regulations and Rulings, Customs Auditors, International Trade Specialists, Financial Systems Specialists.

(c) NEW PERSONNEL.—The Secretary of the Treasury is authorized to appoint up to 20 new personnel to work with personnel of the Department in performing customs revenue functions.

SEC. 413. [6 U.S.C. 213] PRESERVATION OF CUSTOMS FUNDS.

Notwithstanding any other provision of this Act, no funds collected under paragraphs (1) through (8) of section 13031(a) of the Consolidated Omnibus Budget Reconciliation Act of 1985 may be transferred for use by any other agency or office in the Department.

SEC. 414. [6 U.S.C. 214] SEPARATE BUDGET REQUEST FOR CUSTOMS.

The President shall include in each budget transmitted to Congress under section 1105 of title 31, United States Code, a separate budget request for U.S. Customs and Border Protection.

SEC. 415. [6 U.S.C. 215] DEFINITION.

In this subtitle, 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 such 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 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 the United States Customs Service on the day before the effective date of this Act, and of U.S. Customs and Border Protection on the day before the effective date of the U.S. Customs and Border Protection Authorization Act: Import Specialists, Entry Specialists, Drawback Specialists, National Import Specialist, Fines and Penalties Specialists, attorneys of the Office of Regulations and Rulings, Customs Auditors, International Trade Specialists, 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 the day before the effective date of this Act, and of U.S. Customs and Border Protection on the day before the effective date of the U.S. Customs and Border Protection Authorization Act: the Office of Information and Technology, the Office of Laboratory Services, the Office of the Chief Counsel, the Office of Congressional Affairs, the Office of International Affairs, and the Office of Training and Development.

SEC. 416. [6 U.S.C. 216] PROTECTION AGAINST POTENTIAL SYNTHETIC OPIOID EXPOSURE.

(a) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection shall issue a policy that specifies effective protocols and procedures for the safe handling of potential synthetic opioids, including fentanyl, by U.S. Customs and Border Protection officers, agents, other personnel, and canines, and 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 of U.S. Customs and Border Protection 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 such handling.

(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.—The training described in paragraph (1) may be integrated into existing training under section 411(l) for 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 of U.S. Customs and Border Protection shall ensure the availability of personal protective equipment, opioid receptor antagonists, including 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 effectiveness of the policy described in subsection (a)—

(1) the Commissioner of U.S. Customs and Border Protection shall regularly monitor the efficacy of the implementation of such 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 the date of the enactment of this section.

SEC. 417. [6 U.S.C. 217] ALLOCATION OF RESOURCES BY THE SECRETARY.

(a) IN GENERAL.—The Secretary shall ensure that adequate staffing is provided to assure that levels of customs revenue services provided on the day before the effective date of this Act shall continue to be provided.

(b) NOTIFICATION OF CONGRESS.—The Secretary shall notify the Committee on Ways and Means of the House of Representa-

tives and the Committee on Finance of the Senate at least 90 days prior to taking any action which would—

(1) result in any significant reduction in customs revenue services, including hours of operation, provided at any office within the Department or any port of entry;

(2) eliminate or relocate any office of the Department which provides customs revenue services; or

(3) eliminate any port of entry.

(c) DEFINITION.—In this section, the term "customs revenue services" means those customs revenue functions described in paragraphs (1) through (6) and paragraph (8) of section 415.

SEC. 418. [6 U.S.C. 218] ASIA-PACIFIC ECONOMIC COOPERATION BUSINESS TRAVEL CARDS.

(a) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection is authorized to issue an Asia-Pacific Economic Cooperation Business Travel Card (referred to in this section as an "ABT Card") to any individual described in subsection (b).

(b) CARD ISSUANCE.—An individual described in this subsection 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 of U.S. Customs and Border Protection; or

(B) a United States Government official actively engaged in Asia-Pacific Economic Cooperation business, as determined by the Commissioner of U.S. Customs and Border Protection.

(c) INTEGRATION WITH EXISTING TRAVEL PROGRAMS.—The Commissioner of U.S. Customs and Border Protection shall integrate application procedures for, and issuance, renewal, and revocation of, ABT Cards with existing international trusted traveler programs of the Department.

(d) COOPERATION WITH PRIVATE ENTITIES AND NONGOVERNMENTAL ORGANIZATIONS.—In carrying out this section, the Commissioner of U.S. Customs and Border Protection may consult with appropriate private sector entities and nongovernmental organizations, including academic institutions.

(e) FEE.—

(1) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection shall—

(A) prescribe and collect a fee for the issuance and renewal of ABT Cards; and

(B) adjust such fee to the extent the Commissioner determines necessary to comply with paragraph (2).

(2) LIMITATION.—The Commissioner of U.S. Customs and Border Protection shall ensure that the total amount of the fees collected under paragraph (1) during any fiscal year is sufficient to offset the direct and indirect costs associated with carrying out this section during such fiscal year, including the

costs associated with operating and maintaining the ABT Card issuance and renewal processes.

(3) ACCOUNT FOR COLLECTIONS.—There is established in the Treasury of the United States 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 established under paragraph (3) shall—

(A) be credited to the appropriate account of the U.S. Customs and Border Protection for expenses incurred in carrying out this section; and

(B) remain available until expended.

(f) NOTIFICATION.—The Commissioner of U.S. Customs and Border Protection 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 (e)(1).

(g) TRUSTED TRAVELER PROGRAM DEFINED.—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.

[A section 419 exists in law, however, it amends other Acts and is not shown here.]

Subtitle C—Miscellaneous Provisions

SEC. 421. [6 U.S.C. 231] TRANSFER OF CERTAIN AGRICULTURAL INSPECTION FUNCTIONS OF THE DEPARTMENT OF AGRICULTURE.

(a) TRANSFER OF AGRICULTURAL IMPORT AND ENTRY INSPECTION FUNCTIONS.—There shall be transferred to the Secretary the functions of the Secretary of Agriculture relating to agricultural import and entry inspection activities under the laws specified in subsection (b).

(b) COVERED ANIMAL AND PLANT PROTECTION LAWS.—The laws referred to in subsection (a) are the following:

(1) The Act commonly known as the Virus-Serum-Toxin Act (the eighth paragraph under the heading "Bureau of Animal Industry" in the Act of March 4, 1913; 21 U.S.C. 151 et seq.).

(2) Section 1 of the Act of August 31, 1922 (commonly known as the Honeybee Act; 7 U.S.C. 281).

(3) Title III of the Federal Seed Act (7 U.S.C. 1581 et seq.).

(4) The Plant Protection Act (7 U.S.C. 7701 et seq.).

(5) The Animal Health Protection Act (subtitle E of title X of Public Law 107–171; 7 U.S.C. 8301 et seq.).

(6) The Lacey Act Amendments of 1981 (16 U.S.C. 3371 et seq.).

(7) Section 11 of the Endangered Species Act of 1973 (16 U.S.C. 1540).

(c) EXCLUSION OF QUARANTINE ACTIVITIES.—For purposes of this section, the term "functions" does not include any quarantine activities carried out under the laws specified in subsection (b).

(d) EFFECT OF TRANSFER.—

(1) COMPLIANCE WITH DEPARTMENT OF AGRICULTURE REGULATIONS.—The authority transferred pursuant to subsection (a) 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 subsection (b).

(2) RULEMAKING COORDINATION.—The Secretary of Agriculture shall coordinate with the Secretary whenever the Secretary of Agriculture prescribes regulations, policies, or procedures for administering the functions transferred under subsection (a) under a law specified in subsection (b).

(3) EFFECTIVE ADMINISTRATION.—The Secretary, in consultation with the Secretary of Agriculture, may issue such directives and guidelines as are necessary to ensure the effective use of personnel of the Department of Homeland Security to carry out the functions transferred pursuant to subsection (a).

(e) TRANSFER AGREEMENT.—

(1) AGREEMENT REQUIRED; REVISION.—Before the end of the transition period, as defined in section 1501, the Secretary of Agriculture and the Secretary shall enter into an agreement to effectuate the transfer of functions required by subsection (a). The Secretary of Agriculture and the Secretary may jointly revise the agreement as necessary thereafter.

(2) REQUIRED TERMS.—The agreement required by this subsection shall specifically address the following:

(A) The supervision by the Secretary of Agriculture of the training of employees of the Secretary to carry out the functions transferred pursuant to subsection (a).

(B) The transfer of funds to the Secretary under subsection (f).

(3) COOPERATION AND RECIPROCITY.—The Secretary of Agriculture and the Secretary may include as part of the agreement the following:

(A) Authority for the Secretary to perform functions delegated to the Animal and Plant Health Inspection Service of the Department of Agriculture regarding the protection of domestic livestock and plants, but not transferred to the Secretary pursuant to subsection (a).

(B) Authority for the Secretary of Agriculture to use employees of the Department of Homeland Security to carry out authorities delegated to the Animal and Plant Health Inspection Service regarding the protection of domestic livestock and plants.

(f) PERIODIC TRANSFER OF FUNDS TO DEPARTMENT OF HOMELAND SECURITY.—

(1) TRANSFER OF FUNDS.—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 in accordance with the agreement under subsection (e), to the Secretary funds for activities carried out by the Secretary for which such fees were collected.

(2) LIMITATION.—The proportion of fees collected pursuant to such sections that are transferred to the Secretary under this subsection may not exceed the proportion of the costs incurred by the Secretary to all costs incurred to carry out activities funded by such fees.

(g) TRANSFER OF DEPARTMENT OF AGRICULTURE EMPLOYEES.—Not later than the completion of the transition period defined under section 1501, the Secretary of Agriculture shall transfer to the Secretary not more than 3,200 full-time equivalent positions of the Department of Agriculture.

* * * * * * *

SEC. 422. [6 U.S.C. 232] FUNCTIONS OF ADMINISTRATOR OF GENERAL SERVICES.

(a) OPERATION, MAINTENANCE, AND PROTECTION OF FEDERAL BUILDINGS AND GROUNDS.—Nothing in this Act 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 403(3), the Administrator shall retain all powers, functions, and authorities vested in the Administrator under chapter 10 of title 40, United States Code, and other provisions of law that are necessary for the operation, maintenance, and protection of such buildings and grounds.

(b) COLLECTION OF RENTS AND FEES; FEDERAL BUILDINGS FUND.—

(1) STATUTORY CONSTRUCTION.—Nothing in this Act 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 any other official in the Department to obligate amounts in the Federal Buildings Fund established by section 490(f) of title 40, United States Code.

(2) USE OF TRANSFERRED AMOUNTS.—Any 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.

SEC. 423. [6 U.S.C. 233] FUNCTIONS OF TRANSPORTATION SECURITY ADMINISTRATION.

(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 any action that might affect aviation safety, air carrier operations, aircraft airworthiness, or the use of airspace. The Secretary shall establish a liaison office within the Department for the

purpose of consulting with the Administrator of the Federal Aviation Administration.

(b) REPORT TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Secretary of Transportation shall transmit to Congress a report containing a plan for complying with the requirements of section 44901(d) of title 49, United States Code, as amended by section 425 of this Act.

(c) LIMITATIONS ON STATUTORY CONSTRUCTION.—

(1) GRANT OF AUTHORITY.—Nothing in this Act may be construed to vest in the Secretary or any other official in the Department any authority over transportation security that is not vested in the Under Secretary of Transportation for Security, or in the Secretary of Transportation under chapter 449 of title 49, United States Code, on the day before the date of enactment of this Act.

(2) OBLIGATION OF AIP FUNDS.—Nothing in this Act 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, United States Code.

SEC. 424. [6 U.S.C. 234] PRESERVATION OF TRANSPORTATION SECURITY ADMINISTRATION AS A DISTINCT ENTITY.

Notwithstanding any other provision of this Act, the Transportation Security Administration shall be maintained as a distinct entity within the Department.

SEC. 427. [6 U.S.C. 235] 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 1 or more affected agencies, is timely and efficiently exchanged between the affected agencies.

(c) REPORT AND PLAN.—Not later than 18 months after the date of enactment of this Act, the Secretary, in consultation 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 submit to Congress—

(1) a report on the progress made in implementing this section; and

(2) a plan to complete implementation of this section.

SEC. 428. [6 U.S.C. 236] VISA ISSUANCE.

(a) DEFINITION.—In this subsection, the term "consular office" has the meaning given that term under section 101(a)(9) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(9)).

(b) IN GENERAL.—Notwithstanding section 104(a) of the Immigration and Nationality Act (8 U.S.C. 1104(a)) or any other provision of 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, administer, and enforce the provisions of such Act, 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 any officer or employee of the United States, with the consent of the head of the executive agency under whose jurisdiction such 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 such 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) (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 219(a) of the Immigration and Nationality Act (8 U.S.C. 1189(a)).

(J) Section 237(a)(4)(C) of the Immigration and Nationality Act (8 U.S.C. 1227(a)(4)(C)).

(K) Section 401 of the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996 (22 U.S.C. 6034; Public Law 104–114).

(L) Section 613 of the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies Appropriations Act, 1999 (as contained in section 101(b) of division A of Public Law 105–277) (Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999); 112 Stat. 2681; H.R. 4328 (originally H.R. 4276) as amended by section 617 of Public Law 106–553.

(M) Section 103(f) of the Chemical Weapon Convention Implementation Act of 1998 (112 Stat. 2681–865).

(N) Section 801 of H.R. 3427, the Admiral James W. Nance and Meg Donovan Foreign Relations Authorization Act, Fiscal Years 2000 and 2001, as enacted by reference in Public Law 106–113.

(O) Section 568 of the Foreign Operations, Export Financing, and Related Programs Appropriations Act, 2002 (Public Law 107–115).

(P) Section 51 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2723).

(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 HOMELAND SECURITY EMPLOYEES TO DIPLOMATIC AND CONSULAR POSTS.—

(1) IN GENERAL.—The Secretary is authorized to assign employees of the Department to each diplomatic and consular post at which visas are issued, unless the Secretary determines that such an assignment at a particular post would not promote homeland security.

(2) FUNCTIONS.—Employees assigned under paragraph (1) shall perform the following functions:

(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 any such applications, either on the initiative of the employee of the Department or upon request by a consular officer or other person charged with adjudicating such applications.

(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 deemed 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, any such 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 any 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 such 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 is authorized to use the National Foreign Affairs Training Center, on a reimbursable basis, to obtain the training described in subparagraph (A).

(7) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary and the Secretary of State shall submit to Congress—

(A) a report on the implementation of this subsection; and

(B) any legislative proposals necessary to further the objectives of this subsection.

(8) EFFECTIVE DATE.—This subsection shall take effect on the earlier of—

(A) the date on which the President publishes notice in the Federal Register that the President has submitted a report to Congress setting forth a memorandum of un-

derstanding between the Secretary and the Secretary of State governing the implementation of this section; or

(B) the date occurring 1 year after the date of enactment of this Act.

(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) STUDY REGARDING USE OF FOREIGN NATIONALS.—

(1) IN GENERAL.—The Secretary of Homeland Security shall conduct a study of the role of foreign nationals in the granting or refusal of visas and other documents authorizing entry of aliens into the United States. The study shall address the following:

(A) The proper role, if any, of foreign nationals in the process of rendering decisions on such grants and refusals.

(B) Any security concerns involving the employment of foreign nationals.

(C) Whether there are cost-effective alternatives to the use of foreign nationals.

(2) REPORT.—Not later than 1 year after the date of the enactment of this Act, the Secretary shall submit a report containing the findings of the study conducted under paragraph (1) to the Committee on the Judiciary, the Committee on International Relations, and the Committee on Government Reform of the House of Representatives, and the Committee on the Judiciary, the Committee on Foreign Relations, and the Committee on Government Affairs of the Senate.

(h) REPORT.—Not later than 120 days after the date of the enactment of this Act, the Director of the Office of Science and Technology Policy shall submit to Congress a report on how the provisions of this section will affect procedures for the issuance of student visas.

(i) VISA ISSUANCE PROGRAM FOR SAUDI ARABIA.—Notwithstanding any other provision of law, after the date of the enactment of this Act all third party screening programs in Saudi Arabia shall be terminated. On-site personnel of the Department of Homeland Security shall review all visa applications prior to adjudication.

SEC. 429. [6 U.S.C. 237] 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 any 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).

SEC. 430. [6 U.S.C. 238] OFFICE FOR DOMESTIC PREPAREDNESS.

(a) ESTABLISHMENT.—There is established in the Department an Office for Domestic Preparedness.

(b) DIRECTOR.—There shall be a Director of the Office for Domestic Preparedness, who shall be appointed by the President.

(c) RESPONSIBILITIES.—The Office for Domestic Preparedness shall have the primary responsibility within the executive branch of Government 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, and 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) those elements of the Office of National Preparedness of the Federal Emergency Management Agency which relate to terrorism, which shall be consolidated within the Department in the Office for Domestic Preparedness established under this section; and

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

(d) FISCAL YEARS 2003 and 2004.—During fiscal year 2003 and fiscal year 2004, the Director of the Office for Domestic Preparedness established under this section shall manage and carry out those functions of the Office for Domestic Preparedness of the Department of Justice (transferred under this section) before September 11, 2001, under the same terms, conditions, policies, and authorities, and with the required level of personnel, assets, and budget before September 11, 2001.

SEC. 431. [6 U.S.C. 239] OFFICE OF CARGO SECURITY POLICY.

(a) ESTABLISHMENT.—There is established within the Department an Office of Cargo Security Policy (referred to in this section as the "Office").

(b) PURPOSE.—The Office shall—

(1) coordinate all Department policies relating to cargo security; and

(2) consult with stakeholders and coordinate with other Federal agencies in the establishment of standards and regulations and to promote best practices.

(c) DIRECTOR.—

(1) APPOINTMENT.—The Office shall be headed by a Director, who shall—

(A) be appointed by the Secretary; and

(B) report to the Assistant Secretary for Policy.

(2) RESPONSIBILITIES.—The Director shall—

(A) advise the Assistant Secretary for Policy in the development of Department-wide policies regarding cargo security;

(B) coordinate all policies relating to cargo security among the agencies and offices within the Department relating to cargo security; and

(C) coordinate the cargo security policies of the Department with the policies of other executive agencies.

SEC. 432. [6 U.S.C. 240] BORDER ENFORCEMENT SECURITY TASK FORCE.

(a) ESTABLISHMENT.—There is established within the Department a program to be known as the Border Enforcement Security Task Force (referred to in this section as "BEST").

(b) PURPOSE.—The purpose of 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 such agencies.

(c) 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 United States 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 OF UNITS.—The Secretary is authorized to establish BEST units in jurisdictions in which such 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 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.

(d) OPERATION.—After determining the jurisdictions in which to establish BEST units under subsection (c)(2), and in order to provide Federal assistance to such 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.

(e) REPORT.—Not later than 180 days after the date on which BEST is established under this section, and annually thereafter for the following 5 years, 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.

SEC. 433. [6 U.S.C. 241] PREVENTION OF INTERNATIONAL CHILD ABDUCTION.

(a) PROGRAM ESTABLISHED.—The Secretary, through the Commissioner of U.S. Customs and Border Protection (referred to in this section as "CBP"), 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, United States Code) from departing from the territory of the United States if a parent or legal guardian of such child presents a court order from a court of competent jurisdiction prohibiting the removal of such child from the United States to a CBP Officer in sufficient time to prevent such departure for the duration of such 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 within 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.

SEC. 434. [6 U.S.C. 242] DEPARTMENT OF HOMELAND SECURITY BLUE CAMPAIGN.

(a) DEFINITION.—In this section, the term "human trafficking" means an act or practice described in paragraph (9) or (10) of section 103 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7102).

(b) ESTABLISHMENT.—There is established within the Department a program, which shall be known as the "Blue Campaign". The Blue Campaign shall be headed by a Director, who shall be appointed by the Secretary.

(c) PURPOSE.—The purpose of the Blue Campaign shall be to unify and coordinate Department efforts to address human trafficking.

(d) RESPONSIBILITIES.—The Secretary, working through the Director, shall, in accordance with subsection (e)—

(1) issue Department-wide guidance to appropriate Department personnel;

(2) develop training programs for such personnel;

(3) coordinate departmental efforts, including training for such personnel; and

(4) 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.

(e) 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—

(1) programs to help identify instances of human trafficking;

(2) 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;

(3) systematic and routine information sharing within the Department and among Federal, State, tribal, and local law enforcement agencies regarding—

(A) individuals suspected or convicted of human trafficking; and

(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—

(A) train employees of the Transportation Security Administration to 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) developing and utilizing, in consultation with the Blue Campaign Advisory Board established pursuant to subsection (g), 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) leveraging 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.

(f) 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 the date of the enactment of this subsection such training opportunities shall be made available to the following individuals:

(1) Federal, State, local, Tribal, and territorial law enforcement officers.

(2) Non-Federal correction system personnel.

(3) Such other individuals as the Director determines appropriate.

(g) BLUE CAMPAIGN ADVISORY BOARD.—

(1) IN GENERAL.—There is established in the Department a Blue Campaign Advisory Board, which shall be comprised of representatives assigned by the Secretary from—

(A) the Office for Civil Rights and Civil Liberties of the Department;

(B) the Privacy Office of the Department; and

(C) not fewer than four other separate components or offices of the Department.

(2) CHARTER.—The Secretary is authorized to issue a charter for the Blue Campaign Advisory Board, and such charter shall specify the following:

(A) The Board's mission, goals, and scope of its activities.

(B) The duties of the Board's representatives.

(C) The frequency of the Board's meetings.

(3) CONSULTATION.—The Director shall consult the Blue Campaign Advisory Board and, as appropriate, experts from other components and offices of the Center for Countering Human Trafficking of the Department regarding the following:

(A) Recruitment tactics used by human traffickers to inform the development of training and materials by the Blue Campaign.

(B) The development of effective awareness tools for distribution to Federal and non-Federal officials to identify and prevent instances of human trafficking.

(C) Identification of additional persons or entities that may be uniquely positioned to recognize signs of human trafficking and the development of materials for such persons.

(h) CONSULTATION.—With regard to the development of programs under the Blue Campaign and the implementation of such programs, the Director is authorized to consult with State, local, Tribal, and territorial agencies, non-governmental organizations, private sector organizations, and experts.

SEC. 435. [6 U.S.C. 243] MARITIME OPERATIONS COORDINATION PLAN.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of the Maritime Security Improvement Act of 2018, and biennially thereafter, the Secretary shall—

(1) update the Maritime Operations Coordination 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 within the context of other national and Department maritime security strategic guidance and how that work fits with the Maritime Operations Coordination Plan.

SEC. 436. [6 U.S.C. 244] MARITIME SECURITY CAPABILITIES ASSESSMENTS.

Not later than 180 days after the date of enactment of the Maritime Security Improvement Act of 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 Representatives, 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 1092 of the National Defense Authorization Act for Fiscal Year 2017 (6 U.S.C. 223).

Subtitle D—Immigration Enforcement Functions

SEC. 441. [6 U.S.C. 251] TRANSFER OF FUNCTIONS.

In accordance with title XV (relating to transition provisions), there shall be transferred from the Commissioner of Immigration and Naturalization to the Secretary all functions performed under the following programs, and all personnel, assets, and liabilities pertaining to such programs, immediately before such transfer occurs:

(1) The Border Patrol program.
(2) The detention and removal program.
(3) The intelligence program.
(4) The investigations program.
(5) The inspections program.

SEC. 442. [6 U.S.C. 252] ESTABLISHMENT OF BUREAU OF BORDER SECURITY.

(a) ESTABLISHMENT OF BUREAU.—

(1) IN GENERAL.—There shall be in the Department of Homeland Security a bureau to be known as the "Bureau of Border Security".

(2) ASSISTANT SECRETARY.—The head of the Bureau of Border Security shall be the Assistant Secretary of the Bureau of Border Security, who—

(A) shall report directly to the Under Secretary for Border and Transportation Security; and

(B) shall have a minimum of 5 years professional experience in law enforcement, and a minimum of 5 years of management experience.

(3) FUNCTIONS.—The Assistant Secretary of the Bureau of Border Security—

(A) shall establish the policies for performing such functions as are—

(i) transferred to the Under Secretary for Border and Transportation Security by section 441 and delegated to the Assistant Secretary by the Under Secretary for Border and Transportation Security; or

(ii) otherwise vested in the Assistant Secretary by law;

(B) shall oversee the administration of such policies; and

(C) shall advise the Under Secretary for Border and Transportation Security with respect to any policy or operation of the Bureau of Border Security that may affect the Bureau of Citizenship and Immigration Services established under subtitle E, including potentially conflicting policies or operations.

(4) PROGRAM TO COLLECT INFORMATION RELATING TO FOREIGN STUDENTS.—The Assistant Secretary of the Bureau of Border Security shall be 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 such information to carry out the enforcement functions of the Bureau.

(5) MANAGERIAL ROTATION PROGRAM.—

(A) IN GENERAL.—Not later than 1 year after the date on which the transfer of functions specified under section 441 takes effect, the Assistant Secretary of the Bureau of Border Security shall design and implement a managerial rotation program under which employees of such bureau holding positions involving supervisory or managerial responsibility and classified, in accordance with chapter 51 of title 5, United States Code, as a GS–14 or above, shall—

(i) gain some experience in all the major functions performed by such bureau; and

(ii) work in at least one local office of such bureau.

(B) REPORT.—Not later than 2 years after the date on which the transfer of functions specified under section 441 takes effect, the Secretary shall submit a report to the Congress on the implementation of such program.

(b) CHIEF OF POLICY AND STRATEGY.—

(1) IN GENERAL.—There shall be a position of Chief of Policy and Strategy for the Bureau of Border Security.

(2) FUNCTIONS.—In consultation with Bureau of Border Security personnel in local offices, the Chief of Policy and Strategy shall be 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 the Bureau of Citizenship and Immigration Services (established under subtitle E), as appropriate.

(c) LEGAL ADVISOR.—There shall be a principal legal advisor to the Assistant Secretary of the Bureau of Border Security. The legal advisor shall provide specialized legal advice to the Assistant Secretary of the Bureau of Border Security and shall represent the bureau in all exclusion, deportation, and removal proceedings before the Executive Office for Immigration Review.

SEC. 443. [6 U.S.C. 253] PROFESSIONAL RESPONSIBILITY AND QUALITY REVIEW.

The Secretary shall be responsible for—

(1) conducting investigations of noncriminal allegations of misconduct, corruption, and fraud involving any 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 such bureau as a whole and each of its components; and

(3) providing an analysis of the management of U.S. Immigration and Customs Enforcement.

SEC. 444. [6 U.S.C. 254] EMPLOYEE DISCIPLINE.

Notwithstanding any other provision of law, the Secretary may impose disciplinary action on any 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.

SEC. 445. [6 U.S.C. 255] REPORT ON IMPROVING ENFORCEMENT FUNCTIONS.

(a) IN GENERAL.—The Secretary, not later than 1 year after being sworn into office, shall submit to the Committees on Appropriations and the Judiciary of the House of Representatives and of the Senate a report with a plan detailing how the Bureau of Border Security, after the transfer of functions specified under section 441 takes effect, will enforce comprehensively, effectively, and fairly all the enforcement provisions of the Immigration and Nationality Act (8 U.S.C. 1101 et seq.) relating to such functions.

(b) CONSULTATION.—In carrying out subsection (a), the Secretary of Homeland Security shall consult with the Attorney General, the Secretary of State, the Director of the Federal Bureau of Investigation, the Secretary of the Treasury, the Secretary of Labor, the Commissioner of Social Security, the Director of the Ex-

ecutive Office for Immigration Review, and the heads of State and local law enforcement agencies to determine how to most effectively conduct enforcement operations.

SEC. 446. [6 U.S.C. 256] SENSE OF CONGRESS REGARDING CONSTRUCTION OF FENCING NEAR SAN DIEGO, CALIFORNIA.

It is the sense of the Congress that completing the 14-mile border fence project required to be carried out under section 102(b) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1103 note) should be a priority for the Secretary.

Subtitle E—Citizenship and Immigration Services

SEC. 451. [6 U.S.C. 271] ESTABLISHMENT OF BUREAU OF CITIZENSHIP AND IMMIGRATION SERVICES.

(a) ESTABLISHMENT OF BUREAU.—

(1) IN GENERAL.—There shall be in the Department a bureau to be known as the "Bureau of Citizenship and Immigration Services".

(2) DIRECTOR.—The head of the Bureau of Citizenship and Immigration Services shall be the Director of the Bureau of Citizenship and Immigration Services, who—

(A) shall report directly to the Deputy Secretary;

(B) shall have a minimum of 5 years of management experience; and

(C) shall be paid at the same level as the Assistant Secretary of the Bureau of Border Security.

(3) FUNCTIONS.—The Director of the Bureau of Citizenship and Immigration Services—

(A) shall establish the policies for performing such functions as are transferred to the Director by this section or this Act or otherwise vested in the Director by law;

(B) shall oversee the administration of such policies;

(C) shall advise the Deputy Secretary with respect to any policy or operation of the Bureau of Citizenship and Immigration Services that may affect the Bureau of Border Security of the Department, 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 452 to correct serious service problems identified by the Ombudsman; and

(F) shall establish procedures requiring a formal response to any recommendations submitted in the Ombudsman's annual report to Congress within 3 months after its submission to Congress.

(4) MANAGERIAL ROTATION PROGRAM.—

(A) IN GENERAL.—Not later than 1 year after the effective date specified in section 455, the Director of the Bureau of Citizenship and Immigration Services shall design and implement a managerial rotation program under which employees of such bureau holding positions involv-

ing supervisory or managerial responsibility and classified, in accordance with chapter 51 of title 5, United States Code, as a GS–14 or above, shall—

(i) gain some experience in all the major functions performed by such bureau; and

(ii) work in at least one field office and one service center of such bureau.

(B) REPORT.—Not later than 2 years after the effective date specified in section 455, the Secretary shall submit a report to Congress on the implementation of such program.

(5) PILOT INITIATIVES FOR BACKLOG ELIMINATION.—The Director of the Bureau of Citizenship and Immigration Services is authorized to implement innovative pilot initiatives to eliminate any remaining backlog in the processing of immigration benefit applications, and to prevent any backlog in the processing of such applications from recurring, in accordance with section 204(a) of the Immigration Services and Infrastructure Improvements Act of 2000 (8 U.S.C. 1573(a)). Such initiatives may include measures such as increasing personnel, transferring personnel to focus on areas with the largest potential for backlog, and streamlining paperwork.

(b) TRANSFER OF FUNCTIONS FROM COMMISSIONER.—In accordance with title XV (relating to transition provisions), there are transferred from the Commissioner of Immigration and Naturalization to the Director of the Bureau of Citizenship and Immigration Services the following functions, and all personnel, infrastructure, and funding provided to the Commissioner in support of such functions immediately before the effective date specified in section 455:

(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 the effective date specified in section 455.

(c) CHIEF OF POLICY AND STRATEGY.—

(1) IN GENERAL.—There shall be a position of Chief of Policy and Strategy for the Bureau of Citizenship and Immigration Services.

(2) FUNCTIONS.—In consultation with Bureau of Citizenship and Immigration Services personnel in field offices, the Chief of Policy and Strategy shall be 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 the Bureau of Border Security of the Department.

(d) LEGAL ADVISOR.—

(1) IN GENERAL.—There shall be a principal legal advisor to the Director of the Bureau of Citizenship and Immigration Services.

(2) FUNCTIONS.—The legal advisor shall be responsible for—

(A) providing specialized legal advice, opinions, determinations, regulations, and any other assistance to the Director of the Bureau of Citizenship and Immigration Services with respect to legal matters affecting the Bureau of Citizenship and Immigration Services; and

(B) representing the Bureau of Citizenship and Immigration Services in visa petition appeal proceedings before the Executive Office for Immigration Review.

(e) BUDGET OFFICER.—

(1) IN GENERAL.—There shall be a Budget Officer for the Bureau of Citizenship and Immigration Services.

(2) FUNCTIONS.—

(A) IN GENERAL.—The Budget Officer shall be responsible for—

(i) formulating and executing the budget of the Bureau of Citizenship and Immigration Services;

(ii) financial management of the Bureau of Citizenship and Immigration Services; and

(iii) collecting all payments, fines, and other debts for the Bureau of Citizenship and Immigration Services.

(f) CHIEF OF OFFICE OF CITIZENSHIP.—

(1) IN GENERAL.—There shall be a position of Chief of the Office of Citizenship for the Bureau of Citizenship and Immigration Services.

(2) FUNCTIONS.—The Chief of the Office of Citizenship for the Bureau of Citizenship and Immigration Services shall be 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.

SEC. 452. [6 U.S.C. 272] CITIZENSHIP AND IMMIGRATION SERVICES OMBUDSMAN.

(a) IN GENERAL.—Within the Department, there shall be a position of Citizenship and Immigration Services Ombudsman (in this section referred to as the "Ombudsman"). The Ombudsman shall report directly to the Deputy Secretary. The Ombudsman shall have a background in customer service as well as immigration law.

(b) FUNCTIONS.—It shall be the function of the Ombudsman—

(1) to assist individuals and employers in resolving problems with the Bureau of Citizenship and Immigration Services;

(2) to identify areas in which individuals and employers have problems in dealing with the Bureau of Citizenship and Immigration Services; and

(3) to the extent possible, to propose changes in the administrative practices of the Bureau of Citizenship and Immigration Services to mitigate problems identified under paragraph (2).

(c) ANNUAL REPORTS.—

(1) OBJECTIVES.—Not later than June 30 of each calendar year, the Ombudsman shall report to the Committee 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 such calendar year. Any such 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 services and responsiveness of the Bureau of 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 such 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 such 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 such 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 such inventory, the reasons for the inaction, and shall identify any official of the Bureau of Citizenship and Immigration Services who is responsible for such inaction;

(F) shall contain recommendations for such administrative action as may be 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 such other information as the Ombudsman may deem advisable.

(2) REPORT TO BE SUBMITTED DIRECTLY.—Each report required under this subsection shall be provided directly to the committees described in paragraph (1) without any prior comment or amendment from the Secretary, Deputy Secretary, Director of the Bureau of Citizenship and Immigration Services, or any other 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 the Bureau of 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 the Bureau of Citizenship and Immigration Services to identify serious service problems and to present recommendations for such administrative action as may be appropriate to resolve problems encountered by individuals and employers.

(e) PERSONNEL ACTIONS.—

(1) IN GENERAL.—The Ombudsman shall have the responsibility and authority—

(A) to appoint local ombudsmen and make available at least 1 such ombudsman for each State; and

(B) to evaluate and take personnel actions (including dismissal) with respect to any employee of any local office of the Ombudsman.

(2) CONSULTATION.—The Ombudsman may consult with the appropriate supervisory personnel of the Bureau of Citizenship and Immigration Services in carrying out the Ombudsman's responsibilities under this subsection.

(f) RESPONSIBILITIES OF BUREAU OF CITIZENSHIP AND IMMIGRATION SERVICES.—The Director of the Bureau of Citizenship and Immigration Services shall establish procedures requiring a formal response to all recommendations submitted to such director by the Ombudsman within 3 months after submission to such director.

(g) OPERATION OF LOCAL OFFICES.—

(1) IN GENERAL.—Each local ombudsman—

(A) shall report to the Ombudsman or the delegate thereof;

(B) may consult with the appropriate supervisory personnel of the Bureau of Citizenship and Immigration Services regarding the daily operation of the local office of such ombudsman;

(C) shall, at the initial meeting with any individual or employer seeking the assistance of such local office, notify such 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 the Bureau of Citizenship and Immigration Services contact with, or information provided by, such 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 the Bureau of Citizenship and Immigration Services, or any component of the Bureau of Citizenship and Immigration Services.

SEC. 453. [6 U.S.C. 273] PROFESSIONAL RESPONSIBILITY AND QUALITY REVIEW.

(a) IN GENERAL.—The Director of the Bureau of Citizenship and Immigration Services shall be responsible for—

(1) conducting investigations of noncriminal allegations of misconduct, corruption, and fraud involving any employee of the Bureau of Citizenship and Immigration Services that are not subject to investigation by the Inspector General for the Department;

(2) inspecting the operations of the Bureau of Citizenship and Immigration Services and providing assessments of the quality of the operations of such bureau as a whole and each of its components; and

(3) providing an analysis of the management of the Bureau of Citizenship and Immigration Services.

(b) SPECIAL CONSIDERATIONS.—In providing assessments in accordance with subsection (a)(2) with respect to a decision of the Bureau of 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) any fraud or misrepresentation associated with the decision; and

(3) the efficiency with which the decision was rendered.

SEC. 454. [6 U.S.C. 274] EMPLOYEE DISCIPLINE.

The Director of the Bureau of Citizenship and Immigration Services may, notwithstanding any other provision of law, impose disciplinary action, including termination of employment, pursuant to policies and procedures applicable to employees of the Federal Bureau of Investigation, on any employee of the Bureau of Citizenship and Immigration Services who willfully deceives Congress or agency leadership on any matter.

SEC. 455. [6 U.S.C. 271 note] EFFECTIVE DATE.

Notwithstanding section 4, sections 451 through 456, and the amendments made by such sections, shall take effect on the date on which the transfer of functions specified under section 441 takes effect.

SEC. 456. [6 U.S.C. 275] TRANSITION.

(a) REFERENCES.—With respect to any function transferred by this subtitle to, and exercised on or after the effective date specified in section 455 by, the Director of the Bureau of Citizenship and Immigration Services, any reference in any other Federal law, Executive order, rule, regulation, or delegation of authority, or any document of or pertaining to a component of government from which such function is transferred—

(1) to the head of such component is deemed to refer to the Director of the Bureau of Citizenship and Immigration Services; or

(2) to such component is deemed to refer to the Bureau of Citizenship and Immigration Services.

(b) OTHER TRANSITION ISSUES.—

(1) EXERCISE OF AUTHORITIES.—Except as otherwise provided by law, a Federal official to whom a function is transferred by this subtitle 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 the effective date specified in section 455.

(2) TRANSFER AND ALLOCATION OF APPROPRIATIONS AND PERSONNEL.—The personnel of the Department of Justice employed in connection with the functions transferred by this subtitle (and functions that the Secretary determines are properly related to the functions of the Bureau of Citizenship and Immigration Services), and the assets, liabilities, contracts, property, records, and unexpended balance of appropriations, au-

thorizations, allocations, and other funds employed, held, used, arising from, available to, or to be made available to, the Immigration and Naturalization Service in connection with the functions transferred by this subtitle, subject to section 202 of the Budget and Accounting Procedures Act of 1950, shall be transferred to the Director of the Bureau of Citizenship and Immigration Services for allocation to the appropriate component of the Department. Unexpended funds transferred pursuant to this paragraph shall be used only for the purposes for which the funds were originally authorized and appropriated. The Secretary shall have the right to adjust or realign transfers of funds and personnel effected pursuant to this subtitle for a period of 2 years after the effective date specified in section 455.

* * * * * * *

SEC. 459. [6 U.S.C. 276] REPORT ON IMPROVING IMMIGRATION SERVICES.

(a) IN GENERAL.—The Secretary, not later than 1 year after the effective date of this Act, shall submit to the Committees on the Judiciary and Appropriations of the House of Representatives and of the Senate a report with a plan detailing how the Bureau of Citizenship and Immigration Services, after the transfer of functions specified in this subtitle takes effect, will complete efficiently, fairly, and within a reasonable time, the adjudications described in paragraphs (1) through (5) of section 451(b).

(b) CONTENTS.—For each type of adjudication to be undertaken by the Director of the Bureau of Citizenship and Immigration Services, the report shall include the following:

(1) Any potential savings of resources that may be implemented without affecting the quality of the adjudication.

(2) The goal for processing time with respect to the application.

(3) Any statutory modifications with respect to the adjudication that the Secretary considers advisable.

(c) CONSULTATION.—In carrying out subsection (a), the Secretary shall consult with the Secretary of State, the Secretary of Labor, the Assistant Secretary of the Bureau of Border Security of the Department, and the Director of the Executive Office for Immigration Review to determine how to streamline and improve the process for applying for and making adjudications described in section 451(b) and related processes.

SEC. 460. [6 U.S.C. 277] REPORT ON RESPONDING TO FLUCTUATING NEEDS.

Not later than 30 days after the date of the enactment of this Act, the Attorney General shall submit to Congress a report on changes in law, including changes in authorizations of appropriations and in appropriations, that are needed to permit the Immigration and Naturalization Service, and, after the transfer of functions specified in this subtitle takes effect, the Bureau of Citizenship and Immigration Services of the Department, to ensure a prompt and timely response to emergent, unforeseen, or impending changes in the number of applications for immigration benefits, and otherwise to ensure the accommodation of changing immigration service needs.

SEC. 461. [6 U.S.C. 278] APPLICATION OF INTERNET-BASED TECHNOLOGIES.

(a) ESTABLISHMENT OF TRACKING SYSTEM.—The Secretary, not later than 1 year after the effective date of this Act, 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 any 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 the Immigration and Naturalization Service relating to the immigration services and processing of filings related to immigrant services. The study shall also include an estimate of the timeframe and cost and shall consider other factors in implementing such a 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 1 year after the effective date of this Act.

(c) TECHNOLOGY ADVISORY COMMITTEE.—

(1) ESTABLISHMENT.—The Secretary shall establish, not later than 60 days after the effective date of this Act, an advisory committee (in this section referred to as 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).

The Technology Advisory Committee shall be established after consultation with the Committees on the Judiciary of the House of Representatives and the Senate.

(2) COMPOSITION.—The Technology Advisory Committee shall be composed of representatives from high technology companies capable of establishing and implementing the system 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).

SEC. 462. [6 U.S.C. 279] CHILDREN'S AFFAIRS.

(a) TRANSFER OF FUNCTIONS.—There are transferred to the Director of the Office of Refugee Resettlement of the Department of Health and Human Services functions under the immigration laws of the United States with respect to the care of unaccompanied alien children that were vested by statute in, or performed by, the Commissioner of Immigration and Naturalization (or any officer, employee, or component of the Immigration and Naturalization Service) immediately before the effective date specified in subsection (d).

(b) FUNCTIONS.—

(1) IN GENERAL.—Pursuant to the transfer made by subsection (a), the Director of the Office of Refugee Resettlement shall be responsible for—

(A) coordinating and implementing the care and placement of unaccompanied alien children who are in Federal custody by reason of their immigration status, including developing a plan to be submitted to Congress on how to ensure that qualified and independent legal counsel is timely appointed to represent the interests of each such child, consistent with the law regarding appointment of counsel that is in effect on the date of the enactment of this Act;

(B) ensuring that the interests of the child are considered in decisions and actions relating to the care and custody of an unaccompanied alien child;

(C) making placement determinations for all unaccompanied alien children who are in Federal custody by reason of their immigration status;

(D) implementing the placement determinations;

(E) implementing policies with respect to the care and placement of unaccompanied alien children;

(F) identifying a sufficient number of qualified individuals, entities, and facilities to house unaccompanied alien children;

(G) overseeing the infrastructure and personnel of facilities in which unaccompanied alien children reside;

(H) reuniting unaccompanied alien children with a parent abroad in appropriate cases;

(I) compiling, updating, and publishing at least annually a state-by-state list of professionals or other entities qualified to provide guardian and attorney representation services for unaccompanied alien children;

(J) maintaining statistical information and other data on unaccompanied alien children for whose care and placement the Director is responsible, which shall include—

(i) biographical information, such as a child's name, gender, date of birth, country of birth, and country of habitual residence;

(ii) the date on which the child came into Federal custody by reason of his or her immigration status;

(iii) information relating to the child's placement, removal, or release from each facility in which the child has resided;

(iv) in any case in which the child is placed in detention or released, an explanation relating to the detention or release; and

(v) the disposition of any actions in which the child is the subject;

(K) collecting and compiling statistical information from the Department of Justice, the Department of Homeland Security, and the Department of State on each department's actions relating to unaccompanied alien children; and

(L) conducting investigations and inspections of facilities and other entities in which unaccompanied alien children reside, including regular follow-up visits to such facilities, placements, and other entities, to assess the continued suitability of such placements.

(2) COORDINATION WITH OTHER ENTITIES; NO RELEASE ON OWN RECOGNIZANCE.—In making determinations described in paragraph (1)(C), the Director of the Office of Refugee Resettlement—

(A) shall consult with appropriate juvenile justice professionals, the Director of the Bureau of Citizenship and Immigration Services, and the Assistant Secretary of the Bureau of Border Security to ensure that such determinations ensure that unaccompanied alien children described in such subparagraph—

(i) are likely to appear for all hearings or proceedings in which they are involved;

(ii) are protected from smugglers, traffickers, or others who might seek to victimize or otherwise engage them in criminal, harmful, or exploitive activity; and

(iii) are placed in a setting in which they are not likely to pose a danger to themselves or others; and

(B) shall not release such children upon their own recognizance.

(3) DUTIES WITH RESPECT TO FOSTER CARE.—In carrying out the duties described in paragraph (1), the Director of the Office of Refugee Resettlement is encouraged to use the refugee children foster care system established pursuant to section 412(d) of the Immigration and Nationality Act (8 U.S.C. 1522(d)) for the placement of unaccompanied alien children.

(4) RULE OF CONSTRUCTION.—Nothing in paragraph (2)(B) may be construed to require that a bond be posted for an unaccompanied alien child who is released to a qualified sponsor.

(c) RULE OF CONSTRUCTION.—Nothing in this section may be construed to transfer the responsibility for adjudicating benefit determinations under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.) from the authority of any official of the Department of Justice, the Department of Homeland Security, or the Department of State.

(d) EFFECTIVE DATE.—Notwithstanding section 4, this section shall take effect on the date on which the transfer of functions specified under section 441 takes effect.

(e) REFERENCES.—With respect to any function transferred by this section, any reference in any other Federal law, Executive order, rule, regulation, or delegation of authority, or any document of or pertaining to a component of government from which such function is transferred—

(1) to the head of such component is deemed to refer to the Director of the Office of Refugee Resettlement; or

(2) to such component is deemed to refer to the Office of Refugee Resettlement of the Department of Health and Human Services.

(f) OTHER TRANSITION ISSUES.—

(1) EXERCISE OF AUTHORITIES.—Except as otherwise provided by law, a Federal official to whom a function is transferred by this section 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 the effective date specified in subsection (d).

(2) SAVINGS PROVISIONS.—Subsections (a), (b), and (c) of section 1512 shall apply to a transfer of functions under this section in the same manner as such provisions apply to a transfer of functions under this Act to the Department of Homeland Security.

(3) TRANSFER AND ALLOCATION OF APPROPRIATIONS AND PERSONNEL.—The personnel of the Department of Justice employed in connection with the functions transferred by this section, and the assets, liabilities, contracts, property, records, and unexpended balance of appropriations, authorizations, allocations, and other funds employed, held, used, arising from, available to, or to be made available to, the Immigration and Naturalization Service in connection with the functions transferred by this section, subject to section 202 of the Budget and Accounting Procedures Act of 1950, shall be transferred to the Director of the Office of Refugee Resettlement for allocation to the appropriate component of the Department of Health and Human Services. Unexpended funds transferred pursuant to this paragraph shall be used only for the purposes for which the funds were originally authorized and appropriated.

(g) DEFINITIONS.—As used in this section—

(1) the term "placement" means the placement of an unaccompanied alien child in either a detention facility or an alternative to such a facility; and

(2) the term "unaccompanied alien child" means a child who—

(A) has no lawful immigration status in the United States;

(B) has not attained 18 years of age; and

(C) with respect to whom—

(i) there is no parent or legal guardian in the United States; or

(ii) no parent or legal guardian in the United States is available to provide care and physical custody.

Subtitle F—General Immigration Provisions

SEC. 471. [6 U.S.C. 291] ABOLISHMENT OF INS.

(a) IN GENERAL.—Upon completion of all transfers from the Immigration and Naturalization Service as provided for by this Act, the Immigration and Naturalization Service of the Department of Justice is abolished.

(b) PROHIBITION.—The authority provided by section 1502 may be used to reorganize functions or organizational units within the Bureau of Border Security or the Bureau of Citizenship and Immigration Services, but may not be used to recombine the two bureaus into a single agency or otherwise to combine, join, or consolidate functions or organizational units of the two bureaus with each other.

SEC. 472. [6 U.S.C. 292] VOLUNTARY SEPARATION INCENTIVE PAYMENTS.

(a) DEFINITIONS.—For purposes of this section—

(1) the term "employee" means an employee (as defined by section 2105 of title 5, United States Code) who—

(A) has completed at least 3 years of current continuous service with 1 or more covered entities; and

(B) is serving under an appointment without time limitation,

but does not include any person under subparagraphs (A)–(G) of section 663(a)(2) of Public Law 104–208 (5 U.S.C. 5597 note);

(2) the term "covered entity" means—

(A) the Immigration and Naturalization Service;

(B) the Bureau of Border Security of the Department of Homeland Security; and

(C) the Bureau of Citizenship and Immigration Services of the Department of Homeland Security; and

(3) the term "transfer date" means the date on which the transfer of functions specified under section 441 takes effect.

(b) STRATEGIC RESTRUCTURING PLAN.—Before the Attorney General or the Secretary obligates any resources for voluntary separation incentive payments under this section, such official shall submit to the appropriate committees of Congress a strategic restructuring plan, which shall include—

(1) an organizational chart depicting the covered entities after their restructuring pursuant to this Act;

(2) a summary description of how the authority under this section will be used to help carry out that restructuring; and

(3) the information specified in section 663(b)(2) of Public Law 104–208 (5 U.S.C. 5597 note).

As used in the preceding sentence, the "appropriate committees of Congress" are the Committees on Appropriations, Government Reform, and the Judiciary of the House of Representatives, and the Committees on Appropriations, Governmental Affairs, and the Judiciary of the Senate.

(c) AUTHORITY.—The Attorney General and the Secretary may, to the extent necessary to help carry out their respective strategic restructuring plan described in subsection (b), make voluntary separation incentive payments to employees. Any such payment—

(1) shall be paid to the employee, in a lump sum, after the employee has separated from service;

(2) shall be paid from appropriations or funds available for the payment of basic pay of the employee;

(3) shall be equal to the lesser of—

(A) the amount the employee would be entitled to receive under section 5595(c) of title 5, United States Code; or

(B) an amount not to exceed $25,000, as determined by the Attorney General or the Secretary;

(4) may not be made except in the case of any qualifying employee who voluntarily separates (whether by retirement or resignation) before the end of—

(A) the 3-month period beginning on the date on which such payment is offered or made available to such employee; or

(B) the 3-year period beginning on the date of the enactment of this Act,

whichever occurs first;

(5) shall not be a basis for payment, and shall not be included in the computation, of any other type of Government benefit; and

(6) shall not be taken into account in determining the amount of any severance pay to which the employee may be entitled under section 5595 of title 5, United States Code, based on any other separation.

(d) ADDITIONAL AGENCY CONTRIBUTIONS TO THE RETIREMENT FUND.—

(1) IN GENERAL.—In addition to any payments which it is otherwise required to make, the Department of Justice and the Department of Homeland Security shall, for each fiscal year with respect to which it makes any voluntary separation incentive payments under this section, remit to the Office of Personnel Management for deposit in the Treasury of the United States to the credit of the Civil Service Retirement and Disability Fund the amount required under paragraph (2).

(2) AMOUNT REQUIRED.—The amount required under this paragraph shall, for any fiscal year, be the amount under subparagraph (A) or (B), whichever is greater.

(A) FIRST METHOD.—The amount under this subparagraph shall, for any fiscal year, be equal to the minimum amount necessary to offset the additional costs to the retirement systems under title 5, United States Code (payable out of the Civil Service Retirement and Disability Fund) resulting from the voluntary separation of the employees described in paragraph (3), as determined under regulations of the Office of Personnel Management.

(B) SECOND METHOD.—The amount under this subparagraph shall, for any fiscal year, be equal to 45 percent of the sum total of the final basic pay of the employees described in paragraph (3).

(3) COMPUTATIONS TO BE BASED ON SEPARATIONS OCCURRING IN THE FISCAL YEAR INVOLVED.—The employees described in this paragraph are those employees who receive a voluntary separation incentive payment under this section based on their separating from service during the fiscal year with respect to which the payment under this subsection relates.

(4) FINAL BASIC PAY DEFINED.—In this subsection, the term "final basic pay" means, with respect to an employee, the total

amount of basic pay which would be payable for a year of service by such employee, computed using the employee's final rate of basic pay, and, if last serving on other than a full-time basis, with appropriate adjustment therefor.

(e) EFFECT OF SUBSEQUENT EMPLOYMENT WITH THE GOVERNMENT.—An individual who receives a voluntary separation incentive payment under this section and who, within 5 years after the date of the separation on which the payment is based, accepts any compensated employment with the Government or works for any agency of the Government through a personal services contract, shall be required to pay, prior to the individual's first day of employment, the entire amount of the incentive payment. Such payment shall be made to the covered entity from which the individual separated or, if made on or after the transfer date, to the Deputy Secretary or the Under Secretary for Border and Transportation Security (for transfer to the appropriate component of the Department of Homeland Security, if necessary).

(f) EFFECT ON EMPLOYMENT LEVELS.—

(1) INTENDED EFFECT.—Voluntary separations under this section are not intended to necessarily reduce the total number of full-time equivalent positions in any covered entity.

(2) USE OF VOLUNTARY SEPARATIONS.—A covered entity may redeploy or use the full-time equivalent positions vacated by voluntary separations under this section to make other positions available to more critical locations or more critical occupations.

SEC. 473. [6 U.S.C. 293] AUTHORITY TO CONDUCT A DEMONSTRATION PROJECT RELATING TO DISCIPLINARY ACTION.

(a) IN GENERAL.—The Attorney General and the Secretary may each, during a period ending not later than 5 years after the date of the enactment of this Act, conduct a demonstration project for the purpose of determining whether one or more changes in the policies or procedures relating to methods for disciplining employees would result in improved personnel management.

(b) SCOPE.—A demonstration project under this section—

(1) may not cover any employees apart from those employed in or under a covered entity; and

(2) shall not be limited by any provision of chapter 43, 75, or 77 of title 5, United States Code.

(c) PROCEDURES.—Under the demonstration project—

(1) the use of alternative means of dispute resolution (as defined in section 571 of title 5, United States Code) shall be encouraged, whenever appropriate; and

(2) each covered entity under the jurisdiction of the official conducting the project shall be required to provide for the expeditious, fair, and independent review of any action to which section 4303 or subchapter II of chapter 75 of such title 5 would otherwise apply (except an action described in section 7512(5) of such title 5).

(d) ACTIONS INVOLVING DISCRIMINATION.—Notwithstanding any other provision of this section, if, in the case of any matter described in section 7702(a)(1)(B) of title 5, United States Code, there is no judicially reviewable action under the demonstration project within 120 days after the filing of an appeal or other formal re-

quest for review (referred to in subsection (c)(2)), an employee shall be entitled to file a civil action to the same extent and in the same manner as provided in section 7702(e)(1) of such title 5 (in the matter following subparagraph (C) thereof).

(e) CERTAIN EMPLOYEES.—Employees shall not be included within any project under this section if such employees are—

(1) neither managers nor supervisors; and

(2) within a unit with respect to which a labor organization is accorded exclusive recognition under chapter 71 of title 5, United States Code.

Notwithstanding the preceding sentence, an aggrieved employee within a unit (referred to in paragraph (2)) may elect to participate in a complaint procedure developed under the demonstration project in lieu of any negotiated grievance procedure and any statutory procedure (as such term is used in section 7121 of such title 5).

(f) REPORTS.—The General Accounting Office shall prepare and submit to the Committees on Government Reform and the Judiciary of the House of Representatives and the Committees on Governmental Affairs and the Judiciary of the Senate periodic reports on any demonstration project conducted under this section, such reports to be submitted after the second and fourth years of its operation. Upon request, the Attorney General or the Secretary shall furnish such information as the General Accounting Office may require to carry out this subsection.

(g) DEFINITION.—In this section, the term "covered entity" has the meaning given such term in section 472(a)(2).

SEC. 474. [6 U.S.C. 294] SENSE OF CONGRESS.

It is the sense of Congress that—

(1) the missions of the Bureau of Border Security and the Bureau of Citizenship and Immigration Services are equally important and, accordingly, they each should be adequately funded; and

(2) the functions transferred under this subtitle should not, after such transfers take effect, operate at levels below those in effect prior to the enactment of this Act.

SEC. 475. [6 U.S.C. 295] DIRECTOR OF SHARED SERVICES.

(a) IN GENERAL.—Within the Office of Deputy Secretary, there shall be a Director of Shared Services.

(b) FUNCTIONS.—The Director of Shared Services shall be responsible for the coordination of resources for the Bureau of Border Security and the Bureau of Citizenship and Immigration Services, including—

(1) information resources management, including computer databases and information technology;

(2) records and file management; and

(3) forms management.

SEC. 476. [6 U.S.C. 296] SEPARATION OF FUNDING.

(a) IN GENERAL.—There shall be established separate accounts in the Treasury of the United States for appropriated funds and other deposits available for the Bureau of Citizenship and Immigration Services and the Bureau of Border Security.

(b) SEPARATE BUDGETS.—To ensure that the Bureau of Citizenship and Immigration Services and the Bureau of Border Security 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 such entity.

(c) FEES.—Fees imposed for a particular service, application, or benefit shall be deposited into the account established under subsection (a) that is for the bureau with jurisdiction over the function to which the fee relates.

(d) FEES NOT TRANSFERABLE.—No fee may be transferred between the Bureau of Citizenship and Immigration Services and the Bureau of Border Security for purposes not authorized by section 286 of the Immigration and Nationality Act (8 U.S.C. 1356).

SEC. 477. [6 U.S.C. 297] REPORTS AND IMPLEMENTATION PLANS.

(a) DIVISION OF FUNDS.—The Secretary, not later than 120 days after the effective date of this Act, shall submit to the Committees on Appropriations and the Judiciary of the House of Representatives and of the Senate a report on the proposed division and transfer of funds, including unexpended funds, appropriations, and fees, between the Bureau of Citizenship and Immigration Services and the Bureau of Border Security.

(b) DIVISION OF PERSONNEL.—The Secretary, not later than 120 days after the effective date of this Act, shall submit to the Committees on Appropriations and the Judiciary of the House of Representatives and of the Senate a report on the proposed division of personnel between the Bureau of Citizenship and Immigration Services and the Bureau of Border Security.

(c) IMPLEMENTATION PLAN.—

(1) IN GENERAL.—The Secretary, not later than 120 days after the effective date of this Act, and every 6 months thereafter until the termination of fiscal year 2005, shall submit to the Committees on Appropriations and the Judiciary of the House of Representatives and of the Senate an implementation plan to carry out this Act.

(2) CONTENTS.—The implementation plan should include details concerning the separation of the Bureau of Citizenship and Immigration Services and the Bureau of Border Security, including the following:

(A) Organizational structure, including the field structure.

(B) Chain of command.

(C) Procedures for interaction among such bureaus.

(D) Fraud detection and investigation.

(E) The processing and handling of removal proceedings, including expedited removal and applications for relief from removal.

(F) Recommendations for conforming amendments to the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(G) Establishment of a transition team.

(H) Methods to phase in the costs of separating the administrative support systems of the Immigration and Naturalization Service in order to provide for separate admin-

istrative support systems for the Bureau of Citizenship and Immigration Services and the Bureau of Border Security.

(d) COMPTROLLER GENERAL STUDIES AND REPORTS.—

(1) STATUS REPORTS ON TRANSITION.—Not later than 18 months after the date on which the transfer of functions specified under section 441 takes effect, and every 6 months thereafter, until full implementation of this subtitle has been completed, the Comptroller General of the United States shall submit to the Committees on Appropriations and on the Judiciary of the House of Representatives and the Senate a report containing the following:

(A) A determination of whether the transfers of functions made by subtitles D and E have been completed, and if a transfer of functions has not taken place, identifying the reasons why the transfer has not taken place.

(B) If the transfers of functions made by subtitles D and E have been completed, an identification of any issues that have arisen due to the completed transfers.

(C) An identification of any issues that may arise due to any future transfer of functions.

(2) REPORT ON MANAGEMENT.—Not later than 4 years after the date on which the transfer of functions specified under section 441 takes effect, the Comptroller General of the United States shall submit to the Committees on Appropriations and on the Judiciary of the House of Representatives and the Senate a report, following a study, containing the following:

(A) Determinations of whether the transfer of functions from the Immigration and Naturalization Service to the Bureau of Citizenship and Immigration Services and the Bureau of Border Security have improved, with respect to each function transferred, the following:

(i) Operations.

(ii) Management, including accountability and communication.

(iii) Financial administration.

(iv) Recordkeeping, including information management and technology.

(B) A statement of the reasons for the determinations under subparagraph (A).

(C) Any recommendations for further improvements to the Bureau of Citizenship and Immigration Services and the Bureau of Border Security.

(3) REPORT ON FEES.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committees on the Judiciary of the House of Representatives and of the Senate a report examining whether the Bureau of Citizenship and Immigration Services is likely to derive sufficient funds from fees to carry out its functions in the absence of appropriated funds.

SEC. 478. [6 U.S.C. 298] IMMIGRATION FUNCTIONS.

(a) ANNUAL REPORT.—

(1) IN GENERAL.—One year after the date of the enactment of this Act, and each year thereafter, the Secretary shall submit a report to the President, to the Committees on the Judiciary and Government Reform of the House of Representatives, and to the Committees on the Judiciary and Government Affairs of the Senate, on the impact the transfers made by this subtitle has had on immigration functions.

(2) MATTER INCLUDED.—The report shall address the following with respect to the period covered by the report:

(A) The aggregate number of all immigration applications and petitions received, and processed, by the Department.

(B) 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.

(C) 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.

(D) The average processing period for immigration applications and petitions, disaggregated by application or petition type.

(E) The number and types of immigration-related grievances filed with any official of the Department of Justice, and if those grievances were resolved.

(F) Plans to address grievances and improve immigration services.

(G) Whether immigration-related fees were used consistent with legal requirements regarding such use.

(H) 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.

(b) SENSE OF CONGRESS REGARDING IMMIGRATION SERVICES.—It is the sense of Congress that—

(1) the quality and efficiency of immigration services rendered by the Federal Government should be improved after the transfers made by this subtitle take effect; and

(2) the Secretary should undertake efforts to guarantee that concerns regarding the quality and efficiency of immigration services are addressed after such effective date.

Subtitle G—U.S. Customs and Border Protection Public Private Partnerships

SEC. 481. [6 U.S.C. 301] 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, upon the

request of any entity, may enter into a fee agreement with such 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 or will provide such services;

(2) such 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 such services; and

(3) if space is provided by such entity, each facility at which U.S. Customs and Border Protection services are performed shall be maintained and equipped by such entity, without cost to the Federal Government, in accordance with U.S. Customs and Border Protection specifications.

(b) SERVICES DESCRIBED.—The services described in this subsection are any activities of any employee or Office of Field Operations contractor of U.S. Customs and Border Protection (except employees of the U.S. Border Patrol, as established under section 411(e)) pertaining to, or in support of, customs, agricultural processing, border security, or immigration inspection-related matters at a port of entry or any other facility at which U.S. Customs and Border Protection provides or will provide services.

(c) MODIFICATION OF PRIOR AGREEMENTS.—The Commissioner of U.S. Customs and Border Protection, at the request of an entity who has previously entered into an agreement with U.S. Customs and Border Protection for the reimbursement of fees in effect on the date of enactment of this section, may modify such agreement to implement any 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 any appropriations Act, or provided from any account in the Treasury of the United States derived by the collection of fees, to entities under this Act; and

(B) may not enter into a fee agreement under this section if such agreement would unduly and permanently impact services funded in any appropriations Act, or provided from any account in the Treasury of the United States, derived by the collection of fees.

(2) NUMBER.—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) FEE AGREEMENT.—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 Protec-

tion 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 five full-time equivalent U.S. Customs and Border Protection Officers beyond the number of such 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.—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 such 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 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 such services, including the salaries and expenses of employees and contractors of U.S. Customs and Border Protection, to provide such services and other costs incurred by U.S. Customs and Border Protection relating to such services, such as temporary

placement or permanent relocation of such 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 OF FEES.—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 such services, and a process for increasing such 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 such fees.

(i) DEPOSIT OF FUNDS.—

(1) ACCOUNT.—Funds collected pursuant to any 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 such 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 any such agreement and any other costs incurred or to be incurred by U.S. Customs and Border Protection relating to such services.

(2) RETURN OF UNUSED FUNDS.—The Commissioner of U.S. Customs and Border Protection shall return any unused funds collected and deposited into 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 such fee agreement change by mutual agreement to cause a reduction of U.S. Customs and Border Protections services. No interest shall be owed upon the return of any such 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 that a fee under subsection (h) is due, fails to pay such fee in a timely manner. If such 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.

(2) PENALTY.—Any entity that, after notice and demand for payment of any fee under subsection (h), fails to pay such fee in a timely manner shall be liable for a penalty or liquidated damage equal to two times the amount of such fee. Any such amount collected under this paragraph shall be deposited into the appropriate account specified under subsection (i) and shall be available as described in such subsection.

(3) TERMINATION BY THE ENTITY.—Any entity who has previously entered into an agreement with U.S. Customs and Border Protection for the reimbursement of fees in effect on the date of enactment of this section, or under the provisions of this section, may request that such agreement be amended to provide for termination upon advance notice, length, and terms that are negotiated between such 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 that represent the State or Congressional District in which the affected port of entry or facility is located of such 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.

SEC. 482. [6 U.S.C. 301a] PORT OF ENTRY DONATION AUTHORITY.

(a) PERSONAL PROPERTY DONATION AUTHORITY.—

(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 any 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 five years.

(2) LIMITATION ON MONETARY DONATIONS.—Any 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 411(g)(3), which 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 related to—

(A) furniture, fixtures, equipment, or technology, including the installation or deployment of such items; and

(B) the operation and maintenance of such furniture, fixtures, equipment, or technology.

(b) REAL PROPERTY DONATION AUTHORITY.—

(1) IN GENERAL.—Subject to paragraph (3), the Commissioner of U.S. Customs and Border Protection, and the Administrator of General Services [4], as applicable, may enter into an agreement with any 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 of donations with respect to the land port of entry total $75,000,000 or less over the preceding five years.

(2) USE.—Donations accepted pursuant to this subsection may be used for activities of the Office of Field Operations set forth in section 411(g), which 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 a Federal Government-owned land port of entry described in paragraph (1), including expenses related to—

(A) land acquisition, design, construction, repair, or alteration; and

[4] Section 6410(2)(A) of division F of Public Law 117–81 provides for an amendment to strike "Administrator of the General Services Administration" and insert "Administrator of General Services" in the matter preceding paragraph (1). Such amendment should have been made to paragraph (1) in the matter preceding subparagraph (A); however, it was carried out according to the probable intent of Congress.

(B) operation and maintenance of such 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 such termination date.

(c) GENERAL PROVISIONS.—

(1) DURATION.—An agreement entered into under subsection (a) or (b) (and, in the case of such subsection (b), in accordance with paragraph (4) of such subsection) may last as long as required to meet the terms of such 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 any such 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 such criteria publicly available.

(B) CONSIDERATIONS.—Criteria established pursuant to subparagraph (A) shall consider—

(i) the impact of a proposal referred to in such subparagraph 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) such proposal's potential to increase trade and travel efficiency through added capacity;

(iii) such 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 that port of entry or facility and other ports of entry on the same border;

(v) for a donation under subsection (b)—

(I) whether such donation satisfies the requirements of such proposal, or whether additional real property would be required; and

(II) how such donation was acquired, including if eminent domain was used;

(vi) the funding available to complete the intended use of such donation;

(vii) the costs of maintaining and operating such donation;

(viii) the impact of such proposal on U.S. Customs and Border Protection staffing requirements; and

(ix) other factors that the Commissioner or Administrator 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 such entity as to whether such 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 such 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 PROPOSALS.—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. Customs and Border Protection, with the concurrence of the Administrator of General Services, as applicable, shall—

(I) determine whether to approve or deny such proposal; and

(II) notify the entity that submitted such proposal of such determination.

(4) SUPPLEMENTAL FUNDING.—Except as required under section 3307 of title 40, United States Code, real property donations to the Administrator of General Services made pursuant to subsection (a) and (b) at a GSA-owned land port of entry may be used in addition to any other funding for such purpose, 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 any donation made pursuant to subsection (a) or (b). No interest shall be owed to the donor with respect to any donation provided under such subsections 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 either of such subsections, obligate or expend amounts in excess of amounts that have been appropriated pursuant to any appropriations Act for purposes specified in either of such subsections or otherwise made available for any of such 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 [5]

(i) the donation will not be used for the construction of a detention facility or a border fence or wall; and

(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) ANNUAL REPORTS.—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;

[5] A missing em dash after "paragraph (7) that" is so in law. See amendment made by section 6410(3) of division F of Public Law 117–81.

(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) GAO REPORT.—The Comptroller General of the United States shall submit an biennial report to the congressional committees referred to in subsection (c)(7) that evaluates—

(1) fee agreements entered into pursuant to section 481;

(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 such 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 and the Administrator 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.

SEC. 483. [6 U.S.C. 301b] CURRENT AND PROPOSED AGREEMENTS.

Nothing in this subtitle or in section 4 of the Cross-Border Trade Enhancement Act of 2016 may be construed as affecting—

(1) any agreement entered into pursuant to section 560 of division D of the Consolidated and Further Continuing Appropriations Act, 2013 (Public Law 113–6) or section 559 of title V of division F of the Consolidated Appropriations Act, 2014 (6 U.S.C. 211 note; Public Law 113–76), as in existence on the day before the date of the enactment of this subtitle, and any such agreement shall continue to have full force and effect on and after such date; or

(2) a proposal accepted for consideration by U.S. Customs and Border Protection pursuant to such section 559, as in existence on the day before such date of enactment.

SEC. 484. [6 U.S.C. 301c] DEFINITIONS.

In this subtitle:

(1) DONOR.—The term "donor" means any entity that is proposing to make a donation under this Act.

(2) ENTITY.—The term "entity" means any—

(A) person;

(B) partnership, corporation, trust, estate, cooperative, association, or any other organized group of persons;

(C) Federal, State or local government (including any subdivision, agency or instrumentality thereof); or

(D) any other private or governmental entity.

TITLE V—NATIONAL EMERGENCY MANAGEMENT

SEC. 501. [6 U.S.C. 311] DEFINITIONS.

In this title—

(1) the term "Administrator" means the Administrator of the Agency;

(2) the term "Agency" means the Federal Emergency Management Agency;

(3) 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;

(4) the terms "credentialed" and "credentialing" mean having provided, or providing, respectively, documentation that identifies personnel and authenticates and verifies the qualifications of such personnel by ensuring that such personnel possess 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 510;

(5) 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) the term "interoperable" has the meaning given the term "interoperable communications" under section 7303(g)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(g)(1));

(7) the term "National Incident Management System" means a system to enable effective, efficient, and collaborative incident management;

(8) the term "National Response Plan" means the National Response Plan or any successor plan prepared under section 502(a)(6);

(9) the term "Regional Administrator" means a Regional Administrator appointed under section 507;

(10) the term "Regional Office" means a Regional Office established under section 507;

(11) 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;

(12) 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;

(13) the term "tribal government" means the government of any entity described in section 2(13)(B); and

(14) the terms "typed" and "typing" mean having evaluated, or evaluating, respectively, a resource in accordance with standards created under section 510.

SEC. 502. [6 U.S.C. 312] DEFINITION.

In this title, the term "Nuclear Incident Response Team" means a resource that includes—

(1) 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

(2) those entities of the Environmental Protection Agency that perform such support functions (including radiological emergency response functions) and related functions.

SEC. 503. [6 U.S.C. 313] FEDERAL EMERGENCY MANAGEMENT AGENCY.

(a) IN GENERAL.—There is in the Department the Federal Emergency Management Agency, headed by an Administrator.

(b) 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, emer-

gency response providers, 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 Director of 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;

(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; and

(I)[6] 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 such integration, as necessary.

(c) ADMINISTRATOR.—

(1) IN GENERAL.—The Administrator shall be appointed by the President, by and with the advice and consent of the Senate.

(2) QUALIFICATIONS.—The Administrator shall be appointed from among individuals who have—

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

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

(3) REPORTING.—The Administrator shall report to the Secretary, without being required to report through any other official of the Department.

(4) 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.—

[6] Section 3 of Public Law 117–130 amends section 503(b)(2) by adding a new subparagraph (I) at the end along with making conforming changes to subparagraphs (G) and (H). The amendment did not reference the amended Act properly, however, it was carried out to the Homeland Security Act [*of 2002*] to effectuate the probable intent of Congress.

(i) IN GENERAL.—In presenting advice with respect to any matter to the President, the Homeland Security Council, or the Secretary, the Administrator shall, as the Administrator considers appropriate, inform the President, the Homeland 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 REQUEST.—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 such advice.

(iii) RECOMMENDATIONS TO CONGRESS.—After informing the Secretary, the Administrator may make such recommendations to Congress relating to emergency management as the Administrator considers appropriate.

(5) 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 Act.

SEC. 504. [6 U.S.C. 314] 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 title)—

(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 such response;

(B) directing the Domestic Emergency Support Team, the National Disaster Medical System,[7] and (when operating as an organizational unit of the Department pursuant to this title) 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 such 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 any 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;

[7] The phrase ", the National Disaster Medical System," in subsection (a)(3)(B) probably should not appear. Section 301(c)(1) of Public Law 109–417 (120 Stat. 2854) provides for an amendment to the Homeland Security Act of 2002 as follows:

(1) in section 502(3)(B), by striking ", the National Disaster Medical System,"; and

The amendment was not executed because section 502 of the Homeland Security Act of 2002 was redesignated as section 504 by section 611(8) of Public Law 109–295 (120 Stat 1395).

(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 508;

(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 505; and

(21) otherwise carrying out the mission of the Agency as described in section 503(b).

(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.

SEC. 505. [6 U.S.C. 315] FUNCTIONS TRANSFERRED.

(a) IN GENERAL.—Except as provided in subsection (b), there are transferred to the Agency the following:

(1) All functions of the Federal Emergency Management 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, in-

cluding all of its personnel, assets, components, authorities, grant programs, and liabilities, and including the functions of the Under Secretary for Federal Emergency Management relating thereto.

(2) The 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 thereto.

(b) EXCEPTIONS.—The following within the Preparedness Directorate 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).

SEC. 506. [6 U.S.C. 316] PRESERVING THE FEDERAL EMERGENCY MANAGEMENT AGENCY.

(a) DISTINCT ENTITY.—The Agency shall be maintained as a distinct entity within the Department.

(b) REORGANIZATION.—Section 872 shall not apply to the Agency, including any function or organizational unit of the Agency.

(c) 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 708, the authorities, responsibilities, or functions of the Agency or the capability of the Agency to perform those missions, authorities, responsibilities, except as otherwise specifically provided in an Act enacted after the date of enactment of the Post-Katrina Emergency Management Reform Act of 2006.

(2) CERTAIN TRANSFERS PROHIBITED.—No asset, function, or mission of the Agency may be diverted to the principal and continuing use of any other organization, unit, or entity of the Department, including a Joint Task Force established under section 708, except for details or assignments that do not reduce the capability of the Agency to perform its missions.

(d) REPROGRAMMING AND TRANSFER OF FUNDS.—In reprogramming or transferring funds, the Secretary shall comply with any applicable provisions of any Act making appropriations for the Department for fiscal year 2007, or any succeeding fiscal year, relating to the reprogramming or transfer of funds.

SEC. 507. [6 U.S.C. 317] 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 such 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) 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 1 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 preidentify and evaluate suitable

sites where a multijurisdictional incident command system may quickly be established and operated from, if the need for such a system arises; and

(K) performing such other duties relating to such responsibilities as 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. Such training, as appropriate, shall include training with respect to the National Incident Management System, the National Response Plan, and such other subjects as 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 within 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 any geographic, demographic, or other characteristics peculiar to any 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 any weaknesses or deficiencies in preparedness, protection, response, recovery, and mitigation for any 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 multiagency 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) such other personnel as 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.—The duties of an individual assigned to a Regional Office strike team from another relevant agency when such individual is not functioning as a member of the strike team shall be consistent with the emergency preparedness activities of the agency that employs such 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 which 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.

SEC. 508. [6 U.S.C. 318] NATIONAL ADVISORY COUNCIL.

(a) ESTABLISHMENT.—Not later than 60 days after the date of enactment of the Post-Katrina Emergency Management Reform Act of 2006, the Secretary shall establish an advisory body under section 871(a) 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, to be known as the National Advisory Council.

(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 such 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) such other individuals as the Administrator determines to be appropriate.

(2) COORDINATION WITH THE 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 1 or more officers of the Federal Government to serve as ex officio members of the National Advisory Council.

(4) TERMS OF OFFICE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term of office of each member of the National Advisory Council shall be 3 years.

(B) INITIAL APPOINTMENTS.—Of the members initially appointed to the National Advisory Council—

(i) one-third shall be appointed for a term of 1 year; and

(ii) one-third shall be appointed for a term of 2 years.

(d) RESPONSE SUBCOMMITTEE.—

(1) ESTABLISHMENT.—Not later than 30 days after the date of the enactment of the RESPONSE Act of 2016, the Administrator shall establish, as a subcommittee of the National Advisory Council, the Railroad Emergency Services Preparedness, Operational Needs, and Safety Evaluation Subcommittee (referred to in this subsection as the "RESPONSE Subcommittee").

(2) MEMBERSHIP.—Notwithstanding subsection (c), the RESPONSE Subcommittee shall be 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 for 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 after the date of the enactment of the RESPONSE Act of 2016 from among the following:

(i) Members of the National Advisory Council that have the requisite technical knowledge and expertise to address rail emergency response issues, including members from 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 who 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) INITIAL MEETING.—The initial meeting of the RESPONSE Subcommittee shall take place not later than 90 days after the date of enactment of the RESPONSE Act of 2016.

(5) 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, which 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.

(6) 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 related 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 individuals 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 related 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 allocations;

(ii) identifying cost savings 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) adaptation of priority settings for agency funding allocations in response to emerging trends;

(v) 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) 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 increasing the rate of access to the individual responder in existing or emerging communications technology.

(7) REPORT.—

(A) IN GENERAL.—Not later than 1 year after the date of the enactment of the RESPONSE Act of 2016, the RESPONSE Subcommittee shall submit a report to the National Advisory Council that—

(i) includes the recommendations developed under paragraph (6);

(ii) specifies the timeframes for implementing any such recommendations that do not require congressional action; and

(iii) identifies any such 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) RECOMMENDATION.—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.

(8) INTERIM ACTIVITY.—

(A) UPDATES AND OVERSIGHT.—After the submission of the report by the National Advisory Council under paragraph (7), the Administrator shall—

(i) provide annual updates to the congressional committees referred to in paragraph (7)(C) regarding the status of the implementation of the recommendations developed under paragraph (6); and

(ii) coordinate the implementation of the recommendations described in paragraph (6)(G)(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 (7)(A).

(9) TERMINATION.—The RESPONSE Subcommittee shall terminate not later than 90 days after the submission of the report required under paragraph (7)(C).

(e) APPLICABILITY OF CHAPTER 10 OF TITLE 5, UNITED STATES CODE.—

(1) IN GENERAL.—Notwithstanding section 871(a) and subject to paragraph (2), chapter 10 of title 5, United States Code, including subsections (a), (b), and (d) of section 1009 of title 5, United States Code, and section 552b(c) of title 5, United States Code, shall apply to the National Advisory Council.

(2) TERMINATION.—Section 1013(a)(2) of title 5, United States Code, shall not apply to the National Advisory Council.

SEC. 509. [6 U.S.C. 319] NATIONAL INTEGRATION CENTER.

(a) IN GENERAL.—There is established in the Agency a 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 any successor to such system or plan.

(2) SPECIFIC RESPONSIBILITIES.—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 Secretary, acting through the Administrator, shall ensure that the National Response Plan provides for a clear chain of command to lead and coordinate the Federal response to any natural disaster, act of terrorism, or other man-made disaster.

(B) ADMINISTRATOR.—The chain of the command specified in the National Response Plan shall—

(i) provide for a role for 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 503(c)(4) and the responsibility of the Administrator under the Post-Katrina Emergency Management Reform Act of 2006, and the amendments made by that Act, relating to natural disasters, acts of terrorism, and other man-made disasters; and

(ii) provide for a role for 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; JOINT TASK FORCE.—The Principal Federal Official (or the successor thereto) or Director of a Joint Task Force established under section 708 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.

SEC. 510. [6 U.S.C. 320] 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 manmade disasters.

(b) DISTRIBUTION.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, 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 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; and

(B) State, local, and tribal governments, to aid such 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.—Not later than 6 months after receiving the standards provided under subsection (b), 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 in accordance with 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.

SEC. 511. [6 U.S.C. 321] THE NATIONAL INFRASTRUCTURE SIMULATION AND ANALYSIS CENTER.

(a) DEFINITION.—In this section, the term "National Infrastructure Simulation and Analysis Center" means the National Infra-

structure Simulation and Analysis Center established under section 1016(d) of the USA PATRIOT Act (42 U.S.C. 5195c(d)).

(b) AUTHORITY.—

(1) IN GENERAL.—There is in the Department the National Infrastructure Simulation and Analysis Center which shall serve as a source of national expertise to address critical infrastructure protection and continuity through support for activities related to—

(A) counterterrorism, threat assessment, and risk mitigation; and

(B) a natural disaster, act of terrorism, or other man-made disaster.

(2) INFRASTRUCTURE MODELING.—

(A) PARTICULAR SUPPORT.—The support provided under paragraph (1) shall include modeling, simulation, and analysis of the systems and assets comprising critical infrastructure, in order to enhance preparedness, protection, response, recovery, and mitigation activities.

(B) RELATIONSHIP WITH OTHER AGENCIES.—Each Federal agency and department with critical infrastructure responsibilities under Homeland Security Presidential Directive 7, or any successor to such directive, shall establish a formal relationship, including an agreement regarding information sharing, between the elements of such agency or department and the National Infrastructure Simulation and Analysis Center, through the Department.

(C) PURPOSE.—

(i) IN GENERAL.—The purpose of the relationship under subparagraph (B) shall be to permit each Federal agency and department described in subparagraph (B) 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.

(ii) 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 any successor to such directive.

SEC. 512. [6 U.S.C. 321a] EVACUATION PLANS AND EXERCISES.

(a) IN GENERAL.—Notwithstanding any other provision of 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 such plans, including the development of evacuation routes and the purchase and stockpiling of necessary supplies and shelters; and

(3) conduct exercises of such 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 such 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 such information; and

(6) identify shelter locations and capabilities.

(c) ASSISTANCE.—

(1) IN GENERAL.—The Administrator may establish any 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 such use assists such government in building capabilities for terrorism preparedness.

SEC. 513. [6 U.S.C. 321b] DISABILITY COORDINATOR.

(a) IN GENERAL.—After consultation with organizations representing individuals with disabilities, the National Council on Disabilities, and the Interagency Coordinating Council on Prepared-

ness and Individuals with Disabilities, established under Executive Order No. 13347 (6 U.S.C. 312 note), 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 shall be 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 Disabilities, the Interagency Coordinating Council on Preparedness and Individuals with Disabilities established under Executive Order No. 13347 (6 U.S.C. 312 note), 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 are included in the components of the national preparedness system established under section 644 of the Post-Katrina Emergency Management Reform Act of 2006; and

(11) any other duties as assigned by the Administrator.

SEC. 514. [6 U.S.C. 321c] DEPARTMENT AND AGENCY OFFICIALS.

(a) 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 this title.

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

SEC. 515. [6 U.S.C. 321d] NATIONAL OPERATIONS CENTER.

(a) DEFINITION.—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 decisionmaking 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 POSITIONS.—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 pursuant to paragraph (1) in accordance with such rules, regulations, and practices as govern other similar rotating positions at the National Operations Center.

[Section 516 was repealed by section 2(c)(1) of Public Law 115–387.]

SEC. 517. [6 U.S.C. 321f] 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 title shall be construed to limit the ordinary responsibility of the Secretary of Energy and the Administrator of the Environmental Protection Agency for organizing, training, equipping, and utilizing their respective

entities in the Nuclear Incident Response Team, or (subject to the provisions of this title) from exercising direction, authority, and control over them when they are not operating as a unit of the Department.

SEC. 518. [6 U.S.C. 321g] 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 such 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 such subsection.

SEC. 519. [6 U.S.C. 321h] 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.

SEC. 520. [6 U.S.C. 321i] USE OF COMMERCIALLY AVAILABLE TECHNOLOGY, GOODS, AND SERVICES.

It is the sense of Congress that—

(1) the Secretary should, to the maximum extent possible, use off-the-shelf commercially developed technologies to ensure that the Department's information technology systems allow the Department to collect, manage, share, analyze, and disseminate information securely over multiple channels of communication; and

(2) in order to further the policy of the United States to avoid competing commercially with the private sector, the Secretary should rely on commercial sources to supply the goods and services needed by the Department.

SEC. 521. [6 U.S.C. 321j] PROCUREMENT OF SECURITY COUNTERMEASURES FOR STRATEGIC NATIONAL STOCKPILE.

(a) AUTHORIZATION OF APPROPRIATIONS.—For the procurement of security countermeasures under section 319F–2(c) of the Public Health Service Act (referred to in this section as the "security countermeasures program"), there is authorized to be appropriated up to $5,593,000,000 for the fiscal years 2004 through 2013. Of the amounts appropriated under the preceding sentence, not to exceed $3,418,000,000 may be obligated during the fiscal years 2004 through 2008, of which not to exceed $890,000,000 may be obligated during fiscal year 2004. None of the funds made available under this subsection shall be used to procure countermeasures to diagnose, mitigate, prevent, or treat harm resulting from any natu-

rally occurring infectious disease or other public health threat that are not security countermeasures under section 319F–2(c)(1)(B). [8]

(b) SPECIAL RESERVE FUND.—For purposes of the security countermeasures program, the term "special reserve fund" means the "Biodefense Countermeasures" appropriations account or any other appropriation made under subsection (a).

(c) AVAILABILITY.—Amounts appropriated under subsection (a) become available for a procurement under the security countermeasures program only upon the approval by the President of such availability for the procurement in accordance with paragraph (6)(B) of such program.

(d) RELATED AUTHORIZATIONS OF APPROPRIATIONS.—

(1) THREAT ASSESSMENT CAPABILITIES.—For the purpose of carrying out the responsibilities of the Secretary for terror threat assessment under the security countermeasures program, there are authorized to be appropriated such sums as may be necessary for each of the fiscal years 2004 through 2006, for the hiring of professional personnel within the Office of Intelligence and Analysis, who shall be analysts responsible for chemical, biological, radiological, and nuclear threat assessment (including but not limited to analysis of chemical, biological, radiological, and nuclear agents, the means by which such agents could be weaponized or used in a terrorist attack, and the capabilities, plans, and intentions of terrorists and other non-state actors who may have or acquire such agents). All such analysts shall meet the applicable standards and qualifications for the performance of intelligence activities promulgated by the Director of Central Intelligence pursuant to section 104 of the National Security Act of 1947.

(2) INTELLIGENCE SHARING INFRASTRUCTURE.—For the purpose of carrying out the acquisition and deployment of secure facilities (including information technology and physical infrastructure, whether mobile and temporary, or permanent) sufficient to permit the Secretary to receive, not later than 180 days after the date of enactment of the Project BioShield Act of 2004, all classified information and products to which the Under Secretary for Intelligence and Analysis is entitled under subtitle A of title II, there are authorized to be appropriated such sums as may be necessary for each of the fiscal years 2004 through 2006.

SEC. 522. [6 U.S.C. 321k] MODEL STANDARDS AND GUIDELINES FOR CRITICAL INFRASTRUCTURE WORKERS.

(a) IN GENERAL.—Not later than 12 months after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, and in coordination with appropriate national professional organizations, Federal, State, local, and tribal govern-

[8] The last sentence in section 521(a) was added to reflect the probable intent of Congress. Section 403(c) of Public Law 109–417 (120 Stat. 2874) provides as follows:

(c) LIMITATION ON USE OF FUNDS.—Section 510(a) of the Homeland Security Act of 2002 (6 U.S.C. 320(a)) is amended by adding at the end the following: "None of the funds made available under this subsection shall be used to procure countermeasures to diagnose, mitigate, prevent, or treat harm resulting from any naturally occurring infectious disease or other public health threat that are not security countermeasures under section 319F–2(c)(1)(B).".

Section 510 of the Homeland Security Act of 2002 was redesignated as section 521 by section 611(7) of Public Law 109–295 (120 Stat. 1395).

ment 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 such governments with credentialing critical infrastructure workers that may respond to a natural disaster, act of terrorism, or other manmade disaster.

SEC. 523. [6 U.S.C. 321l] GUIDANCE AND RECOMMENDATIONS.

(a) IN GENERAL.—Consistent with their responsibilities and authorities under law, as of the day before the date of the enactment of this section, 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 any 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 any requirement established under any other provision of law.

SEC. 524. [6 U.S.C. 321m] 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 in accordance with this section.

(2) DESIGNATION OF OFFICER.—The Secretary shall designate an officer responsible for the accreditation and certification program under this section. Such officer (hereinafter referred to in this section 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 Secretary for Infrastructure Protection, based on consideration of the expertise of the Assistant Secretary in, and responsibilities for—

(i) protection of critical infrastructure;

(ii) risk assessment methodologies; and

(iii) interacting 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 such 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.—Not later than 210 days after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, 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 102(f)(4), 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 any 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) PROGRAM.—The program developed and implemented under this subsection shall assess whether a private sector entity complies with voluntary preparedness standards.

(ii) GUIDELINES.—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 102(f)(4), 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 within 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 any 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 any 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 within the private sector, including preparedness standards, business continuity standards, or best practices, established—

(I) under any other provision of Federal law; or

(II) by any 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) IN GENERAL.—Not later than 210 days after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, 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 (hereinafter referred to in this section as a "selected entity") shall not perform certifications under this subsection.

(ii) CONTENTS.—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) IN GENERAL.—Any 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) CONTENTS AND USE.—The procedures and requirements developed under clause (i) shall—

(I) ensure reasonable uniformity in any accreditation and certification processes if there is more than one selected entity; and

(II) be used by any selected entity in conducting accreditations and overseeing the certification process under this subsection.

(iii) DISAGREEMENT.—Any disagreement among selected entities in developing procedures under clause (i) shall be resolved by the designated officer.

(C) DESIGNATION.—A selected entity may accredit any 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 section 124 of title 13, United States Code of Federal Regulations.

(E) TREATMENT OF OTHER CERTIFICATIONS.—At the request of any entity seeking certification, any selected entity may consider, as appropriate, other relevant certifications acquired by the entity seeking certification. If the selected entity determines that such 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 such procedures and requirements;

(iii) agree not to have any beneficial interest in or any direct or indirect control over—

(I) a private sector entity for which that third party conducts a certification under this subsection; or

(II) any organization that provides preparedness consulting services to private sector entities;

(iv) agree not to have any other conflict of interest with respect to any private sector entity for which that 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 any proprietary information of a private sector entity obtained under this subsection.

(G) MONITORING.—

(i) IN GENERAL.—The designated officer and any selected entity shall regularly monitor and inspect the operations of any 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) REVOCATION.—If the designated officer or any selected entity determines that a third party is not meeting the procedures or 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 any certification 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 organizations, appropriate representatives of State and local governments, including emergency management officials, and each private sector advisory council created under section 102(f)(4), shall annually review the voluntary accreditation and certification program established under this subsection to ensure the effectiveness of such program (including the operations and management of such program by any 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 any 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 such listing.

(c) RULE OF CONSTRUCTION.—Nothing in this section may be construed as—

(1) a requirement to replace any preparedness, emergency response, or business continuity standards, requirements, or best practices established—

(A) under any other provision of federal law; or

(B) by any Sector Risk Management Agency, as those agencies are defined under Homeland Security Presidential Directive–7; or

(2) exempting any 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.

SEC. 525. [6 U.S.C. 321n] 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) any 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 publically available.

SEC. 526. [6 U.S.C. 321o] 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 gov-

ernmental 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.

(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 1 year after the date of enactment of the Integrated Public Alert and Warning System Modernization Act of 2015, and annually thereafter through 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 function 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 these 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) 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).

SEC. 527. [6 U.S.C. 321p] 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.

SEC. 528. [6 U.S.C. 321q] COORDINATION OF DEPARTMENT OF HOMELAND SECURITY EFFORTS RELATED TO FOOD, AGRICULTURE, AND VETERINARY DEFENSE AGAINST TERRORISM.

(a) PROGRAM REQUIRED.—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 such 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) Other activities as determined necessary by the Secretary.

(c) RULE OF CONSTRUCTION.—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.

SEC. 529. [6 U.S.C. 321r] 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 protective 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 within 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 of the Department, 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.

TITLE VI—TREATMENT OF CHARITABLE TRUSTS FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES AND OTHER GOVERNMENTAL ORGANIZATIONS

SEC. 601. [6 U.S.C. 331] TREATMENT OF CHARITABLE TRUSTS FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES AND OTHER GOVERNMENTAL ORGANIZATIONS.

(a) FINDINGS.—Congress finds the following:

(1) Members of the Armed Forces of the United States defend the freedom and security of our Nation.

(2) Members of the Armed Forces of the United States have lost their lives while battling the evils of terrorism around the world.

(3) Personnel of the Central Intelligence Agency (CIA) charged with the responsibility of covert observation of terrorists around the world are often put in harm's way during their service to the United States.

(4) Personnel of the Central Intelligence Agency have also lost their lives while battling the evils of terrorism around the world.

(5) Employees of the Federal Bureau of Investigation (FBI) and other Federal agencies charged with domestic protection of the United States put their lives at risk on a daily basis for the freedom and security of our Nation.

(6) United States military personnel, CIA personnel, FBI personnel, and other Federal agents in the service of the United States are patriots of the highest order.

(7) CIA officer Johnny Micheal Spann became the first American to give his life for his country in the War on Terrorism declared by President George W. Bush following the terrorist attacks of September 11, 2001.

(8) Johnny Micheal Spann left behind a wife and children who are very proud of the heroic actions of their patriot father.

(9) Surviving dependents of members of the Armed Forces of the United States who lose their lives as a result of terrorist attacks or military operations abroad receive a $6,000 death benefit, plus a small monthly benefit.

(10) The current system of compensating spouses and children of American patriots is inequitable and needs improvement.

(b) DESIGNATION OF JOHNNY MICHEAL SPANN PATRIOT TRUSTS.—Any charitable corporation, fund, foundation, or trust (or separate fund or account thereof) which otherwise meets all applicable requirements under law with respect to charitable entities and meets the requirements described in subsection (c) shall be eli-

gible to characterize itself as a "Johnny Micheal Spann Patriot Trust".

(c) REQUIREMENTS FOR THE DESIGNATION OF JOHNNY MICHEAL SPANN PATRIOT TRUSTS.—The requirements described in this subsection are as follows:

(1) Not taking into account funds or donations reasonably necessary to establish a trust, at least 85 percent of all funds or donations (including any earnings on the investment of such funds or donations) received or collected by any Johnny Micheal Spann Patriot Trust must be distributed to (or, if placed in a private foundation, held in trust for) surviving spouses, children, or dependent parents, grandparents, or siblings of 1 or more of the following:

(A) members of the Armed Forces of the United States;

(B) personnel, including contractors, of elements of the intelligence community, as defined in section 3(4) of the National Security Act of 1947;

(C) employees of the Federal Bureau of Investigation; and

(D) officers, employees, or contract employees of the United States Government,

whose deaths occur in the line of duty and arise out of terrorist attacks, military operations, intelligence operations, or law enforcement operations or accidents connected with activities occurring after September 11, 2001, and related to domestic or foreign efforts to curb international terrorism, including the Authorization for Use of Military Force (Public Law 107–40; 115 Stat. 224).

(2) Other than funds or donations reasonably necessary to establish a trust, not more than 15 percent of all funds or donations (or 15 percent of annual earnings on funds invested in a private foundation) may be used for administrative purposes.

(3) No part of the net earnings of any Johnny Micheal Spann Patriot Trust may inure to the benefit of any individual based solely on the position of such individual as a shareholder, an officer or employee of such Trust.

(4) None of the activities of any Johnny Micheal Spann Patriot Trust shall be conducted in a manner inconsistent with any law that prohibits attempting to influence legislation.

(5) No Johnny Micheal Spann Patriot Trust may participate in or intervene in any political campaign on behalf of (or in opposition to) any candidate for public office, including by publication or distribution of statements.

(6) Each Johnny Micheal Spann Patriot Trust shall comply with the instructions and directions of the Director of Central Intelligence, the Attorney General, or the Secretary of Defense relating to the protection of intelligence sources and methods, sensitive law enforcement information, or other sensitive national security information, including methods for confidentially disbursing funds.

(7) Each Johnny Micheal Spann Patriot Trust that receives annual contributions totaling more than $1,000,000 must be audited annually by an independent certified public accounting

firm. Such audits shall be filed with the Internal Revenue Service, and shall be open to public inspection, except that the conduct, filing, and availability of the audit shall be consistent with the protection of intelligence sources and methods, of sensitive law enforcement information, and of other sensitive national security information.

(8) Each Johnny Micheal Spann Patriot Trust shall make distributions to beneficiaries described in paragraph (1) at least once every calendar year, beginning not later than 12 months after the formation of such Trust, and all funds and donations received and earnings not placed in a private foundation dedicated to such beneficiaries must be distributed within 36 months after the end of the fiscal year in which such funds, donations, and earnings are received.

(9)(A) When determining the amount of a distribution to any beneficiary described in paragraph (1), a Johnny Micheal Spann Patriot Trust should take into account the amount of any collateral source compensation that the beneficiary has received or is entitled to receive as a result of the death of an individual described in paragraph (1).

(B) Collateral source compensation includes all compensation from collateral sources, including life insurance, pension funds, death benefit programs, and payments by Federal, State, or local governments related to the death of an individual described in paragraph (1).

(d) TREATMENT OF JOHNNY MICHEAL SPANN PATRIOT TRUSTS.—Each Johnny Micheal Spann Patriot Trust shall refrain from conducting the activities described in clauses (i) and (ii) of section 301(20)(A) of the Federal Election Campaign Act of 1971 so that a general solicitation of funds by an individual described in paragraph (1) of section 323(e) of such Act will be permissible if such solicitation meets the requirements of paragraph (4)(A) of such section.

(e) NOTIFICATION OF TRUST BENEFICIARIES.—Notwithstanding any other provision of law, and in a manner consistent with the protection of intelligence sources and methods and sensitive law enforcement information, and other sensitive national security information, the Secretary of Defense, the Director of the Federal Bureau of Investigation, or the Director of Central Intelligence, or their designees, as applicable, may forward information received from an executor, administrator, or other legal representative of the estate of a decedent described in subparagraph (A), (B), (C), or (D) of subsection (c)(1), to a Johnny Micheal Spann Patriot Trust on how to contact individuals eligible for a distribution under subsection (c)(1) for the purpose of providing assistance from such Trust: *Provided*, That, neither forwarding nor failing to forward any information under this subsection shall create any cause of action against any Federal department, agency, officer, agent, or employee.

(f) REGULATIONS.—Not later than 90 days after the date of enactment of this Act, the Secretary of Defense, in coordination with the Attorney General, the Director of the Federal Bureau of Investigation, and the Director of Central Intelligence, shall prescribe regulations to carry out this section.

TITLE VII—MANAGEMENT

SEC. 701. [6 U.S.C. 341] UNDER SECRETARY FOR MANAGEMENT.

(a) IN GENERAL.—The Under Secretary for Management shall serve as the Chief Management Officer and principal advisor to the Secretary on matters related 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, shall be 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, vehicle fleets (under subsection (c)), 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 within 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 im-

plement 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 such 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 six 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.

(b) WAIVERS FOR CONDUCTING BUSINESS WITH SUSPENDED OR DEBARRED CONTRACTORS.—Not later than five 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 thereto, 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.

(c) VEHICLE FLEETS.—

(1) IN GENERAL.—In carrying out responsibilities regarding vehicle fleets pursuant to subsection (a)(5), the Under Secretary for Management 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 (4).

(C) Ensuring that components formally document fleet management decisions.

(D) Approving component fleet management plans, vehicle leases, and vehicle acquisitions.

(2) 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 such 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 (6); 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 (5)(B).

(B) EXCEPTION REGARDING CERTAIN LEASING AND ACQUISITIONS.—If exigent circumstances warrant such, 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 such exigent circumstances a component head so leases, acquires, or replaces a vehicle, such component head shall provide to the Under Secretary an explanation of such circumstances.

(3) ONGOING OVERSIGHT.—

(A) QUARTERLY MONITORING.—In accordance with paragraph (4), 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 such 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 such information to inform the annual component fleet analyses referred to in paragraph (4).

(4) ANNUAL REVIEW OF COMPONENT FLEET ANALYSES.—

(A) IN GENERAL.—To determine the optimal fleet size and associated resources needed for each fiscal year beginning with fiscal year 2018, component heads shall annu-

ally submit to the Under Secretary for Management a vehicle allocation tool and fleet management plan using information described in paragraph (3)(A). Such tools and plans may be submitted in classified form if a component head determines that such 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 (2)(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 such mileage for leased vehicles, in accordance with such paragraph.

(ii) The role of vehicle fleets in supporting mission requirements for each component.

(iii) Any other information determined relevant by such component heads.

(C) FLEET MANAGEMENT PLANS.—Component heads shall use information described in subparagraph (B) to develop a fleet management plan for each such component. Such fleet management plans shall include the following:

(i) A plan for how each such component may achieve optimal fleet size determined by the vehicle allocation tool required under such subparagraph, including the elimination of excess vehicles in accordance with paragraph (5), if applicable.

(ii) A cost benefit analysis supporting such plan.

(iii) A schedule each such 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 such 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 (2) relating to fleet management and use of vehicles from home to work. The Under Secretary shall use such tools and plans when reviewing annual component requests for vehicle fleet funding in accordance with paragraph (6).

(5) GUIDANCE TO DEVELOP FLEET MANAGEMENT PLANS.—The Under Secretary for Management shall provide guidance, pursuant to paragraph (1)(B) on how component heads may achieve optimal fleet size in accordance with paragraph (4), 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.

(6) 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 (4) and (5), the Under Secretary 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 such component vehicle fleets.

(7) ACCOUNTABILITY FOR VEHICLE FLEET MANAGEMENT.—

(A) PROHIBITION ON CERTAIN NEW VEHICLE LEASES AND ACQUISITIONS.—The Under Secretary for Management and component heads may not approve in any fiscal year beginning with fiscal year 2019 a vehicle lease, acquisition, or replacement request if such component heads did not comply in the prior fiscal year with paragraph (4).

(B) PROHIBITION ON CERTAIN PERFORMANCE COMPENSATION.—No Department official with vehicle fleet management responsibilities may receive annual performance compensation in pay in any fiscal year beginning with fiscal year 2019 if such official did not comply in the prior fiscal year with paragraph (4).

(C) PROHIBITION ON CERTAIN CAR SERVICES.—Notwithstanding any other provision of law, no senior executive service official of the Department whose office has a vehicle fleet may receive access to a car service in any fiscal year beginning with fiscal year 2019 if such official did not comply in the prior fiscal year with paragraph (4).

(8) 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.

(9) DEFINITIONS.—In this subsection:

(A) COMPONENT HEAD.—The term "component head" means the head of any component of the Department with a vehicle fleet.

(B) EXCESS VEHICLE.—The term "excess vehicle" means any 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 such 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, as the case may be, including vehicles used for law enforcement and other purposes.

(d) APPOINTMENT AND EVALUATION.—The Under Secretary for Management shall—

(1) be appointed by the President, by and with the advice and consent of the Senate, from among persons 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) enter into an annual performance agreement with the Secretary that shall set forth measurable individual and organizational goals; and

(3) be subject to an annual performance evaluation by the Secretary, who shall determine as part of each such 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).

(e)[9] 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.

[9] Two subsection (e)s' in section 701 is so in law. See amendments made by section 1903(b)(3), (4) of Public Law 114–328 (130 Stat. 2674) and section 2(2), (3) of Public Law 115–38.

(e)[9] INTEROPERABLE COMMUNICATIONS DEFINED.—In this section, the term "interoperable communications" has the meaning given that term in section 7303(g) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(g)).

SEC. 702. [6 U.S.C. 342] CHIEF FINANCIAL OFFICER.

(a) In General.—The Chief Financial Officer shall perform functions as specified in chapter 9 of title 31, United States Code, and, with respect to all such functions and other responsibilities that may be assigned to the Chief Financial Officer from time to time, shall also report to the Under Secretary for Management.

(b) PROGRAM ANALYSIS AND EVALUATION FUNCTION.—

(1) ESTABLISHMENT OF OFFICE OF PROGRAM ANALYSIS AND EVALUATION.—Not later than 90 days after the date of enactment of this subsection, the Secretary shall establish an Office of Program Analysis and Evaluation within the Department (in this section referred to as the "Office").

(2) RESPONSIBILITIES.—The Office shall perform the following functions:

(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 pursuant to section 874(b)(2).

(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 pursuant to section 874(b)(2).

(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 874.

(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, United States Code.

(H) Provide leadership in developing and promoting improved analytical tools and methods for analyzing homeland security planning and the allocation of resources.

(I) Any other responsibilities delegated by the Secretary consistent with an effective program analysis and evaluation function.

(3) DIRECTOR OF PROGRAM ANALYSIS AND EVALUATION.—There shall be a Director of Program Analysis and Evaluation, who—

(A) shall be 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, in accordance with section 872(a).

(B) EXEMPTION FROM LIMITATIONS.—Section 872(b) shall not apply to any action by the Secretary under this paragraph.

(c) NOTIFICATION REGARDING TRANSFER OR REPROGRAMMING OF FUNDS.—In any case in which appropriations available to the Department or any officer of the Department are transferred or reprogrammed and notice of such transfer or reprogramming is submitted to the Congress (including any officer, office, or Committee of the Congress), the Chief Financial Officer of the Department shall simultaneously submit such notice to the Select Committee on Homeland Security (or any successor to the jurisdiction of that committee) and the Committee on Government Reform of the House of Representatives, and to the Committee on Governmental Affairs of the Senate.

SEC. 703. [6 U.S.C. 343] 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.—As used in this subsection:

(A) GEOSPATIAL INFORMATION.—The term "geospatial information" means graphical or digital data depicting natural or manmade physical features, phenomena, or boundaries of the earth and any information related thereto, including surveys, maps, charts, remote sensing data, and images.

(B) GEOSPATIAL TECHNOLOGY.—The term "geospatial technology" means any 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.—The Office of Geospatial Management is established within the Office of the Chief Information Officer.

(B) GEOSPATIAL INFORMATION OFFICER.—

(i) APPOINTMENT.—The Office of Geospatial Management shall be administered by the Geospatial Information Officer, who shall be appointed by the Secretary and serve under the direction of the Chief Information Officer.

(ii) FUNCTIONS.—The Geospatial Information Officer shall assist 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 such geospatial information as may be necessary 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 assure interoperability and prevent unnecessary duplication.

(D) RESPONSIBILITIES.—In carrying out this subsection, the responsibilities of the Chief Information Officer shall 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 (44 U.S.C. 3501 note), to facilitate the interoperability of geospatial information pertaining to homeland security among all users of such information within—

(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; 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.

(3) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out this subsection for each fiscal year.

SEC. 704. [6 U.S.C. 344] CHIEF HUMAN CAPITAL OFFICER.

(a) IN GENERAL.—The Chief Human Capital Officer shall report directly to the Under Secretary for Management.

(b) RESPONSIBILITIES.—In addition to the responsibilities set forth in chapter 14 of title 5, United States Code, 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 to section 844, 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 such survey and submit to the Secretary such analysis, including, as appropriate, recommendations to improve workforce satisfaction or morale within the Department;

(12) review and approve all component employee engagement action plans to ensure such 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 such 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, United States Code.

(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 within the Department of fulfilling the workforce strategies developed under subsection (c);

(2) information on employee development opportunities catalogued pursuant to paragraph (9) of subsection (b) 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 paragraph (2) of subsection (b);

(4) information on the activities of the steering committee established pursuant to section 711(a), 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 (division C of Public Law 111–117; 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 888.

SEC. 705. [6 U.S.C. 345] ESTABLISHMENT OF 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 such 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 any such 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 on the implementation of this section, including the use of funds appropriated to carry out this section, and detailing any allegations of abuses described under subsection (a)(1) and any actions taken by the Department in response to such allegations.

SEC. 706. [6 U.S.C. 346] CONSOLIDATION AND CO-LOCATION OF OFFICES.

Not later than 1 year after the date of the enactment of this Act, the Secretary shall develop and submit to Congress a plan for consolidating and co-locating—

(1) any regional offices or field offices of agencies that are transferred to the Department under this Act, if such officers are located in the same municipality; and

(2) portions of regional and field offices of other Federal agencies, to the extent such offices perform functions that are transferred to the Secretary under this Act.

SEC. 707. [6 U.S.C. 347] QUADRENNIAL HOMELAND SECURITY REVIEW.

(a) REQUIREMENT.—

(1) QUADRENNIAL REVIEWS REQUIRED.—In fiscal year 2009, 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 REVIEWS.—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,,[10] and the Director of National Intelligence;

(B) key officials of the Department, including the Under Secretary for Strategy, Policy, and Plans;

(C) representatives from appropriate advisory committees established pursuant to section 871, including the Homeland Security Advisory Council and the Homeland Security Science and Technology Advisory Committee, or otherwise established, including the Aviation Security Advisory Committee established pursuant to section 44946 of title 49, United States Code; and

(D) other relevant governmental and nongovernmental entities, including State, local, and tribal government offi-

[10] Two commas are so law. See amendment made by section 1740(b)(1) of division A of Public Law 116–92.

cials, 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 874.

(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, the 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 submission 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 GMDrisk assessment under section 320(d)(1)(E);

(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, upon request, provide 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 such quadrennial homeland security review.

(B) Information regarding the risk assessment required pursuant to subsection (c)(2)(B), including the following:

(i) The risk model utilized to generate such risk assessment.

(ii) Information, including data used in the risk model, utilized to generate such risk assessment.

(iii) Sources of information, including other risk assessments, utilized to generate such risk assessment.

(iv) Information on assumptions, weighing factors, and subjective judgments utilized to generate such risk assessment, together with information on the rationale or basis thereof.

(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 such report were integrated into the acquisition strategy and expenditure plans for the Department.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out this section.

SEC. 708. [6 U.S.C. 348] JOINT TASK FORCES.

(a) DEFINITION.—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 such threats and trends;

(3) the ability to evaluate such 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) JOINT TASK FORCES.—

(1) 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 paragraph (2).

(2) PURPOSES.—

(A) IN GENERAL.—Subject to subparagraph (B), the purposes referred to in paragraph (1) are or relate to the following:

(i) Securing the land and maritime borders of the United States.

(ii) Homeland security crises.

(iii) Establishing regionally-based operations.

(B) LIMITATION.—

(i) 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 title V of this Act, including section 504(a)(3)(A), unless the responsibilities of such a Joint Task Force—

(I) do not include operational functions related to incident management, including coordination of operations; and

(II) are consistent with the requirements of paragraphs (3) and (4)(A) of section 503(c) and section 509(c) of this Act, and section 302 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5143).

(ii) RESPONSIBILITIES AND FUNCTIONS 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 Agency under title V of this Act or any other provision of law, including the diversion of any asset, function, or mission from the Agency or the Administrator of the Agency pursuant to section 506.

(3) JOINT TASK FORCE DIRECTORS.—

(A) DIRECTOR.—Each Joint Task Force established and operated pursuant to paragraph (1) shall be headed by a Director, appointed by the President, for a term of not more than two years. The Secretary shall submit to the President recommendations for such appointments after consulting with the heads of the components of the Department with membership on any such Joint Task Force. Any Director appointed by the President shall be—

(i) a current senior official of the Department with not less than one 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 one 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 any such Joint Task Force.

(B) EXTENSION.—The Secretary may extend the appointment of a Director of a Joint Task Force under subparagraph (A) for not more than two years if the Secretary determines that such an extension is in the best interest of the Department.

(4) JOINT TASK FORCE DEPUTY DIRECTORS.—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 of such Joint Task Force.

(5) RESPONSIBILITIES.—The Director of a Joint Task Force, subject to the oversight, direction, and guidance of the Secretary, shall—

(A) when established for the purpose referred to in paragraph (2)(A)(i), maintain situational awareness within

the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(B) provide operational plans and requirements for standard operating procedures and contingency operations within the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(C) plan and execute joint task force activities within the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(D) set and accomplish strategic objectives through integrated operational planning and execution;

(E) 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;

(F) when established for the purpose referred to in paragraph (2)(A)(i), establish operational and investigative priorities within the areas of responsibility of the Joint Task Force, as determined by the Secretary;

(G) coordinate with foreign governments and other Federal, State, and local agencies, as appropriate, to carry out the mission of the Joint Task Force; and

(H) carry out other duties and powers the Secretary determines appropriate.

(6) PERSONNEL AND RESOURCES.—

(A) IN GENERAL.—The Secretary may, upon request of the Director of a Joint Task Force, and giving appropriate consideration of risk to the other primary missions of the Department, allocate to such Joint Task Force on a temporary basis personnel and equipment of components and offices of the Department.

(B) 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 such Joint Task Force if such Joint Task Force had not been established.

(C) 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.

(D) CONSIDERATION OF IMPACT.—When reviewing requests for allocation of component personnel and equipment under subparagraph (A), the Secretary shall consider the impact of such 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 888.

(E) LIMITATION.—Personnel and equipment of the Coast Guard allocated under this paragraph may be used only to carry out operations and investigations related to the missions specified in section 888.

(F) REPORT.—The Secretary shall, at the time the budget of the President is submitted to Congress for a fiscal year under section 1105(a) of title 31, United States Code, 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 paragraph to each Joint Task Force to carry out the mission of such Joint Task Force during the fiscal year immediately preceding each such report, and a description of the degree to which the resources drawn from each component or office impact the primary mission of such component or office.

(7) COMPONENT RESOURCE AUTHORITY.—As directed by the Secretary—

(A) 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 such Joint Task Force required under this section;

(B) the resources referred to in subparagraph (A) shall be under the operational authority, direction, and control of the Director of the Joint Task Force to which such resources are assigned; and

(C) 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 such personnel or equipment.

(8) JOINT TASK FORCE 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 of such Joint Task Force in carrying out the mission and responsibilities of such Joint Task Force.

(B) REPORT.—The Secretary shall include in the report submitted under paragraph (6)(F)—

(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.

(9) MISSION; ESTABLISHMENT OF PERFORMANCE METRICS.—The Secretary shall—

(A) using leading practices in performance management and lessons learned by other law enforcement task forces and joint operations, establish—

(i) the mission, strategic goals, and objectives of each Joint Task Force;

(ii) the criteria for terminating each Joint Task Force; and

(iii) 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 clause (i), including—

(I) targets for each Joint Task Force to achieve by not later than one and three years after such establishment; and

(II) a description of the methodology used to establish such metrics;

(B) not later than 120 days after the date of the enactment of the DHS Joint Task Forces Reauthorization Act of 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 subparagraph (A); and

(C) not later than one year after the date of the enactment of the DHS Joint Task Forces Reauthorization Act of 2022 and annually thereafter, submit to the committees specified in subparagraph (B) a report that contains information on the progress in implementing the outcome-based and other appropriate performance metrics established pursuant to subparagraph (A)(iii).

(10) JOINT DUTY TRAINING PROGRAM.—

(A) IN GENERAL.—The Secretary shall—

(i) establish a joint duty training program in the Department for the purposes of—

(I) enhancing coordination within the Department; and

(II) promoting workforce professional development; and

(ii) tailor such joint duty training program to improve joint operations as part of the Joint Task Forces.

(B) ELEMENTS.—The joint duty training program established under subparagraph (A) shall address, at a minimum, the following topics:

(i) National security strategy.

(ii) Strategic and contingency planning.

(iii) Command and control of operations under joint command.

(iv) International engagement.

(v) The homeland security enterprise.

(vi) Interagency collaboration.

(vii) Leadership.

(viii) Specific subject matters relevant to the Joint Task Force, including matters relating to the missions specified in section 888, to which the joint duty training program is assigned.

(C) TRAINING REQUIRED.—

(i) DIRECTORS AND DEPUTY DIRECTORS.—Except as provided in clauses (iii) and (iv), an individual shall complete the joint duty training program before being appointed Director or Deputy Director of a Joint Task Force.

(ii) JOINT TASK FORCE STAFF.—Each official serving on the staff of a Joint Task Force shall complete the joint duty training program within the first year of assignment to such Joint Task Force.

(iii) EXCEPTION.—Clause (i) shall not apply to the first Director or Deputy Director appointed to a Joint Task Force on or after the date of the enactment of this section.

(iv) WAIVER.—The Secretary may waive the application of clause (i) if the Secretary determines that such a waiver is in the interest of homeland security or necessary to carry out the mission for which a Joint Task Force was established.

(11) NOTIFICATION OF JOINT TASK FORCE FORMATION OR TERMINATION.—

(A) IN GENERAL.—Not later than seven days after establishing or terminating a Joint Task Force under this subsection, 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, and 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 such establishment or termination, as the case may be. The contents of any such notification shall include the following:

(i) The criteria and conditions required to establish or terminate the Joint Task Force at issue.

(ii) The primary mission, strategic goals, objectives, and plan of operations of such Joint Task Force.

(iii) If such notification is a notification of termination, information on the effectiveness of such Joint Task Force as measured by the outcome-based performance metrics and other appropriate performance metrics established pursuant to paragraph (9)(A)(iii).

(iv) The funding and resources required to establish or terminate such Joint Task Force.

(v) The number of personnel of each component or office permanently assigned to such Joint Task Force.

(vi) The number of personnel of each component and office assigned on a temporary basis to such Joint Task Force.

(vii) If such notification is a notification of establishment, the anticipated costs of establishing and operating such Joint Task Force.

(viii) If such notification is a notification of termination, funding allocated in the immediately preceding fiscal year to such Joint Task Force for—

(I) operations, notwithstanding such termination; and

(II) activities associated with such termination.

(ix) The anticipated establishment or actual termination date of such Joint Task Force, as the case may be.

(B) WAIVER AUTHORITY.—The Secretary may waive the requirement under subparagraph (A) in the event of an emergency circumstance that imminently threatens the protection of human life or property.

(12) REVIEW.—

(A) IN GENERAL.—Not later than one year after the date of the enactment of the DHS Joint Task Forces Reauthorization Act of 2022, the Comptroller General of the United States 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 (b)(2) as among the range of options available to the Secretary to conduct joint operations among departmental components and offices and a review of the Joint Task Forces established under this subsection.

(B) CONTENTS.—The review required under subparagraph (A) shall include—

(i) an assessment of methodology utilized to determine whether to establish or terminate each Joint Task Force; and

(ii) 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 paragraph (9)(A)(iii)) to evaluate the effectiveness of each Joint Task Force in measuring progress with respect to the mission, strategic goals, and objectives (established pursuant to paragraph (9)(A)(i)) of such Joint Task Force.

(13) SUNSET.—This section expires on September 30, 2024.

(c) JOINT DUTY ASSIGNMENT PROGRAM.—After establishing the joint duty training program under subsection (b)(10), the Secretary shall establish a joint duty assignment program within the Department for the purposes of enhancing coordination in the Department and promoting workforce professional development.

SEC. 709. [6 U.S.C. 349] OFFICE OF STRATEGY, POLICY, AND PLANS.

(a) IN GENERAL.—There is established in the Department an Office of Strategy, Policy, and Plans.

(b) HEAD OF OFFICE.—The Office of Strategy, Policy, and Plans shall be headed by an Under Secretary for Strategy, Policy, and Plans, who shall serve as the principal policy advisor to the Secretary. The Under Secretary for Strategy, Policy, and Plans shall be appointed by the President, by and with the advice and consent of the Senate.

(c) 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 707;

(4) manage Department leadership councils and provide analytics and support to such 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.

(d) DEPUTY UNDER SECRETARY.—

(1) IN GENERAL.—The Secretary may—

(A) establish within 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 such position.

(2) LIMITATION ON ESTABLISHMENT OF DEPUTY UNDER SECRETARY POSITIONS.—A Deputy Under Secretary position (or any substantially similar position) within the Office of Strategy, Policy, and Plans may not be established except for the position provided for by paragraph (1), unless the Secretary receives prior authorization from Congress.

(3) DEFINITIONS.—For purposes of paragraph (1)—

(A) the term "career employee" means any employee (as such term is defined in section 2105 of title 5, United States Code), but does not include a political appointee; and

(B) the term "political appointee" means any employee who occupies a position which has been excepted from the competitive service by reason of its confidential, policy-determining, policy-making, or policy-advocating character.

(e) 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 such component.

(f) 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 such 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 United States 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 applications and petitions filed by an alien (or filed on behalf of an alien) and denied, and the reasons for such denials, disaggregated by category of denial and application or petition type.

(g) ASSISTANT SECRETARY.—

(1) IN GENERAL.—There is established within the Office of Strategy, Policy, and Plans an Assistant Secretary, who shall assist the Secretary in carrying out the duties under paragraph (2) and the responsibilities under paragraph (3). Notwithstanding section 103(a)(1), the Assistant Secretary established under this paragraph shall be appointed by the President without the advice and consent of the Senate.

(2) DUTIES.—At the direction of the Secretary, the Assistant Secretary established under paragraph (1) shall be responsible for policy formulation regarding matters relating to economic security and trade, as such matters relate to the mission and the operations of the Department.

(3) ADDITIONAL RESPONSIBILITIES.—In addition to the duties specified in paragraph (2), the Assistant Secretary established under paragraph (1), at the direction 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.

(4) 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 such term in section 890B(c)(2).

(h) LIMITATION.—Nothing in this section overrides or otherwise affects the requirements specified in section 888.

SEC. 710. [6 U.S.C. 350] WORKFORCE HEALTH AND MEDICAL SUPPORT.

(a) 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.

(b) RESPONSIBILITIES.—The Under Secretary for Management, in coordination with the Chief Medical Officer, shall—

(1) provide oversight and coordinate the medical and health activities of the Department for the human and animal personnel of the Department;

(2) establish medical, health, veterinary, and occupational health exposure policy, guidance, strategies, and initiatives for the human and animal personnel of the Department;

(3) as deemed appropriate by the Under Secretary, provide medical liaisons to the components of the Department, on a reimbursable basis, to provide subject matter expertise on occupational medical and public health issues;

(4) 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 such detailed Commissioned Corps officers; and

(5) perform such other duties relating to the responsibilities described in this subsection as the Secretary may require.

SEC. 711. [6 U.S.C. 351] EMPLOYEE ENGAGEMENT.

(a) STEERING COMMITTEE.—Not later than 120 days after the date of the enactment of this section, 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 within the Department, such as perceptions 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 within 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 within 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 paragraph (1) of such subsection, to execute strategies to improve employee engagement, morale, and communications within 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 such 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 the date that is five years after the date of the enactment of this section.

SEC. 712. [6 U.S.C. 352] 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 such 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 such awards from the Secretary; and

(5) publicize such program within the Department.

(b) INTERNAL REVIEW BOARD.—The internal review board described in subsection (a)(3) shall, when carrying out its function under such subsection, 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.

SEC. 713. [6 U.S.C. 353] ACQUISITION PROFESSIONAL CAREER PROGRAM.

(a) ESTABLISHMENT.—There is established in the Department an acquisition professional career program to develop a cadre of acquisition professionals within the Department.

(b) ADMINISTRATION.—The Under Secretary for Management shall administer the acquisition professional career program established pursuant to subsection (a).

(c) 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 such 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 such 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.

(d) REPORTS.—Not later than one year after the date of the enactment of this section, 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 such 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 such 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 such components or offices.

(5) Program attrition rates and post-program graduation retention data, including information on how such 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.

(e) DEFINITIONS.—In this section:

(1) HISPANIC-SERVING INSTITUTION.—The term "Hispanic-serving institution" has the meaning given such term in section 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(2) of Higher Education Act of 1965 (20 U.S.C. 1061(2)).

(3) INSTITUTION OF HIGHER EDUCATION.—The term "institution of higher education" has the meaning given such term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

Subtitle A—Coordination with Non-Federal Entities

SEC. 801. [6 U.S.C. 361] OFFICE FOR STATE AND LOCAL GOVERNMENT COORDINATION.

(a) ESTABLISHMENT.—There is established within the Office of the Secretary the Office for State and Local Government Coordination, to oversee and coordinate departmental programs for and relationships with State and local governments.

(b) RESPONSIBILITIES.—The Office established under subsection (a) 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.

Subtitle B—Inspector General

[SEC. 811. REPEALED]

* * * * * * *

SEC. 812. LAW ENFORCEMENT POWERS OF INSPECTOR GENERAL AGENTS.

(a)

* * * * * * *

(b) [5 U.S.C. app. 6 note] PROMULGATION OF INITIAL GUIDELINES.—

(1) DEFINITION.—In this subsection, the term "memoranda of understanding" means the agreements between the Department of Justice and the Inspector General offices described under section 6(e)(3) of the Inspector General Act of 1978 (5 U.S.C. App.) (as added by subsection (a) of this section) that—

(A) are in effect on the date of enactment of this Act; and

(B) authorize such offices to exercise authority that is the same or similar to the authority under section 6(e)(1) of such Act.

(2) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall promulgate guidelines under section 6(e)(4) of the Inspector General Act of 1978 (5 U.S.C. App.) (as added by subsection (a) of this section) applicable to the Inspector General offices described under section 6(e)(3) of that Act.

(3) MINIMUM REQUIREMENTS.—The guidelines promulgated under this subsection shall include, at a minimum, the operational and training requirements in the memoranda of understanding.

(4) NO LAPSE OF AUTHORITY.—The memoranda of understanding in effect on the date of enactment of this Act shall remain in effect until the guidelines promulgated under this subsection take effect.

(c) [5 U.S.C. app. 6 note] EFFECTIVE DATES.—

(1) IN GENERAL.—Subsection (a) shall take effect 180 days after the date of enactment of this Act.

(2) INITIAL GUIDELINES.—Subsection (b) shall take effect on the date of enactment of this Act.

Subtitle C—United States Secret Service

SEC. 821. [6 U.S.C. 381] FUNCTIONS TRANSFERRED.

In accordance with title XV, there shall be transferred to the Secretary the functions, personnel, assets, and obligations of the United States Secret Service, which shall be maintained as a distinct entity within the Department, including the functions of the Secretary of the Treasury relating thereto.

SEC. 822. [6 U.S.C. 383] NATIONAL COMPUTER FORENSICS INSTITUTE.

(a) IN GENERAL; MISSION.—There is authorized for fiscal years 2023 through 2028 within the United States Secret Service a National Computer Forensics Institute (in this section referred to as the "Institute"). The Institute's mission shall be to educate, train, and equip State, local, territorial, and Tribal law enforcement officers, prosecutors, and judges, as well as participants in the United States 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 crimes, 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.

(b) CURRICULUM.—In furtherance of subsection (a), 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 subsection (a) shall relate to the following:

(1) 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.

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

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

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

(c) 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 subsection (a). When selecting participants for such 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.

(d) EQUIPMENT.—The Institute may provide recipients of education and training provided pursuant to subsection (a) 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.

(e) 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 subsection (a) educated and trained by the Institute.

(f) SAVINGS PROVISION.—All authorized activities and functions carried out by the Institute at any location as of the day before the date of the enactment of this section are authorized to continue to be carried out at any such location on and after such date.

(g) 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 subsection (a).

(h) ANNUAL REPORTS TO CONGRESS.—

(1) IN GENERAL.—The Secretary shall include in the annual report required under section 1116 of title 31, United States Code, information regarding the activities of the Institute, including, where possible, the following:

(A) An identification of jurisdictions with recipients of the education and training provided pursuant to subsection (a) during such year.

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

(C) Any information regarding projected future demand for the education and training provided pursuant to subsection (a).

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

(E) A description of the nomination process for potential recipients of the information and training provided pursuant to subsection (a).

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

(2) EXCEPTION.—Any information required under paragraph (1) that is submitted as part of the annual budget submitted by the President to Congress under section 1105 of title 31, United States Code, is not required to be included in the report required under paragraph (1).

(i) DEFINITIONS.—In this section:

(1) CYBERSECURITY THREAT.—The term "cybersecurity threat" has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

(2) INCIDENT.—The term "incident" has the meaning given such term in section 2209(a).

(3) INFORMATION SYSTEM.—The term "information system" has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501(9))).

Subtitle D—Acquisitions

SEC. 831. [6 U.S.C. 391] RESEARCH AND DEVELOPMENT PROJECTS.

(a) AUTHORITY.—Until September 30, 2024, and subject to subsection (d), the Secretary may carry out a pilot program under which the Secretary may exercise the following authorities:

(1) IN GENERAL.—When the Secretary carries out basic, applied, and advanced research and development projects, including the expenditure of funds for such projects, the Secretary may exercise the same authority (subject to the same limitations and conditions) with respect to such research and projects as the Secretary of Defense may exercise under section 4021 of title 10, United States Code (except for subsections (b) and (f)), after making a determination that the use of a contract, grant, or cooperative agreement for such project is not feasible or appropriate. The annual report required under subsection (b) of this section, as applied to the Secretary by this paragraph, shall be submitted to the President of the Senate and the Speaker of the House of Representatives.

(2) PROTOTYPE PROJECTS.—The Secretary—

(A) may, under the authority of paragraph (1), carry out prototype projects under section 4022 of title 10, United States Code; and

(B) in applying the authorities of such section 4022, the Secretary shall perform the functions of the Secretary of Defense as prescribed in such section.

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

(1) procure the temporary or intermittent services of experts or consultants (or organizations thereof) in accordance with section 3109(b) of title 5, United States Code; 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 thereof), without regard to the pay limitations of such section 3109.

(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 that is authorized to 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 such projects.

(d) DEFINITION OF NONTRADITIONAL GOVERNMENT CONTRACTOR.—In this section, the term "nontraditional Government contractor" has the same meaning as the term "nontraditional defense contractor" as defined in section 4022(e) of title 10, United States Code.

SEC. 832. [6 U.S.C. 392] PERSONAL SERVICES.

The Secretary—

(1) may procure the temporary or intermittent services of experts or consultants (or organizations thereof) in accordance with section 3109 of title 5, United States Code; 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 such section 3109.

SEC. 833. [6 U.S.C. 393] SPECIAL STREAMLINED ACQUISITION AUTHORITY.

(a) AUTHORITY.—

(1) IN GENERAL.—The Secretary may use the authorities set forth in this section with respect to any procurement made during the period beginning on the effective date of this Act and ending September 30, 2007, if the Secretary determines in writing that the mission of the Department (as described in section 101) would be seriously impaired without the use of such authorities.

(2) DELEGATION.—The authority to make the determination described in paragraph (1) may not be delegated by the Secretary to an officer of the Department who is not appointed by the President with the advice and consent of the Senate.

(3) NOTIFICATION.—Not later than the date that is 7 days after the date of any determination under paragraph (1), the Secretary shall submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate—

(A) notification of such determination; and

(B) the justification for such determination.

(b) INCREASED MICRO-PURCHASE THRESHOLD FOR CERTAIN PROCUREMENTS.—

(1) IN GENERAL.—The Secretary may designate certain employees of the Department to make procurements described in subsection (a) for which in the administration of section 32 of the Office of Federal Procurement Policy Act (41 U.S.C. 428) the amount specified in subsections (c), (d), and (f) of such section 32 shall be deemed to be $7,500.

(2) NUMBER OF EMPLOYEES.—The number of employees designated under paragraph (1) shall be—

(A) fewer than the number of employees of the Department who are authorized to make purchases without obtaining competitive quotations, pursuant to section 32(c) of the Office of Federal Procurement Policy Act (41 U.S.C. 428(c));

(B) sufficient to ensure the geographic dispersal of the availability of the use of the procurement authority under such paragraph at locations reasonably considered to be potential terrorist targets; and

(C) sufficiently limited to allow for the careful monitoring of employees designated under such paragraph.

(3) REVIEW.—Procurements made under the authority of this subsection shall be subject to review by a designated supervisor on not less than a monthly basis. The supervisor responsible for the review shall be responsible for no more than 7 employees making procurements under this subsection.

(c) SIMPLIFIED ACQUISITION PROCEDURES.—

(1) IN GENERAL.—With respect to a procurement described in subsection (a), the Secretary may deem the simplified acquisition threshold referred to in section 4(11) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(11)) to be—

(A) in the case of a contract to be awarded and performed, or purchase to be made, within the United States, $200,000; and

(B) in the case of a contract to be awarded and performed, or purchase to be made, outside of the United States, $300,000.

* * * * * * *

(d) APPLICATION OF CERTAIN COMMERCIAL ITEMS AUTHORITIES.—

(1) IN GENERAL.—With respect to a procurement described in subsection (a), the Secretary may deem any item or service to be a commercial item for the purpose of Federal procurement laws.

(2) LIMITATION.—The $5,000,000 limitation provided in section 31(a)(2) of the Office of Federal Procurement Policy Act (41 U.S.C. 427(a)(2)) and section 303(g)(1)(B) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 253(g)(1)(B)) shall be deemed to be $7,500,000 for purposes of property or services under the authority of this subsection.

(3) CERTAIN AUTHORITY.—Authority under a provision of law referred to in paragraph (2) that expires under section 4202(e) of the Clinger-Cohen Act of 1996 (divisions D and E of Public Law 104–106; 10 U.S.C. 2304 note) shall, notwithstanding such section, continue to apply for a procurement described in subsection (a).

(e) REPORT.—Not later than 180 days after the end of fiscal year 2005, the Comptroller General shall submit to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives a report on the use of the authorities provided in this section. The report shall contain the following:

(1) An assessment of the extent to which property and services acquired using authorities provided under this section contributed to the capacity of the Federal workforce to facilitate the mission of the Department as described in section 101.

(2) An assessment of the extent to which prices for property and services acquired using authorities provided under this section reflected the best value.

(3) The number of employees designated by each executive agency under subsection (b)(1).

(4) An assessment of the extent to which the Department has implemented subsections (b)(2) and (b)(3) to monitor the use of procurement authority by employees designated under subsection (b)(1).

(5) Any recommendations of the Comptroller General for improving the effectiveness of the implementation of the provisions of this section.

SEC. 834. [6 U.S.C. 394] UNSOLICITED PROPOSALS.

(a) REGULATIONS REQUIRED.—Within 1 year of the date of enactment of this Act, the Federal Acquisition Regulation shall be revised to include regulations with regard to unsolicited proposals.

(b) CONTENT OF REGULATIONS.—The regulations prescribed under subsection (a) shall require that before initiating a comprehensive evaluation, an agency contact point shall consider, among other factors, that the proposal—

(1) is not submitted in response to a previously published agency requirement; and

(2) contains technical and cost information for evaluation and overall scientific, technical or socioeconomic merit, or cost-related or price-related factors.

SEC. 835. [6 U.S.C. 395] PROHIBITION ON CONTRACTS WITH CORPORATE EXPATRIATES.

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

(b) 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 the date of enactment of this Act, 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 such expanded affiliated group.

(c) DEFINITIONS AND SPECIAL RULES.—

(1) RULES FOR APPLICATION OF SUBSECTION (b).—In applying subsection (b) for purposes of subsection (a), the following rules shall apply:

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

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

(ii) stock of such entity which is sold in a public offering related to the acquisition described in subsection (b)(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 sub-

section (b)(2) are met, such 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 such 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 (b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as I partnership.

(E) TREATMENT OF CERTAIN RIGHTS.—The Secretary shall prescribe such regulations as may be 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.

(2) 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 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting "more than 50 percent" for "at least 80 percent" each place it appears.

(3) FOREIGN INCORPORATED ENTITY.—The term "foreign incorporated entity" means any entity which is, or but for subsection (b) would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

(4) OTHER DEFINITIONS.—The terms "person", "domestic", and "foreign" have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

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

SEC. 836. [6 U.S.C. 397] 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 one-third of funds obligated in a specific fiscal year for the procurement of such covered items shall be covered items that are manufactured or supplied in the United States by entities that qualify as small business concerns, as such term is described under section 3 of the Small Business Act (15 U.S.C. 632).

(ii) Covered items may only be supplied pursuant to subparagraph (A) 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 such a covered item, including the end-item manufacturer of such 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 such a covered item with an insignia (such as any patch, badge, or emblem) and each supplier of such an insignia, if such covered item with such insignia or such insignia, as the case may be, is not produced, applied, or assembled in the United States, shall—

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

(ii) report any pilferage or theft of such covered item with such insignia or such insignia occurring at

any stage before delivery of such covered item with such insignia or such insignia; and

(iii) destroy any such defective or unusable covered item with insignia or insignia in a manner established by the Secretary, and maintain records, for three years after the creation of such records, of such destruction that include the date of such 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 such 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 such 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 one year after the date of the enactment of this section 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 such 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 the date of the enactment of this section.

Subtitle E—Human Resources Management

SEC. 841. [6 U.S.C. 411] ESTABLISHMENT OF HUMAN RESOURCES MANAGEMENT SYSTEM.

(a) AUTHORITY.—

(1) SENSE OF CONGRESS.—It is the sense of Congress that—

(A) it is extremely important that employees of the Department be allowed to participate in a meaningful way in the creation of any human resources management system affecting them;

(B) such employees have the most direct knowledge of the demands of their jobs and have a direct interest in ensuring that their human resources management system is conducive to achieving optimal operational efficiencies;

(C) the 21st century human resources management system envisioned for the Department should be one that benefits from the input of its employees; and

(D) this collaborative effort will help secure our homeland.

* * * * * * *

(b) EFFECT ON PERSONNEL.—

(1) NONSEPARATION OR NONREDUCTION IN GRADE OR COMPENSATION OF FULL-TIME PERSONNEL AND PART-TIME PERSONNEL HOLDING PERMANENT POSITIONS.—Except as otherwise provided in this Act, the transfer under this Act of full-time personnel (except special Government employees) and part-time personnel holding permanent positions shall not cause any such employee to be separated or reduced in grade or compensation for 1 year after the date of transfer to the Department.

(2) POSITIONS COMPENSATED IN ACCORDANCE WITH EXECUTIVE SCHEDULE.—Any person who, on the day preceding such person's date of transfer pursuant to this Act, held a position compensated in accordance with the Executive Schedule prescribed in chapter 53 of title 5, United States Code, and who, without a break in service, is appointed in the Department to a position having duties comparable to the duties performed immediately preceding such appointment shall continue to be compensated in such new position at not less than the rate provided for such position, for the duration of the service of such person in such new position.

(3) COORDINATION RULE.—Any exercise of authority under chapter 97 of title 5, United States Code (as amended by subsection (a)), including under any system established under

such chapter, shall be in conformance with the requirements of this subsection.

SEC. 842. [6 U.S.C. 412] LABOR-MANAGEMENT RELATIONS.

(a) LIMITATION ON EXCLUSIONARY AUTHORITY.—

(1) IN GENERAL.—No agency or subdivision of an agency which is transferred to the Department pursuant to this Act shall be excluded from the coverage of chapter 71 of title 5, United States Code, as a result of any order issued under section 7103(b)(1) of such 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 within such 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 any order to the extent that such order excludes any 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 such title 5; or

(B) any such 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 which is recognized as an appropriate unit for purposes of chapter 71 of title 5, United States Code, as of the day before the effective date of this Act (and any subdivision of any such unit) shall, if such unit (or subdivision) is transferred to the Department pursuant to this Act, continue to be so recognized for such purposes, unless—

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

(B) a majority of the employees within such 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.—No position or employee within a unit (or subdivision of a unit) as to which continued recognition is given in accordance with paragraph (1) shall be excluded from such unit (or subdivision), for purposes of chapter 71 of such title 5, unless the primary job duty of such position or employee—

(A) materially changes; and

(B) consists of intelligence, counterintelligence, or investigative work directly related to terrorism investigation.

In the case of any positions within a unit (or subdivision) which are first established on or after the effective date of this Act and any employees first appointed on or after such date, the preceding sentence shall be applied disregarding subparagraph (A).

(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 such subsections 10 days after the President has submitted to Congress a written explanation of the reasons for such determination.

(d) COORDINATION RULE.—No other provision of this Act or of any amendment made by this Act may be construed or applied in a manner so as to limit, supersede, or otherwise affect the provisions of this section, except to the extent that it does so by specific reference to this section.

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

SEC. 843. [6 U.S.C. 413] USE OF COUNTERNARCOTICS ENFORCEMENT ACTIVITIES IN CERTAIN EMPLOYEE PERFORMANCE APPRAISALS.

(a) 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 within the Department or other Federal, State, or local agencies, in counternarcotics enforcement.

(b) DEFINITIONS.—For purposes of this section—

(1) the term "National Drug Control Program Agency" means—

(A) a National Drug Control Program Agency, as defined in section 702(7) of the Office of National Drug Control Policy Reauthorization Act of 1998 (as last in effect); and

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

(i) the counternarcotics officer, appointed under section 878; or

(ii) if applicable, the counternarcotics officer's successor in function (as determined by the Secretary); and

(2) 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, United States Code, or otherwise.

SEC. 844. [6 U.S.C. 414] HOMELAND SECURITY ROTATION PROGRAM.

(a)[11] ESTABLISHMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this section, 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.

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

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

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

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

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

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

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

(G) complement and incorporate (but not replace) rotational programs within the Department in effect on the date of enactment of this section.

(3) ADMINISTRATION.—

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

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

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

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

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

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

[11] So in original. There is no subsection (b).

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

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

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

(viii) coordinate with rotational programs within the Department in effect on the date of enactment of this section.

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

(5) REPORTING.—Not later than 180 days after the date of the establishment of the Rotation Program, the Secretary shall submit a report on the status of the Rotation Program, including a description of the Rotation Program, the number of employees participating, and how the Rotation Program is used in succession planning and leadership development to the appropriate committees of Congress.

SEC. 845. [6 U.S.C. 415] HOMELAND SECURITY EDUCATION PROGRAM.

(a) ESTABLISHMENT.—The Secretary, acting through the Administrator, 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 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 National 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 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 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 any employee selected for the 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 to 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 payment, except that such 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) such other method as is provided by lay [12] for the recovery of amounts owing to the Government.

SEC. 846. [6 U.S.C. 417] 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 2209) 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—

[12] So in original. The word "lay" probably should be "law".

(A) the Agency (including the 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.

Subtitle F—Federal Emergency Procurement Flexibility

SEC. 851. [6 U.S.C. 421] DEFINITION.

In this subtitle, the term "executive agency" has the meaning given that term under section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

SEC. 852. [6 U.S.C. 422] PROCUREMENTS FOR DEFENSE AGAINST OR RECOVERY FROM TERRORISM OR NUCLEAR, BIOLOGICAL, CHEMICAL, OR RADIOLOGICAL ATTACK.

The authorities provided in this subtitle apply to any procurement of property or services by or for an executive agency that, as determined by the head of the executive agency, are to be used to facilitate defense against or recovery from terrorism or nuclear, biological, chemical, or radiological attack, but only if a solicitation of offers for the procurement is issued during the 1-year period beginning on the date of the enactment of this Act.

SEC. 853. [6 U.S.C. 423] INCREASED SIMPLIFIED ACQUISITION THRESHOLD FOR PROCUREMENTS IN SUPPORT OF HUMANITARIAN OR PEACEKEEPING OPERATIONS OR CONTINGENCY OPERATIONS.

(a) TEMPORARY THRESHOLD AMOUNTS.—For a procurement referred to in section 852 that is carried out in support of a humanitarian or peacekeeping operation or a contingency operation, the simplified acquisition threshold definitions shall be applied as if the amount determined under the exception provided for such an operation in those definitions were—

(1) in the case of a contract to be awarded and performed, or purchase to be made, inside the United States, $200,000; or

(2) in the case of a contract to be awarded and performed, or purchase to be made, outside the United States, $300,000.

(b) SIMPLIFIED ACQUISITION THRESHOLD DEFINITIONS.—In this section, the term "simplified acquisition threshold definitions" means the following:

(1) Section 134 of title 41, United States Code.

(2) Section 153 of title 41, United States Code.

(3) Section 3015 of title 10, United States Code.

(c) SMALL BUSINESS RESERVE.—For a procurement carried out pursuant to subsection (a), section 15(j) of the Small Business Act (15 U.S.C. 644(j)) shall be applied as if the maximum anticipated value identified therein is equal to the amounts referred to in subsection (a).

SEC. 854. [6 U.S.C. 424] INCREASED MICRO-PURCHASE THRESHOLD FOR CERTAIN PROCUREMENTS.

In the administration of section 32 of the Office of Federal Procurement Policy Act (41 U.S.C. 428) with respect to a procurement

referred to in section 852, the amount specified in subsections (c), (d), and (f) of such section 32 shall be deemed to be $7,500.

SEC. 855. [6 U.S.C. 425] APPLICATION OF CERTAIN COMMERCIAL ITEMS AUTHORITIES TO CERTAIN PROCUREMENTS.

(a) AUTHORITY.—

(1) IN GENERAL.—The head of an executive agency may apply the provisions of law listed in paragraph (2) to a procurement referred to in section 852 without regard to whether the property or services are commercial items.

(2) COMMERCIAL ITEM LAWS.—The provisions of law referred to in paragraph (1) are as follows:

(A) Sections 1901 and 1906 of title 41, United States Code.

(B) Section 3205 of title 10, United States Code.

(C) Section 3305 of title 41, United States Code.

(b) INAPPLICABILITY OF LIMITATION ON USE OF SIMPLIFIED ACQUISITION PROCEDURES.—

(1) IN GENERAL.—The $5,000,000 limitation provided in section 1901(a)(2) of title 41, United States Code, section 3205(a)(2) of title 10, United States Code, and section 3305(a)(2) of title 41, United States Code, shall not apply to purchases of property or services to which any of the provisions of law referred to in subsection (a) are applied under the authority of this section.

(2) OMB GUIDANCE.—The Director of the Office of Management and Budget shall issue guidance and procedures for the use of simplified acquisition procedures for a purchase of property or services in excess of $5,000,000 under the authority of this section.

(c) CONTINUATION OF AUTHORITY FOR SIMPLIFIED PURCHASE PROCEDURES.—Authority under a provision of law referred to in subsection (a)(2) that expires under section 4202(e) of the Clinger-Cohen Act of 1996 (divisions D and E of Public Law 104–106; 10 U.S.C. 2304 note) shall, notwithstanding such section, continue to apply for use by the head of an executive agency as provided in subsections (a) and (b).

SEC. 856. [6 U.S.C. 426] USE OF STREAMLINED PROCEDURES.

(a) REQUIRED USE.—The head of an executive agency shall, when appropriate, use streamlined acquisition authorities and procedures authorized by law for a procurement referred to in section 852, including authorities and procedures that are provided under the following provisions of law:

(1) FEDERAL PROPERTY AND ADMINISTRATIVE SERVICES ACT OF 1949.—In division C of subtitle I of title 41, United States Code:

(A) Paragraphs (1), (2), (6), and (7) of subsection (a) of section 3304 of such title, relating to use of procedures other than competitive procedures under certain circumstances (subject to subsection (d) of such section).

(B) Section 4106 of such title, relating to orders under task and delivery order contracts.

(2) TITLE 10, UNITED STATES CODE.—In part V of subtitle A of title 10, United States Code:

(A) Paragraphs (1), (2), (6), and (7) of subsection (a) of section 3204, relating to use of procedures other than competitive procedures under certain circumstances (subject to subsection (d) of such section).

(B) Section 3406, relating to orders under task and delivery order contracts.

(3) OFFICE OF FEDERAL PROCUREMENT POLICY ACT.—Paragraphs (1)(B), (1)(D), and (2)(A) of section 1708(b) of title 41, United Sates Code, relating to inapplicability of a requirement for procurement notice.

(b) WAIVER OF CERTAIN SMALL BUSINESS THRESHOLD REQUIREMENTS.—Subclause (II) of section 8(a)(1)(D)(i) of the Small Business Act (15 U.S.C. 637(a)(1)(D)(i)) and clause (ii) of section 31(b)(2)(A) of such Act (15 U.S.C. 657a(b)(2)(A)) shall not apply in the use of streamlined acquisition authorities and procedures referred to in paragraphs (1)(A) and (2)(A) of subsection (a) for a procurement referred to in section 852.

SEC. 857. [6 U.S.C. 427] REVIEW AND REPORT BY COMPTROLLER GENERAL.

(a) REQUIREMENTS.—Not later than March 31, 2004, the Comptroller General shall—

(1) complete a review of the extent to which procurements of property and services have been made in accordance with this subtitle; and

(2) submit a report on the results of the review to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives.

(b) CONTENT OF REPORT.—The report under subsection (a)(2) shall include the following matters:

(1) ASSESSMENT.—The Comptroller General's assessment of—

(A) the extent to which property and services procured in accordance with this title have contributed to the capacity of the workforce of Federal Government employees within each executive agency to carry out the mission of the executive agency; and

(B) the extent to which Federal Government employees have been trained on the use of technology.

(2) RECOMMENDATIONS.—Any recommendations of the Comptroller General resulting from the assessment described in paragraph (1).

(c) CONSULTATION.—In preparing for the review under subsection (a)(1), the Comptroller shall consult with the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives on the specific issues and topics to be reviewed. The extent of coverage needed in areas such as technology integration, employee training, and human capital management, as well as the data requirements of the study, shall be included as part of the consultation.

SEC. 858. [6 U.S.C. 428] IDENTIFICATION OF NEW ENTRANTS INTO THE FEDERAL MARKETPLACE.

The head of each executive agency shall conduct market research on an ongoing basis to identify effectively the capabilities, including the capabilities of small businesses and new entrants into Federal contracting, that are available in the marketplace for meeting the requirements of the executive agency in furtherance of defense against or recovery from terrorism or nuclear, biological, chemical, or radiological attack. The head of the executive agency shall, to the maximum extent practicable, take advantage of commercially available market research methods, including use of commercial databases, to carry out the research.

* * * * * * *

Subtitle G—Support Anti-terrorism by Fostering Effective Technologies Act of 2002

SEC. 861. [6 U.S.C. 101 note] SHORT TITLE.

This subtitle may be cited as the "Support Anti-terrorism by Fostering Effective Technologies Act of 2002" or the "SAFETY Act".

SEC. 862. [6 U.S.C. 441] ADMINISTRATION.

(a) IN GENERAL.—The Secretary shall be responsible for the administration of this subtitle.

(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 subtitle in accordance with criteria that shall include, but not be limited to, 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 such anti-terrorism technology.

(4) Substantial likelihood that such anti-terrorism technology will not be deployed unless protections under the system of risk management provided under this subtitle are extended.

(5) Magnitude of risk exposure to the public if such 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 such acts.

(c) REGULATIONS.—The Secretary may issue such regulations, after notice and comment in accordance with section 553 of title 5, United States Code, as may be necessary to carry out this subtitle.

SEC. 863. [6 U.S.C. 442] 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 or response or recovery from such act and such claims result or may result in loss to the Seller. The substantive law for decision in any such action shall be derived from the law, including choice of law principles, of the State in which such acts of terrorism occurred, unless such law is inconsistent with or preempted by Federal law. Such 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.—Such 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 or response or recovery from such act and such 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.—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) IN GENERAL.—Noneconomic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff, and no plaintiff may recover noneconomic damages unless the plaintiff suffered physical harm.

(B) DEFINITION.—For purposes of subparagraph (A), 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.

(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 such acts of terrorism that result 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) of this subsection, have been deployed in defense against or response or recovery from such act and such claims

result or may result in loss to the Seller, there shall be a rebuttable presumption that the government contractor defense applies in such 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 such technology under this subsection. This presumption of the government contractor 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 will be exclusively responsible for the review and approval of anti-terrorism technology for purposes of establishing a government contractor 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 or response or recovery from such act and such 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 will conduct a comprehensive review of the design of such technology and determine whether it will perform as intended, conforms to the Seller's specifications, and is safe for use as intended. The Seller will conduct safety and hazard analyses on such technology and will supply the Secretary with all such information.

(3) CERTIFICATE.—For anti-terrorism technology reviewed and approved by the Secretary, the Secretary will 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 such act of terrorism; or

(2) participates in a conspiracy to commit any such act of terrorism or any such criminal act.

SEC. 864. [6 U.S.C. 443] RISK MANAGEMENT.

(a) IN GENERAL.—

(1) LIABILITY INSURANCE REQUIRED.—Any person or entity that sells or otherwise provides a qualified anti-terrorism technology to Federal and non-Federal Government customers ("Seller") shall obtain liability insurance of such types and in such amounts as shall be required in accordance with 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 or response or recovery from such act.

(2) MAXIMUM AMOUNT.—For the total claims related to 1 such 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 pursuant to this subsection shall, in addition to the Seller, protect the following, to the extent of their potential liability for involvement in the manufacture, qualification, sale, use, or operation of qualified anti-terrorism technologies deployed in defense against or response or 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.—Such 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 or response or recovery from such act.

(c) EXTENT OF LIABILITY.—Notwithstanding any other provision of 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 or response or recovery from such act and such 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.

SEC. 865. [6 U.S.C. 444] DEFINITIONS.

For purposes of this subtitle, the following definitions apply:

(1) QUALIFIED ANTI-TERRORISM TECHNOLOGY.—For purposes of this subtitle, the term "qualified anti-terrorism technology" means any 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 such acts might otherwise cause, that is designated as such by the Secretary.

(2) ACT OF TERRORISM.—(A) The term "act of terrorism" means any act that the Secretary determines meets the re-

quirements under subparagraph (B), as such requirements are further defined and specified by the Secretary.

(B) REQUIREMENTS.—An act meets the requirements of this subparagraph if the act—

(i) is unlawful;

(ii) 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; and

(iii) 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.

(3) INSURANCE CARRIER.—The term "insurance carrier" means any corporation, association, society, order, firm, company, mutual, partnership, individual aggregation of individuals, or any other legal entity that provides commercial property and casualty insurance. Such term includes any affiliates of a commercial insurance carrier.

(4) LIABILITY INSURANCE.—

(A) IN GENERAL.—The term "liability insurance" means insurance for legal liabilities incurred by the insured resulting from—

(i) loss of or damage to property of others;

(ii) ensuing loss of income or extra expense incurred because of loss of or damage to property of others;

(iii) bodily injury (including) to persons other than the insured or its employees; or

(iv) loss resulting from debt or default of another.

(5) LOSS.—The term "loss" means death, bodily injury, or loss of or damage to property, including business interruption loss.

(6) NON-FEDERAL GOVERNMENT CUSTOMERS.—The term "non-Federal Government customers" means any customer of a Seller that is not an agency or instrumentality of the United States Government with authority under Public Law 85–804 to provide for indemnification under certain circumstances for third-party claims against its contractors, including but not limited to State and local authorities and commercial entities.

Subtitle H—Miscellaneous Provisions

SEC. 871. [6 U.S.C. 451] ADVISORY COMMITTEES.

(a) IN GENERAL.—The Secretary may establish, appoint members of, and use the services of, advisory committees, as the Secretary may deem necessary. An advisory committee established under this section may be exempted by the Secretary from chapter 10 of title 5, United States Code, but the Secretary shall publish notice in the Federal Register announcing the establishment of

such a 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, United States Code) shall be eligible for certifications under subsection (b)(3) of section 208 of title 18, United States Code, for official actions taken as a member of such advisory committee.

(b) TERMINATION.—Any 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 such determination is made. The Secretary may make any number of subsequent extensions consistent with this subsection.

SEC. 872. [6 U.S.C. 452] REORGANIZATION.

(a) REORGANIZATION.—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—

(1) pursuant to section 1502(b); or

(2) after the expiration of 60 days after providing notice of such action to the appropriate congressional committees, which shall include an explanation of the rationale for the action.

(b) LIMITATIONS.—

(1) IN GENERAL.—Authority under subsection (a)(1) does not extend to the abolition of any agency, entity, organizational unit, program, or function established or required to be maintained by this Act.

(2) ABOLITIONS.—Authority under subsection (a)(2) does not extend to the abolition of any agency, entity, organizational unit, program, or function established or required to be maintained by statute.

SEC. 873. [6 U.S.C. 453] USE OF APPROPRIATED FUNDS.

(a) DISPOSAL OF PROPERTY.—

(1) STRICT COMPLIANCE.—If specifically authorized to dispose of real property in this or any other Act, the Secretary shall exercise this authority in strict compliance with section 204 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 485).

(2) DEPOSIT OF PROCEEDS.—The Secretary shall deposit the proceeds of any exercise of property disposal authority into the miscellaneous receipts of the Treasury in accordance with section 3302(b) of title 31, United States Code.

(b) GIFTS.—Except as authorized by section 2601 of title 10, United States Code, by section 93 of title 14, United States Code, or by section 525 or 884 of this Act, 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 such appropriations Act.

(c) BUDGET REQUEST.—Under section 1105 of title 31, United States Code, the President shall submit to Congress a detailed

budget request for the Department for fiscal year 2004, and for each subsequent fiscal year.

SEC. 874. [6 U.S.C. 454] FUTURE YEAR HOMELAND SECURITY PROGRAM.

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

(b) CONTENTS.—The Future Years Homeland Security Program under subsection (a) 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, United States Code;

(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).

(c) EFFECTIVE DATE.—This section shall take effect with respect to the preparation and submission of the fiscal year 2005 budget request for the Department and for any subsequent fiscal year, except that the first Future Years Homeland Security Program shall be submitted not later than 90 days after the Department's fiscal year 2005 budget request is submitted to Congress.

SEC. 875. [6 U.S.C. 455] MISCELLANEOUS AUTHORITIES.

(a) SEAL.—The Department shall have a seal, whose design is subject to the approval of the President.

(b) PARTICIPATION OF MEMBERS OF THE ARMED FORCES.—With respect to the Department, the Secretary shall have the same authorities that the Secretary of Transportation has with respect to the Department of Transportation under section 324 of title 49, United States Code.

(c) REDELEGATION OF FUNCTIONS.—Unless otherwise provided in the delegation or by law, any function delegated under this Act may be redelegated to any subordinate.

(d) INVESTIGATION OF CERTAIN VIOLENT ACTS, SHOOTINGS, AND MASS KILLINGS.—

(1) IN GENERAL.—At the request of an appropriate law enforcement official of a State or political subdivision, the Secretary, through deployment of the Secret Service or United States 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 Federal office or employment.

(2) DEFINITIONS.—For purposes of this subsection—

(A) the term "mass killings" means 3 or more killings in a single incident; and

(B) the term "place of public use" has the meaning given that term under section 2332f(e)(6) of title 18, United States Code.

SEC. 876. [6 U.S.C. 456] MILITARY ACTIVITIES.

Nothing in this Act shall confer upon the Secretary any authority to engage in warfighting, the military defense of the United States, or other military activities, nor shall anything in this Act 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.

SEC. 877. [6 U.S.C. 457] REGULATORY AUTHORITY AND PREEMPTION.

(a) REGULATORY AUTHORITY.—Except as otherwise provided in sections 306(c), 862(c), and 1706(b), this Act vests no new regulatory authority in the Secretary or any other Federal official, and transfers to the Secretary or another Federal official only such regulatory authority as exists on the date of enactment of this Act within any agency, program, or function transferred to the Department pursuant to this Act, or that on such date of enactment is exercised by another official of the executive branch with respect to such agency, program, or function. Any such transferred authority may not be exercised by an official from whom it is transferred upon transfer of such agency, program, or function to the Secretary or another Federal official pursuant to this Act. This Act may not be construed as altering or diminishing the regulatory authority of any other executive agency, except to the extent that this Act transfers such authority from the agency.

(b) PREEMPTION OF STATE OR LOCAL LAW.—Except as otherwise provided in this Act, this Act preempts no State or local law, except that any authority to preempt State or local law vested in any Federal agency or official transferred to the Department pursuant to this Act shall be transferred to the Department effective on the date of the transfer to the Department of that Federal agency or official.

SEC. 878. [6 U.S.C. 458] OFFICE OF COUNTERNARCOTICS ENFORCEMENT.

(a) OFFICE.—There is established in the Department an Office of Counternarcotics Enforcement, which shall be headed by a Director appointed by the President.

(b) ASSIGNMENT OF PERSONNEL.—

(1) IN GENERAL.—The Secretary shall assign permanent staff to the Office, 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, any other branch of the Federal Government, any State or local government, or any sub-

division 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) within 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 Directorate of Border and Transportation Security, 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 submission by the President to Congress of any 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 such request. The review and evaluation shall—

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

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

(C) compare such 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 of 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 responsibility 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.

SEC. 879. [6 U.S.C. 459] OFFICE OF INTERNATIONAL AFFAIRS.

(a) ESTABLISHMENT.—There is established within the Office of the Secretary an Office of International Affairs. The Office shall be headed by a Director, who 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. Such 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 within the Department in coordination with other Federal officials with responsibility for counter-terrorism matters.

SEC. 880. [6 U.S.C. 460] PROHIBITION OF THE TERRORISM INFORMATION AND PREVENTION SYSTEM.

Any and all activities of the Federal Government to implement the proposed component program of the Citizen Corps known as Operation TIPS (Terrorism Information and Prevention System) are hereby prohibited.

SEC. 881. [6 U.S.C. 461] REVIEW OF PAY AND BENEFIT PLANS.

Notwithstanding any other provision of this Act, the Secretary shall, in consultation with the Director of the Office of Personnel Management, review the pay and benefit plans of each agency whose functions are transferred under this Act to the Department and, within 90 days after the date of enactment, submit a plan to the President of the Senate and the Speaker of the House of Representatives and the appropriate committees and subcommittees of Congress, for ensuring, to the maximum extent practicable, the elimination of disparities in pay and benefits throughout the Department, especially among law enforcement personnel, that are inconsistent with merit system principles set forth in section 2301 of title 5, United States Code.

SEC. 882. [6 U.S.C. 462] OFFICE FOR NATIONAL CAPITAL REGION COORDINATION.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—There is established within the Office of the Secretary the Office of National Capital Region Coordination, to oversee and coordinate 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, United States Code.

(2) DIRECTOR.—The Office established under paragraph (1) shall be headed by a Director, who shall be appointed by the Secretary.

(3) COOPERATION.—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.

(b) RESPONSIBILITIES.—The Office established under subsection (a)(1) 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.

(c) ANNUAL REPORT.—The Office established under subsection (a) 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.

(d) LIMITATION.—Nothing contained in this section shall be construed as limiting the power of State and local governments.

SEC. 883. [6 U.S.C. 463] REQUIREMENT TO COMPLY WITH LAWS PROTECTING EQUAL EMPLOYMENT OPPORTUNITY AND PROVIDING WHISTLEBLOWER PROTECTIONS.

Nothing in this Act 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 pursuant to the provisions in section 2302(b)(1) of title 5, United States Code, and the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (Public Law 107–174)); or

(2) to provide whistleblower protections for employees of the Department (including pursuant to the provisions in section 2302(b)(8) and (9) of such title and the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002).

SEC. 884. [6 U.S.C. 464] FEDERAL LAW ENFORCEMENT TRAINING CENTERS.

(a) ESTABLISHMENT.—The Secretary shall maintain in the Department the Federal Law Enforcement Training Centers (FLETC), headed by a Director, who shall report to the Secretary.

(b) POSITION.—The Director shall occupy a career-reserved position within the Senior Executive Service.

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

(1) develop training goals and establish strategic and tactical organizational program plan 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 related 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 related 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 such 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 related 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 is authorized to provide training to employees of Federal agencies who are engaged, directly or indirectly, in homeland security operations or Federal law enforcement activities, including such operations or activities related to domestic preparedness and response to threats or acts of terrorism. In carrying out such 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 such law enforcement 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, upon request, information on activities undertaken in the previous year pursuant to subparagraph (A).

(5) FLETC DETAILS TO DHS.—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, such partner organization shall reimburse FLETC for the salary equivalent for such 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 such training, unless such 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, United States Code.

(8) PROVISION OF NON-FEDERAL TRAINING.—

(A) IN GENERAL.—The Director is authorized to charge and retain fees that would pay for its 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 such training at the International Law Enforcement Academies wherever established.

(iii) Private sector security officers, participants in the Federal Flight Deck Officer program under section 44921 of title 49, United States Code, 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 so waived.

(9) REIMBURSEMENT.—The Director is authorized to reimburse travel or other expenses for non-Federal personnel who attend activities related to training sponsored by FLETC, at travel and per diem rates established by the General Services Administration.

(10) STUDENT SUPPORT.—In furtherance of its training mission, the Director is authorized to 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 any other provision of law, the Director is authorized to 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 the provisions of section 8344 or 8468 of title 5, United States Code, or 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, United States Code, 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 which would result in the displacement of any employee.

(12) TRAVEL FOR INTERMITTENT EMPLOYEES.—The Director is authorized to reimburse intermittent Federal employees traveling from outside a commuting distance (to be predetermined by the Director) for travel expenses.

(e) ON-FLETC HOUSING.—Notwithstanding any other provision of law, 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.—In order to further the goals and objectives of FLETC, the Director is authorized to—

(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 to 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 such fiscal year;

(5) in accordance with the purchasing authority provided under section 505 of the Department of Homeland Security Appropriations Act, 2004 (Public Law 108–90; 6 U.S.C. 453a)—

(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 FLETC graduates who have died in the line of duty.

(g) 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 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 the Federal Law Enforcement Training Centers.

(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 such term in section 2105 of title 5, United States Code.

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

(A) an Executive Department as defined in section 101 of title 5, United States Code;

(B) an independent establishment as defined in section 104 of title 5, United States Code;

(C) a Government corporation as defined in section 9101 of title 31, United States Code;

(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 criminal investigators (commonly known as "agents") and uniformed police (commonly known as "officers"), who has statutory authority to search, seize, make arrests, or to 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, any agency or instrumentality of a local government, or any 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 any Federal agency participating in FLETC's training programs under a formal memorandum of understanding.

(10) STATE.—The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of 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.

(h) 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 such purpose.

SEC. 885. [6 U.S.C. 465] JOINT INTERAGENCY TASK FORCE.

(a) ESTABLISHMENT.—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.

(b) STRUCTURE.—It is the sense of Congress that the Secretary should model the Joint Interagency Homeland Security Task Force on the approach taken by the Joint Interagency Task Forces for drug interdiction at Key West, Florida and Alameda, California, to the maximum extent feasible and appropriate.

SEC. 886. [6 U.S.C. 466] SENSE OF CONGRESS REAFFIRMING THE CONTINUED IMPORTANCE AND APPLICABILITY OF THE POSSE COMITATUS ACT.

(a) FINDINGS.—Congress finds the following:

(1) Section 1385 of title 18, United States Code (commonly known as the "Posse Comitatus Act"), prohibits the use of the Armed Forces as a posse comitatus to execute the laws except in cases and under circumstances expressly authorized by the Constitution or Act of Congress.

(2) Enacted in 1878, the Posse Comitatus Act was expressly intended to prevent United States Marshals, on their own initiative, from calling on the Army for assistance in enforcing Federal law.

(3) The Posse Comitatus Act has served the Nation well in limiting the use of the Armed Forces to enforce the law.

(4) Nevertheless, by its express terms, the Posse Comitatus Act is not a complete barrier to the use of the Armed Forces for a range of domestic purposes, including law enforcement functions, when the use of the Armed Forces is author-

ized by Act of Congress or the President determines that the use of the Armed Forces is required to fulfill the President's obligations under the Constitution to respond promptly in time of war, insurrection, or other serious emergency.

(5) Existing laws, including chapter 13 of title 10, United States Code (commonly known as the "Insurrection Act"), and the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.), grant the President broad powers that may be invoked in the event of domestic emergencies, including an attack against the Nation using weapons of mass destruction, and these laws specifically authorize the President to use the Armed Forces to help restore public order.

(b) SENSE OF CONGRESS.—Congress reaffirms the continued importance of section 1385 of title 18, United States Code, and it is the sense of Congress that nothing in this Act should be construed to alter the applicability of such section to any use of the Armed Forces as a posse comitatus to execute the laws.

SEC. 887. [6 U.S.C. 467] COORDINATION WITH THE 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 in accordance with 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 of Homeland Security, 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 of Homeland Security, 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.

SEC. 888. [6 U.S.C. 468] PRESERVING COAST GUARD MISSION PERFORMANCE.

(a) DEFINITIONS.—In this section:

(1) NON-HOMELAND SECURITY MISSIONS.—The term "non-homeland security missions" means the following missions of the Coast Guard:

(A) Marine safety.

(B) Search and rescue.

(C) Aids to navigation.

(D) Living marine resources (fisheries law enforcement).

(E) Marine environmental protection.

(F) Ice operations.

(2) HOMELAND SECURITY MISSIONS.—The term "homeland security missions" means the following missions of the Coast Guard:

(A) Ports, waterways and coastal security.

(B) Drug interdiction.

(C) Migrant interdiction.

(D) Defense readiness.

(E) Other law enforcement.

(b) TRANSFER.—There are transferred to the Department the authorities, functions, personnel, and assets of the Coast Guard, which shall be maintained as a distinct entity within the Department, including the authorities and functions of the Secretary of Transportation relating thereto.

(c) MAINTENANCE OF STATUS OF FUNCTIONS AND ASSETS.—Notwithstanding any other provision of this Act, the authorities, functions, and capabilities of the Coast Guard to perform its missions shall be maintained intact and without significant reduction after the transfer of the Coast Guard to the Department, except as specified in subsequent Acts.

(d) CERTAIN TRANSFERS PROHIBITED.—No mission, function, or asset (including for purposes of this subsection any ship, aircraft, or helicopter) of the Coast Guard may be diverted to the principal and continuing use of any other 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.

(e) 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 subsequent Acts.

(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 such 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.

(f) DIRECT REPORTING TO SECRETARY.—Upon the transfer of the Coast Guard to the Department, the Commandant shall report directly to the Secretary without being required to report through any other official of the Department.

(g) 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 3 of title 14, United States Code.

SEC. 889. HOMELAND SECURITY FUNDING ANALYSIS IN PRESIDENT'S BUDGET.

(a)

* * * * * * *

(c) [31 U.S.C. 1105 note] EFFECTIVE DATE.—This section and the amendment made by this section shall apply beginning with respect to the fiscal year 2005 budget submission.

* * * * * * *

SEC. 890A. [6 U.S.C. 473] CYBER CRIMES CENTER, CHILD EXPLOITATION INVESTIGATIONS UNIT, COMPUTER FORENSICS UNIT, AND CYBER CRIMES UNIT.

(a) CYBER CRIMES CENTER.—

(1) IN GENERAL.—The Secretary shall operate, within United States Immigration and Customs Enforcement, Homeland Security Investigations, a Cyber Crimes Center (referred to in this section 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, within the Center, a Child Exploitation Investigations Unit (referred to in this subsection as the "CEIU").

(2) FUNCTIONS.—The CEIU—

(A) shall coordinate all United States 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, upon 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 Forces;

(D) shall provide psychological support and counseling services for United States 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) is authorized to 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 United States Immigration and Customs Enforcement;

(B) the number of arrests by United States Immigration and Customs Enforcement in child exploitation investigations, disaggregated by type, including—

(i) the number of child victims identified through investigations carried out by United States 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 United States 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 is authorized to enter into cooperative agreements to accomplish the functions set forth in paragraphs (2) and (3).

(6) ACCEPTANCE OF GIFTS.—

(A) IN GENERAL.—The Secretary is authorized to accept monies 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) shall not be subject to the Federal Acquisition Regulation for competition when the services provided by the entities referred to in such subparagraph are donated or of minimal cost to the Department.

(7) REPORTS.—Not later than 1 year after the date of the enactment of the HERO Act of 2015, and annually for the following 4 years, 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, within the Center, a Computer Forensics Unit (referred to in this subsection 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) United States 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, upon request and subject to the availability of funds;

(B) shall provide computer hardware, software, and forensic licenses for all computer forensics personnel within United States 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) is authorized to 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 is authorized to enter into cooperative agreements to accomplish the functions set forth in paragraph (2).

(4) ACCEPTANCE OF GIFTS.—

(A) IN GENERAL.—The Secretary is authorized to accept monies and in-kind donations from the Virtual Global Task Force, national laboratories, Federal agencies, not-for-profit organizations, and educational institutions to cre-

ate and expand public awareness campaigns in support of the functions of the CFU.

(B) EXEMPTION FROM FEDERAL ACQUISITION REGULATION.—Gifts authorized under subparagraph (A) shall not be subject to the Federal Acquisition Regulation for competition when the services provided by the entities referred to in such subparagraph are donated or of minimal cost to the Department.

(d) CYBER CRIMES UNIT.—

(1) IN GENERAL.—The Secretary shall operate, within the Center, a Cyber Crimes Unit (referred to in this subsection as the "CCU").

(2) FUNCTIONS.—The CCU—

(A) shall oversee the cyber security strategy and cyber-related operations and programs for United States Immigration and Customs Enforcement;

(B) shall enhance United States 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) United States 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, upon 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) is authorized to 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 is authorized to enter into cooperative agreements to accomplish the functions set forth in paragraph (2).

(e) HERO CHILD-RESCUE CORPS.—

(1) ESTABLISHMENT.—

(A) IN GENERAL.—There is established within the Center a Human Exploitation Rescue Operation Child-Rescue Corps Program (referred to in this section 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, including in investigative, intelligence, analyst, inspection, and forensic positions or any other positions determined appropriate by the employing agency.

(3) FUNCTIONS.—The HERO Child-Rescue Program shall—

(A) provide, recruit, train, and equip participants of the 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 of the 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 within 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 within 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 assign-

ments 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 upon 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 CORPS HIRING.—The Secretary shall establish within Homeland Security Investigations positions, which shall be in addition to any positions in existence on the date of enactment of this subsection, 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 amount made available pursuantto paragraph (1) in each of fiscal years 2022 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).

SEC. 890B. [6 U.S.C. 474] HOMELAND SECURITY CRITICAL DOMAIN RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—

(1) RESEARCH AND DEVELOPMENT.—The Secretary is authorized to 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 of such 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

such domain. Such 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 within the supply chains of such domains.

(vi) The degree to which the conditions referred to in clauses (i) through (v) would place such 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) of this paragraph, respectively, the Secretary may conduct additional research into those critical domains, or specific elements thereof, 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 such a domain. For each such high-risk domain, or element thereof, such research shall—

(i) describe the underlying infrastructure and processes;

(ii) analyze present and projected performance of industries that comprise or support such domain;

(iii) examine the extent to which the supply chain of a product or service necessary to such 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 such 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 such other industries;

(v) consider each such domain's performance capacities in stable economic environments, adversarial supply conditions, and under crisis economic constraints;

(vi) identify and define needs and requirements to establish supply resiliency within each such domain; and

(vii) consider the effects of sector consolidation, including foreign consolidation, either through mergers or acquisitions, or due to recent geographic realignment, on such industries' performances.

(3) CONSULTATION.—In conducting the research under paragraph (1) and subparagraph (B) of paragraph (2), the Sec-

retary may consult with appropriate Federal agencies, State agencies, and private sector stakeholders.

(4) PUBLICATION.—Beginning one year after the date of the enactment of this section, the Secretary shall publish a report containing information relating to the research under paragraph (1) and subparagraph (B) of paragraph (2), including findings, evidence, analysis, and recommendations. Such report shall be updated annually through 2026.

(b) SUBMISSION TO CONGRESS.—Not later than 90 days after the publication of each report required under paragraph (4) of subsection (a), 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 each such report, together with a description of actions the Secretary, in consultation with appropriate Federal agencies, will undertake or has undertaken in response to each such report.

(c) DEFINITIONS.—In this section:

(1) 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.

(2) 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.

(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $1,000,000 for each of fiscal years 2022 through 2026 to carry out this section.

SEC. 890C. [6 U.S.C. 475] 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 such a 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 such foreign law enforcement unit has committed a gross violation of human

rights, consistent with the limitations set forth in section 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 who 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 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), 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 is authorized to 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 the date of the enactment of this section, 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 such members, disaggregated by country;

(3) relevant enforcement statistics, such as arrests and progress made on joint investigations, in each such 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.

SEC. 890D. [6 U.S.C. 475a] MENTOR-PROTÉGÉ PROGRAM.

(a) ESTABLISHMENT.—There is established in the Department a mentor-protégé program (in this section referred to as the "Program") under which a mentor firm enters into an agreement with a protégé firm for the purpose of assisting the protégé firm to compete for prime contracts and subcontracts of the Department.

(b) ELIGIBILITY.—The Secretary shall establish criteria for mentor firms and protégé 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.

(c) 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 protégé 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 protégé 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 protégé 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 such action is in the best interest of the Department.

(d) PROGRAM DURATION.—A mentor firm and protégé firm approved under subsection (c) shall enter into an agreement to participate in the Program for a period of not less than 36 months.

(e) PROGRAM BENEFITS.—A mentor firm and protégé firm that enter into an agreement under subsection (d) 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

protégé 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 such protégé firm.

(3) A protégé firm may receive technical, managerial, financial, or any other mutually agreed upon benefit from a mentor firm, including a subcontract award.

(f) REPORTING.—Not later than one year after the date of the enactment of this section 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 protégé firm entered into under this section, including the number of protégé 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 protégé firms;

(3) identifies contracts within the Department in which a mentor firm serving as the prime contractor provided subcontracts to a protégé firm under the Program; and

(4) assesses the degree to which there has been—

(A) an increase in the technical capabilities of protégé firms; and

(B) an increase in the quantity and estimated value of prime contract and subcontract awards to protégé firms for the period covered by the report.

(g) 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 (h)) conflicts with any other provision of law, regulation, or policy, this section shall control.

(h) 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" in section 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 protégé 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 in section 317 of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

(4) PROTÉGÉ FIRM.—The term "protégé 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 small business concern owned and controlled by women" have the meanings given such terms, respectively, under section 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 such term in section 8(d)(3)(C) of the Small Business Act (15 U.S.C. 637(d)(3)(C)).

Subtitle I—Information Sharing

SEC. 891. [6 U.S.C. 481] SHORT TITLE; FINDINGS; AND SENSE OF CONGRESS.

(a) SHORT TITLE.—This subtitle may be cited as the "Homeland Security Information Sharing Act".

(b) FINDINGS.—Congress finds the following:

(1) The Federal Government is required by the Constitution to provide for the common defense, which includes terrorist attack.

(2) The Federal Government relies on State and local personnel to protect against terrorist attack.

(3) The Federal Government collects, creates, manages, and protects classified and sensitive but unclassified information to enhance homeland security.

(4) Some homeland security information is needed by the State and local personnel to prevent and prepare for terrorist attack.

(5) The needs of State and local personnel to have access to relevant homeland security information to combat terrorism must be reconciled with the need to preserve the protected sta-

tus of such information and to protect the sources and methods used to acquire such information.

(6) Granting security clearances to certain State and local personnel is one way to facilitate the sharing of information regarding specific terrorist threats among Federal, State, and local levels of government.

(7) Methods exist to declassify, redact, or otherwise adapt classified information so it may be shared with State and local personnel without the need for granting additional security clearances.

(8) State and local personnel have capabilities and opportunities to gather information on suspicious activities and terrorist threats not possessed by Federal agencies.

(9) The Federal Government and State and local governments and agencies in other jurisdictions may benefit from such information.

(10) Federal, State, and local governments and intelligence, law enforcement, and other emergency preparation and response agencies must act in partnership to maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks.

(11) Information systems, including the National Law Enforcement Telecommunications System and the Terrorist Threat Warning System, have been established for rapid sharing of classified and sensitive but unclassified information among Federal, State, and local entities.

(12) Increased efforts to share homeland security information should avoid duplicating existing information systems.

(c) SENSE OF CONGRESS.—It is the sense of Congress that Federal, State, and local entities should share homeland security information to the maximum extent practicable, with special emphasis on hard-to-reach urban and rural communities.

SEC. 892. [6 U.S.C. 482] FACILITATING HOMELAND SECURITY INFORMATION SHARING PROCEDURES.

(a) PROCEDURES FOR DETERMINING EXTENT OF SHARING OF HOMELAND SECURITY INFORMATION.—

(1) 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 such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.

(2) The President shall ensure that such procedures apply to all agencies of the Federal Government.

(3) Such procedures shall not change the substantive requirements for the classification and safeguarding of classified information.

(4) Such procedures shall not change the requirements and authorities to protect sources and methods.

(b) PROCEDURES FOR SHARING OF HOMELAND SECURITY INFORMATION.—

(1) 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 such information may be shared, as determined in accordance with subsection (a), together with assessments of the credibility of such information.

(2) 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 such information;

(C) be configured to allow the efficient and effective sharing of information; and

(D) be accessible to appropriate State and local personnel.

(3) The procedures prescribed under paragraph (1) shall establish conditions on the use of information shared under paragraph (1)—

(A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose;

(B) to ensure the security and confidentiality of such information;

(C) to protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(4) The procedures prescribed under paragraph (1) shall ensure, to the greatest extent practicable, that the information sharing system through which information is shared under such paragraph include existing information sharing systems, including, but not limited to, the National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation.

(5) 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 such paragraph.

(6) The procedures prescribed under paragraph (1) shall ensure that appropriate State and local personnel are authorized to use such information sharing systems—

(A) to access information shared with such personnel; and

(B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.

(7) Under procedures prescribed jointly by the Director of Central 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 such information with existing intelligence.

(c) SHARING OF CLASSIFIED INFORMATION AND SENSITIVE BUT UNCLASSIFIED INFORMATION WITH STATE AND LOCAL PERSONNEL.—

(1) 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 (a).

(2) It is the sense of Congress that such procedures may include 1 or more of the following means:

(A) Carrying out security clearance investigations with respect to appropriate State and local personnel.

(B) With respect to information that is sensitive but unclassified, entering into nondisclosure agreements with appropriate State and local personnel.

(C) Increased use of information-sharing partnerships that include appropriate State and local personnel, such as the Joint Terrorism Task Forces of the Federal Bureau of Investigation, the Anti-Terrorism Task Forces of the Department of Justice, and regional Terrorism Early Warning Groups.

(3)(A) The Secretary shall establish a program to provide appropriate training to officials described in subparagraph (B) in order to assist such officials in—

(i) identifying sources of potential terrorist threats through such methods as the Secretary determines appropriate;

(ii) reporting information relating to such 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) 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) 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) The Secretary shall carry out this paragraph in consultation with the Director of Central Intelligence and the Attorney General.

(d) RESPONSIBLE OFFICIALS.—For each affected Federal agency, the head of such agency shall designate an official to administer this Act with respect to such agency.

(e) 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 such a government to disclose information shall not apply to such information.

(f) DEFINITIONS.—As used in this section:

(1) The term "homeland security information" means any 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) The term "intelligence community" has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(3) The term "State and local personnel" means any of the following persons involved in prevention, preparation, or response for 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 pursuant to this section.

(4) The term "State" includes the District of Columbia and any commonwealth, territory, or possession of the United States.

(g) CONSTRUCTION.—Nothing in this Act shall be construed as authorizing any department, bureau, agency, officer, or employee of the Federal Government to request, receive, or transmit to any other Government entity or personnel, or transmit to any State or local entity or personnel otherwise authorized by this Act to receive

homeland security information, any information collected by the Federal Government solely for statistical purposes in violation of any other provision of law relating to the confidentiality of such information.

SEC. 893. [6 U.S.C. 483] REPORT.

(a) REPORT REQUIRED.—Not later than 12 months after the date of the enactment of this Act, the President shall submit to the congressional committees specified in subsection (b) a report on the implementation of section 892. The report shall include any recommendations for additional measures or appropriation requests, beyond the requirements of section 892, to increase the effectiveness of sharing of information between and among Federal, State, and local entities.

(b) SPECIFIED CONGRESSIONAL COMMITTEES.—The congressional committees referred to in subsection (a) are the following committees:

(1) The Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives.

(2) The Select Committee on Intelligence and the Committee on the Judiciary of the Senate.

SEC. 894. [6 U.S.C. 484] AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated such sums as may be necessary to carry out section 892.

SEC. 895. [6 U.S.C. 484a] RECIPROCAL INFORMATION SHARING.

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 such terms are defined in section 111 of the Adam Walsh Child Protection and Safety Act of 2006 (34 U.S.C. 20911)) to a foreign government upon the request of the foreign government, and may receive comparable information from the foreign government.

Subtitle J—Secure Handling of Ammonium Nitrate

SEC. 899A. [6 U.S.C. 488] DEFINITIONS.

In this subtitle:

(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) any mixture containing a percentage of ammonium nitrate that is equal to or greater than the percentage determined by the Secretary under section 899B(b).

(2) AMMONIUM NITRATE FACILITY.—The term "ammonium nitrate facility" means any 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 any person who purchases ammonium nitrate from an ammonium nitrate facility.

SEC. 899B. [6 U.S.C. 488a] 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 subtitle to prevent the misappropriation or use of ammonium nitrate in an act of terrorism. Such regulations shall be carried out by the Cybersecurity and Infrastructure Security Agency.

(b) AMMONIUM NITRATE MIXTURES.—Not later than 90 days after the date of the enactment of this subtitle, 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) REGISTRATION.—The Secretary shall establish a process by which any 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 subtitle.

(2) REGISTRATION INFORMATION.—Any 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 such facility, for purposes of this subtitle; and

(C) such other information as the Secretary may determine is appropriate.

(d) REGISTRATION OF AMMONIUM NITRATE PURCHASERS.—

(1) REGISTRATION.—The Secretary shall establish a process by which any 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 subtitle.

(2) REGISTRATION INFORMATION.—Any 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 two-year period beginning on the date of that sale or transfer; and

(B) include in such 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 in accordance with paragraph (1), the owner of an ammonium nitrate facility shall take reasonable actions to ensure the protection of the information included in such records.

(f) EXEMPTION FOR EXPLOSIVE PURPOSES.—The Secretary may exempt from this subtitle 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, United States Code.

(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, United States Code, 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 subtitle.

(2) EXCEPTION.—The Secretary may disclose any information obtained by the Secretary under this subtitle to—

(A) an officer or employee of the United States, or a person that has entered into a contract with the United States, who has a need to know the information to perform the duties of the officer, employee, or person; or

(B) to a State agency under section 899D, under appropriate arrangements to ensure the protection of the information.

(i) REGISTRATION PROCEDURES AND CHECK OF TERRORIST SCREENING DATABASE.—

(1) REGISTRATION PROCEDURES.—

(A) GENERALLY.—The Secretary shall establish procedures to efficiently receive applications for registration numbers under this subtitle, conduct the checks required under paragraph (2), and promptly issue or deny a registration number.

(B) INITIAL SIX-MONTH REGISTRATION PERIOD.—The Secretary shall take steps to maximize the number of registration applications that are submitted and processed during the six-month period described in section 899F(e).

(2) CHECK OF TERRORIST SCREENING DATABASE.—

(A) CHECK REQUIRED.—The Secretary shall conduct a check of appropriate identifying information of any 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 subtitle.

(3) EXPEDITED REVIEW OF APPLICATIONS.—

(A) IN GENERAL.—Following the six-month period described in section 899F(e), the Secretary shall, to the extent practicable, issue or deny registration numbers under this subtitle 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) APPEALS PROCESS.—The Secretary shall establish an expedited appeals process for persons denied a registration number under this subtitle.

(ii) TIME PERIOD FOR RESOLUTION.—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 subtitle.

(5) RESTRICTIONS ON USE AND MAINTENANCE OF INFORMATION.—

(A) IN GENERAL.—Any 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 any other provision of this subtitle, the Secretary may share any such 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 subtitle to submit such information as may be necessary to carry out the requirements of this section.

(B) REQUIREMENT TO UPDATE INFORMATION.—The Secretary may require persons issued a registration under this subtitle to update registration information submitted to the Secretary under this subtitle, as appropriate.

(7) RE-CHECKS AGAINST TERRORIST SCREENING DATABASE.—

(A) RE-CHECKS.—The Secretary shall, as appropriate, recheck persons provided a registration number pursuant to this subtitle against the terrorist screening database of the Department, and may revoke such registration number if the Secretary determines such 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 such person shall have an opportunity to appeal, as provided in paragraph (4).

SEC. 899C. [6 U.S.C. 488b] 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 subtitle or for the purpose of deterring or preventing the misappropriation or use of ammonium nitrate in an act of terrorism.

SEC. 899D. [6 U.S.C. 488c] 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 the provisions of this subtitle; 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 subtitle.

(b) DELEGATION.—

(1) AUTHORITY.—The Secretary may delegate to a State the authority to assist the Secretary in the administration and enforcement of this subtitle.

(2) DELEGATION REQUIRED.—At the request of a Governor of a State, the Secretary shall delegate to that State the au-

thority to carry out functions under sections 899B and 899C, if the Secretary determines that the State is capable of satisfactorily carrying out such 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 899B(c)(1) 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 any 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 OF MATERIALS.—Materials made available under subparagraph (A) shall be designed to notify prospective ammonium nitrate purchasers of—

(i) the record-keeping requirements under section 899B; and

(ii) the penalties for violating such requirements.

SEC. 899E. [6 U.S.C. 488d] THEFT REPORTING REQUIREMENT.

Any person who is required to comply with section 899B(e) who has knowledge of the theft or unexplained loss of ammonium nitrate shall report such theft or loss to the appropriate Federal law enforcement authorities not later than 1 calendar day of the date on which the person becomes aware of such theft or loss. Upon receipt of such report, the relevant Federal authorities shall inform State, local, and tribal law enforcement entities, as appropriate.

SEC. 899F. [6 U.S.C. 488e] PROHIBITIONS AND PENALTY.

(a) PROHIBITIONS.—

(1) TAKING POSSESSION.—No person shall purchase ammonium nitrate from an ammonium nitrate facility unless such person is registered under subsection (c) or (d) of section 899B,

or is an agent of a person registered under subsection (c) or (d) of that section.

(2) TRANSFERRING POSSESSION.—An owner of an ammonium nitrate facility shall not transfer possession of ammonium nitrate from the ammonium nitrate facility to any ammonium nitrate purchaser who is not registered under subsection (c) or (d) of section 899B, or to any agent acting on behalf of an ammonium nitrate purchaser when such purchaser is not registered under subsection (c) or (d) of section 899B.

(3) OTHER PROHIBITIONS.—No person shall—

(A) purchase ammonium nitrate without a registration number required under subsection (c) or (d) of section 899B;

(B) own or operate an ammonium nitrate facility without a registration number required under section 899B(c); or

(C) fail to comply with any requirement or violate any other prohibition under this subtitle.

(b) CIVIL PENALTY.—A person that violates this subtitle 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 such person to do business; and

(3) any other matter that the Secretary determines that justice requires.

(d) NOTICE AND OPPORTUNITY FOR A HEARING.—No civil penalty may be assessed under this subtitle 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 subtitle.

SEC. 899G. [6 U.S.C. 488f] PROTECTION FROM CIVIL LIABILITY.

(a) IN GENERAL.—Notwithstanding any other provision of law, an owner of an ammonium nitrate facility that in good faith refuses to sell or transfer ammonium nitrate to any 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, United States Code), 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 a person 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 race, sex, national origin, creed, religion, status as a veteran, or status as a member of the Armed Forces of the United States of that person.

SEC. 899H. [6 U.S.C. 488g] PREEMPTION OF OTHER LAWS.

(a) OTHER FEDERAL REGULATIONS.—Except as provided in section 899G, nothing in this subtitle affects any regulation issued by any agency other than an agency of the Department.

(b) STATE LAW.—Subject to section 899G, this subtitle preempts the laws of any State to the extent that such laws are inconsistent with this subtitle, except that this subtitle 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.

SEC. 899I. [6 U.S.C. 488h] DEADLINES FOR REGULATIONS.

The Secretary—

(1) shall issue a proposed rule implementing this subtitle not later than 6 months after the date of the enactment of this subtitle; and

(2) issue a final rule implementing this subtitle not later than 1 year after such date of enactment.

SEC. 899J. [6 U.S.C. 488i] AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Secretary—

(1) $2,000,000 for fiscal year 2008; and

(2) $10,750,000 for each of fiscal years 2009 through 2012.

TITLE IX—NATIONAL HOMELAND SECURITY COUNCIL

SEC. 901. [6 U.S.C. 491] NATIONAL HOMELAND SECURITY COUNCIL.

There is established within the Executive Office of the President a council to be known as the "Homeland Security Council" (in this title referred to as the "Council").

SEC. 902. [6 U.S.C. 492] FUNCTION.

The function of the Council shall be to advise the President on homeland security matters.

SEC. 903. [6 U.S.C. 493] MEMBERSHIP.

(a) MEMBERS— [13] The members of the Council shall be the following:

(1) The President.

(2) The Vice President.

(3) The Secretary of Homeland Security.

(4) The Attorney General.

(5) The Secretary of Defense.

[13] A period probably should appear prior to the dash in the heading for subsection (a) of section 903.

(6) Such other individuals as 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 Council and subject to the direction of the President, attend and participate in meetings of the Council.

SEC. 904. [6 U.S.C. 494] OTHER FUNCTIONS AND ACTIVITIES.

For the purpose of more effectively coordinating the policies and functions of the United States Government relating to homeland security, the Council shall—

(1) assess the objectives, commitments, and risks of the United States in the interest of homeland security and to make resulting recommendations to the President;

(2) oversee and review homeland security policies of the Federal Government and to make resulting recommendations to the President; and

(3) perform such other functions as the President may direct.

SEC. 905. [6 U.S.C. 495] STAFF COMPOSITION.

The Council shall have a staff, the head of which shall be a civilian Executive Secretary, who shall be appointed by the President. The President is authorized to 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.

SEC. 906. [6 U.S.C. 496] RELATION TO THE 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.

TITLE X—INFORMATION SECURITY

SEC. 1001. INFORMATION SECURITY.

(a) [6 U.S.C. 101 note] SHORT TITLE.—This title may be cited as the "Federal Information Security Management Act of 2002".

(b) [Omitted-amends another Act]

(c) [6 U.S.C. 511] INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES.—

(1) NATIONAL SECURITY RESPONSIBILITIES.—(A) Nothing in this Act (including any amendment made by this Act) 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)(5) of title 44, United States Code.

(B) [Omitted-amends another Act]

(2) ATOMIC ENERGY ACT OF 1954.—Nothing in this Act shall supersede any requirement made by or under the Atomic En-

ergy 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.).

* * * * * * *

SEC. 1006. [6 U.S.C. 512] CONSTRUCTION.

Nothing in this Act, or the amendments made by this Act, 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)).

TITLE XI—DEPARTMENT OF JUSTICE DIVISIONS

Subtitle A—Executive Office for Immigration Review

SEC. 1101. LEGAL STATUS OF EOIR.

(a) [6 U.S.C. 521] EXISTENCE OF EOIR.—There is in the Department of Justice the Executive Office for Immigration Review, which shall be subject to the direction and regulation of the Attorney General under section 103(g) of the Immigration and Nationality Act, as added by section 1102.

* * * * * * *

SEC. 1103. [6 U.S.C. 522] STATUTORY CONSTRUCTION.

Nothing in this Act, any amendment made by this Act, or in section 103 of the Immigration and Nationality Act, as amended by section 1102, shall be construed to limit judicial deference to regulations, adjudications, interpretations, orders, decisions, judgments, or any other actions of the Secretary of Homeland Security or the Attorney General.

Subtitle B—Transfer of the Bureau of Alcohol, Tobacco and Firearms to the Department of Justice

SEC. 1111. [6 U.S.C. 531] BUREAU OF ALCOHOL, TOBACCO, FIREARMS, AND EXPLOSIVES.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—There is established within the Department of Justice under the general authority of the Attorney General the Bureau of Alcohol, Tobacco, Firearms, and Explosives (in this section referred to as the "Bureau").

(2) DIRECTOR.—There shall be at the head of the Bureau a Director, Bureau of Alcohol, Tobacco, Firearms, and Explosives (in this subtitle referred to as the "Director"). The Director shall be appointed by the President, by and with the advice

and consent of the Senate and shall perform such functions as the Attorney General shall direct. The Director shall receive compensation at the rate prescribed by law under section 5314 of title V, United States Code, for positions at level III of the Executive Schedule.

(3) COORDINATION.—The Attorney General, acting through the Director and such other officials of the Department of Justice as the Attorney General may designate, shall provide for the coordination of all firearms, explosives, tobacco enforcement, and arson enforcement functions vested in the Attorney General so as to assure maximum cooperation between and among any officer, employee, or agency of the Department of Justice involved in the performance of these and related functions.

(4) PERFORMANCE OF TRANSFERRED FUNCTIONS.—The Attorney General may make such provisions as the Attorney General determines appropriate to authorize the performance by any officer, employee, or agency of the Department of Justice of any function transferred to the Attorney General under this section.

(b) RESPONSIBILITIES.—Subject to the direction of the Attorney General, the Bureau shall be responsible for investigating—

(1) criminal and regulatory violations of the Federal firearms, explosives, arson, alcohol, and tobacco smuggling laws;

(2) the functions transferred by subsection (c); and

(3) any other function related to the investigation of violent crime or domestic terrorism that is delegated to the Bureau by the Attorney General.

(c) TRANSFER OF AUTHORITIES, FUNCTIONS, PERSONNEL, AND ASSETS TO THE DEPARTMENT OF JUSTICE.—

(1) IN GENERAL.—Subject to paragraph (2), but notwithstanding any other provision of law, there are transferred to the Department of Justice the authorities, functions, personnel, and assets of the Bureau of Alcohol, Tobacco and Firearms, which shall be maintained as a distinct entity within the Department of Justice, including the related functions of the Secretary of the Treasury.

(2) ADMINISTRATION AND REVENUE COLLECTION FUNCTIONS.—There shall be retained within the Department of the Treasury the authorities, functions, personnel, and assets of the Bureau of Alcohol, Tobacco and Firearms relating to the administration and enforcement of chapters 51 and 52 of the Internal Revenue Code of 1986, sections 4181 and 4182 of the Internal Revenue Code of 1986, and title 27, United States Code.

(3) BUILDING PROSPECTUS.—Prospectus PDC-98W10, giving the General Services Administration the authority for site acquisition, design, and construction of a new headquarters building for the Bureau of Alcohol, Tobacco and Firearms, is transferred, and deemed to apply, to the Bureau of Alcohol, Tobacco, Firearms, and Explosives established in the Department of Justice under subsection (a).

(d) TAX AND TRADE BUREAU.—

(1) ESTABLISHMENT.—There is established within the Department of the Treasury the Tax and Trade Bureau.

(2) ADMINISTRATOR.—The Tax and Trade Bureau shall be headed by an Administrator, who shall perform such duties as assigned by the Under Secretary for Enforcement of the Department of the Treasury. The Administrator shall occupy a career-reserved position within the Senior Executive Service.

(3) RESPONSIBILITIES.—The authorities, functions, personnel, and assets of the Bureau of Alcohol, Tobacco and Firearms that are not transferred to the Department of Justice under this section shall be retained and administered by the Tax and Trade Bureau.

* * * * * * *

SEC. 1114. [6 U.S.C. 532] EXPLOSIVES TRAINING AND RESEARCH FACILITY.

(a) ESTABLISHMENT.—There is established within the Bureau an Explosives Training and Research Facility at Fort AP Hill, Fredericksburg, Virginia.

(b) PURPOSE.—The facility established under subsection (a) shall be utilized to train Federal, State, and local law enforcement officers to—

(1) investigate bombings and explosions;

(2) properly handle, utilize, and dispose of explosive materials and devices;

(3) train canines on explosive detection; and

(4) conduct research on explosives.

(c) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There are authorized to be appropriated such sums as may be necessary to establish and maintain the facility established under subsection (a).

(2) AVAILABILITY OF FUNDS.—Any amounts appropriated pursuant to paragraph (1) shall remain available until expended.

SEC. 1115. [6 U.S.C. 533] PERSONNEL MANAGEMENT DEMONSTRATION PROJECT.

Notwithstanding any other provision of law, the Personnel Management Demonstration Project established under section 102 of title I of division C of the Omnibus Consolidated and Emergency Supplemental Appropriations Act for Fiscal Year 1999 (Public Law 105–277; 122 Stat. 2681–585) shall be transferred to the Attorney General of the United States for continued use by the Bureau of Alcohol, Tobacco, Firearms, and Explosives, Department of Justice, and the Secretary of the Treasury for continued use by the Tax and Trade Bureau.

Subtitle C—Explosives

SEC. 1121. [18 U.S.C. 841 note] SHORT TITLE.

This subtitle may be referred to as the "Safe Explosives Act".

SEC. 1122. PERMITS FOR PURCHASERS OF EXPLOSIVES.

(a)

* * * * * * *

(i) [18 U.S.C. 843 note] EFFECTIVE DATE.—

(1) IN GENERAL.—The amendments made by this section shall take effect 180 days after the date of enactment of this Act.

(2) EXCEPTION.—Notwithstanding any provision of this Act, a license or permit issued under section 843 of title 18, United States Code, before the date of enactment of this Act, shall remain valid until that license or permit is revoked under section 843(d) or expires, or until a timely application for renewal is acted upon.

* * * * * * *

SEC. 1128. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated such sums as necessary to carry out this subtitle and the amendments made by this subtitle.

TITLE XII—AIRLINE WAR RISK INSURANCE LEGISLATION

* * * * * * *

SEC. 1204. REPORT.

Not later than 90 days after the date of enactment of this Act, the Secretary shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives a report that—

(A) evaluates the availability and cost of commercial war risk insurance for air carriers and other aviation entities for passengers and third parties;

(B) analyzes the economic effect upon air carriers and other aviation entities of available commercial war risk insurance; and

(C) describes the manner in which the Department could provide an alternative means of providing aviation war risk reinsurance covering passengers, crew, and third parties through use of a risk-retention group or by other means.

TITLE XIII—FEDERAL WORKFORCE IMPROVEMENT

Subtitle A—Chief Human Capital Officers

SEC. 1301. [5 U.S.C. 101 note] SHORT TITLE.

This title may be cited as the "Chief Human Capital Officers Act of 2002".

* * * * * * *

SEC. 1303. [5 U.S.C. 1401 note] CHIEF HUMAN CAPITAL OFFICERS COUNCIL.

(a) ESTABLISHMENT.—There is established a Chief Human Capital Officers Council, consisting of—

(1) the Director of the Office of Personnel Management, who shall act as chairperson of the Council;

(2) the Deputy Director for Management of the Office of Management and Budget, who shall act as vice chairperson of the Council; and

(3) the Chief Human Capital Officers of Executive departments and any other members who are designated by the Director of the Office of Personnel Management.

(b) FUNCTIONS.—The Chief Human Capital Officers Council shall meet periodically to advise and coordinate the activities of the agencies of its members on such matters as modernization of human resources systems, improved quality of human resources information, and legislation affecting human resources operations and organizations.

(c) EMPLOYEE LABOR ORGANIZATIONS AT MEETINGS.—The Chief Human Capital Officers Council shall ensure that representatives of Federal employee labor organizations are present at a minimum of 1 meeting of the Council each year. Such representatives shall not be members of the Council.

(d) ANNUAL REPORTS.—

(1) IN GENERAL.—Each year, the Chief Human Capital Officers Council shall submit to Congress a report that includes the following:

(A) A description of the activities of the Council.

(B) A description of employment barriers that prevent the agencies of its members from hiring qualified applicants, including those for digital talent positions, and recommendations for addressing the barriers that would allow such agencies to more effectively hire qualified applicants.

(2) PUBLIC AVAILABILITY.—Not later than 30 days after the date on which the Council submits a report under paragraph (1), the Director of the Office of Personnel Management shall make the report publicly available on the website of the Office of Personnel Management.

SEC. 1305. [5 U.S.C. 1103 note] EFFECTIVE DATE.

This subtitle shall take effect 180 days after the date of enactment of this Act.

Subtitle B—Reforms Relating to Federal Human Capital Management

* * * * * * *

SEC. 1313. PERMANENT EXTENSION, REVISION, AND EXPANSION OF AUTHORITIES FOR USE OF VOLUNTARY SEPARATION INCENTIVE PAY AND VOLUNTARY EARLY RETIREMENT.

(a) VOLUNTARY SEPARATION INCENTIVE PAYMENTS.—

(1)

* * * * * * *

(2) [5 U.S.C. 3521 note] ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS.—The Director of the Administrative Office of the United States Courts may, by regulation, establish a program substantially similar to the program established under paragraph (1) for individuals serving in the judicial branch.

(3) [5 U.S.C. 3521 note] CONTINUATION OF OTHER AUTHORITY.—Any agency exercising any voluntary separation incentive authority in effect on the effective date of this subsection may continue to offer voluntary separation incentives consistent with that authority until that authority expires.

(4) [5 U.S.C. 3521 note] EFFECTIVE DATE.—This subsection shall take effect 60 days after the date of enactment of this Act.

* * * * * * *

(b) FEDERAL EMPLOYEE VOLUNTARY EARLY RETIREMENT.—

(1)

* * * * * * *

(3) [5 U.S.C. 8336 note] GENERAL ACCOUNTING OFFICE AUTHORITY.—The amendments made by this subsection shall not be construed to affect the authority under section 1 of Public Law 106–303 (5 U.S.C. 8336 note; 114 State. 1063).

* * * * * * *

(5) [5 U.S.C. 8336 note] REGULATIONS.—The Office of Personnel Management may prescribe regulations to carry out this subsection.

(c) [5 U.S.C. 3521 note] SENSE OF CONGRESS.—It is the sense of Congress that the implementation of this section is intended to reshape the Federal workforce and not downsize the Federal workforce.

* * * * * * *

Subtitle C—Reforms Relating to the Senior Executive Service

* * * * * * *

SEC. 1321. REPEAL OF RECERTIFICATION REQUIREMENTS OF SENIOR EXECUTIVES.

(a)

* * * * * * *

(b) [5 U.S.C. 3592 note] SAVINGS PROVISION.—Notwithstanding the amendments made by subsection (a)(2)(A), an appeal under the final sentence of section 3592(a) of title 5, United States Code, that is pending on the day before the effective date of this section—

(1) shall not abate by reason of the enactment of the amendments made by subsection (a)(2)(A); and

(2) shall continue as if such amendments had not been enacted.

(c) [5 U.S.C. 3593 note] APPLICATION.—The amendment made by subsection (a)(2)(B) shall not apply with respect to an individual who, before the effective date of this section, leaves the Senior Executive Service for failure to be recertified as a senior executive under section 3393a of title 5, United States Code.

* * * * * * *

Subtitle D—Academic Training

* * * * * * *

SEC. 1332. MODIFICATIONS TO NATIONAL SECURITY EDUCATION PROGRAM.

(a) [5 U.S.C. 3301 note] FINDINGS AND POLICIES.—

(1) FINDINGS.—Congress finds that—

(A) the United States Government actively encourages and financially supports the training, education, and development of many United States citizens;

(B) as a condition of some of those supports, many of those citizens have an obligation to seek either compensated or uncompensated employment in the Federal sector; and

(C) it is in the United States national interest to maximize the return to the Nation of funds invested in the development of such citizens by seeking to employ them in the Federal sector.

(2) POLICY.—It shall be the policy of the United States Government to—

(A) establish procedures for ensuring that United States citizens who have incurred service obligations as the result of receiving financial support for education and training from the United States Government and have applied for Federal positions are considered in all recruitment and hiring initiatives of Federal departments, bureaus, agencies, and offices; and

(B) advertise and open all Federal positions to United States citizens who have incurred service obligations with the United States Government as the result of receiving financial support for education and training from the United States Government.

(b) [Omitted—Amends another Act]

SEC. 1333. [6 U.S.C. 665a] 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, United States Code.

(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 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).

(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 thereof;

(2) receive tuition assistance from the Secretary; and

(3) upon graduation from an institution of higher education and successful completion of the Program (as defined by the Secretary), receive 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 in defined in section 124.103 of title 13, Code of Federal Regulations, or 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 such offer, the

Secretary shall appoint, without regard to provisions of subchapter I of chapter 33 of title 5, United States Code, (except for section 3328 of such title) such individual to the position specified in such offer.

(e) REPORTS.—

(1) REPORTS.—Not later than 1 year after the date of the enactment of this section, and on an annual basis thereafter, the Secretary shall submit to the appropriate committees of Congress a report on the Program.

(2) MATTERS.—Each report under paragraph (1) shall include, with respect to the most recent year, the following:

(A) 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.

(B) Information on specific recruiting efforts conducted by the Secretary to increase participation in the Program.

(C) 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 such participation, including on whether the duties of the individual under the Program relate primarily to intelligence or to cybersecurity.

(D) The number of individuals who accepted an offer of employment under the Program and an identification of the element within the Department to which each individual was appointed.

TITLE XIV—ARMING PILOTS AGAINST TERRORISM

SEC. 1401. [49 U.S.C. 40101 note] SHORT TITLE.

This title may be cited as the "Arming Pilots Against Terrorism Act".

SEC. 1402. FEDERAL FLIGHT DECK OFFICER PROGRAM.

(a)

* * * * * * *

(c) [6 U.S.C. 513] FEDERAL AIR MARSHAL PROGRAM.—

(1) SENSE OF CONGRESS.—It is the sense of Congress that the Federal air marshal program is critical to aviation security.

(2) LIMITATION ON STATUTORY CONSTRUCTION.—Nothing in this Act, including any amendment made by this Act, shall be construed as preventing the Under Secretary of Transportation for Security from implementing and training Federal air marshals.

SEC. 1403. CREW TRAINING.

(a)

* * * * * * *

(c) BENEFITS AND RISKS OF PROVIDING FLIGHT ATTENDANTS WITH NONLETHAL WEAPONS.—

(1) STUDY.—The Under Secretary of Transportation for Security shall conduct a study to evaluate the benefits and risks of providing flight attendants with nonlethal weapons to aide in combating air piracy and criminal violence on commercial airlines.

(2) REPORT.—Not later than 6 months after the date of enactment of this Act, the Under Secretary shall transmit to Congress a report on the results of the study.

SEC. 1404. COMMERCIAL AIRLINE SECURITY STUDY.

(a) STUDY.—The Secretary of Transportation shall conduct a study of the following:

(1) The number of armed Federal law enforcement officers (other than Federal air marshals), who travel on commercial airliners annually and the frequency of their travel.

(2) The cost and resources necessary to provide such officers with supplemental training in aircraft anti-terrorism training that is comparable to the training that Federal air marshals are provided.

(3) The cost of establishing a program at a Federal law enforcement training center for the purpose of providing new Federal law enforcement recruits with standardized training comparable to the training that Federal air marshals are provided.

(4) The feasibility of implementing a certification program designed for the purpose of ensuring Federal law enforcement officers have completed the training described in paragraph (2) and track their travel over a 6-month period.

(5) The feasibility of staggering the flights of such officers to ensure the maximum amount of flights have a certified trained Federal officer on board.

(b) REPORT.—Not later than 6 months after the date of enactment of this Act, the Secretary shall transmit to Congress a report on the results of the study. The report may be submitted in classified and redacted form.

* * * * * * *

TITLE XV—TRANSITION

Subtitle A—Reorganization Plan

SEC. 1501. [6 U.S.C. 541] DEFINITIONS.

For purposes of this title:

(1) The term "agency" includes any entity, organizational unit, program, or function.

(2) The term "transition period" means the 12-month period beginning on the effective date of this Act.

SEC. 1502. [6 U.S.C. 542] REORGANIZATION PLAN.

(a) SUBMISSION OF PLAN.—Not later than 60 days after the date of the enactment of this Act, the President shall transmit to the appropriate congressional committees a reorganization plan regarding the following:

(1) The transfer of agencies, personnel, assets, and obligations to the Department pursuant to this Act.

(2) Any consolidation, reorganization, or streamlining of agencies transferred to the Department pursuant to this Act.

(b) PLAN ELEMENTS.—The plan transmitted under subsection (a) shall contain, consistent with this Act, such elements as the President deems appropriate, including the following:

(1) Identification of any functions of agencies transferred to the Department pursuant to this Act that will not be transferred to the Department under the plan.

(2) Specification of the steps to be taken by the Secretary to organize the Department, including the delegation or assignment of functions transferred to the Department among officers of the Department in order to permit the Department to carry out the functions transferred under the plan.

(3) Specification of the funds available to each agency that will be transferred to the Department as a result of transfers under the plan.

(4) Specification of the proposed allocations within the Department of unexpended funds transferred in connection with transfers under the plan.

(5) Specification of any proposed disposition of property, facilities, contracts, records, and other assets and obligations of agencies transferred under the plan.

(6) Specification of the proposed allocations within the Department of the functions of the agencies and subdivisions that are not related directly to securing the homeland.

(c) MODIFICATION OF PLAN.—The President may, on the basis of consultations with the appropriate congressional committees, modify or revise any part of the plan until that part of the plan becomes effective in accordance with subsection (d).

(d) EFFECTIVE DATE.—

(1) IN GENERAL.—The reorganization plan described in this section, including any modifications or revisions of the plan under subsection (d), shall become effective for an agency on the earlier of—

(A) the date specified in the plan (or the plan as modified pursuant to subsection (d)), except that such date may not be earlier than 90 days after the date the President has transmitted the reorganization plan to the appropriate congressional committees pursuant to subsection (a); or

(B) the end of the transition period.

(2) STATUTORY CONSTRUCTION.—Nothing in this subsection may be construed to require the transfer of functions, personnel, records, balances of appropriations, or other assets of an agency on a single date.

(3) SUPERSEDES EXISTING LAW.—Paragraph (1) shall apply notwithstanding section 905(b) of title 5, United States Code.

SEC. 1503. [6 U.S.C. 543] REVIEW OF CONGRESSIONAL COMMITTEE STRUCTURES.

It is the sense of Congress that each House of Congress should review its committee structure in light of the reorganization of responsibilities within the executive branch by the establishment of the Department.

Subtitle B—Transitional Provisions

SEC. 1511. [6 U.S.C. 551] TRANSITIONAL AUTHORITIES.

(a) PROVISION OF ASSISTANCE BY OFFICIALS.—Until the transfer of an agency to the Department, any official having authority over or functions relating to the agency immediately before the effective date of this Act shall provide to the Secretary such assistance, including the use of personnel and assets, as the Secretary may request in preparing for the transfer and integration of the agency into the Department.

(b) SERVICES AND PERSONNEL.—During the transition period, upon the request of the Secretary, the head of any executive agency may, on a reimbursable basis, provide services or detail personnel to assist with the transition.

(c) ACTING OFFICIALS.—(1) During the transition period, pending the advice and consent of the Senate to the appointment of an officer required by this Act to be appointed by and with such advice and consent, the President may designate any officer whose appointment was required to be made by and with such advice and consent and who was such an officer immediately before the effective date of this Act (and who continues in office) or immediately before such designation, to act in such office until the same is filled as provided in this Act. While so acting, such officers shall receive compensation at the higher of—

(A) the rates provided by this Act for the respective offices in which they act; or

(B) the rates provided for the offices held at the time of designation.

(2) Nothing in this Act shall be understood to require the advice and consent of the Senate to the appointment by the President to a position in the Department of any officer whose agency is transferred to the Department pursuant to this Act and whose duties following such transfer are germane to those performed before such transfer.

(d) TRANSFER OF PERSONNEL, ASSETS, OBLIGATIONS, AND FUNCTIONS.—Upon the transfer of an agency to the Department—

(1) the personnel, assets, and obligations held by or available in connection with the agency shall be transferred to the Secretary for appropriate allocation, subject to the approval of the Director of the Office of Management and Budget and in accordance with the provisions of section 1531(a)(2) of title 31, United States Code; and

(2) the Secretary shall have all functions relating to the agency that any other official could by law exercise in relation to the agency immediately before such transfer, and shall have in addition all functions vested in the Secretary by this Act or other law.

(e) PROHIBITION ON USE OF TRANSPORTATION TRUST FUNDS.—

(1) IN GENERAL.—Notwithstanding any other provision of this Act, no funds derived from the Highway Trust Fund, Airport and Airway Trust Fund, Inland Waterway Trust Fund, or Harbor Maintenance Trust Fund, may be transferred to, made

available to, or obligated by the Secretary or any other official in the Department.

(2) LIMITATION.—This subsection shall not apply to security-related funds provided to the Federal Aviation Administration for fiscal years preceding fiscal year 2003 for (A) operations, (B) facilities and equipment, or (C) research, engineering, and development, and to any funds provided to the Coast Guard from the Sport Fish Restoration and Boating Trust Fund for boating safety programs.

SEC. 1512. [6 U.S.C. 552] SAVINGS PROVISIONS.

(a) COMPLETED ADMINISTRATIVE ACTIONS.—(1) Completed administrative actions of an agency shall not be affected by the enactment of this Act or the transfer of such agency to the Department, but shall continue in effect according to their terms until amended, modified, superseded, terminated, set aside, or revoked in accordance with law by an officer of the United States or a court of competent jurisdiction, or by operation of law.

(2) For purposes of paragraph (1), the term "completed administrative action" includes orders, determinations, rules, regulations, personnel actions, permits, agreements, grants, contracts, certificates, licenses, registrations, and privileges.

(b) PENDING PROCEEDINGS.—Subject to the authority of the Secretary under this Act—

(1) pending proceedings in an agency, including notices of proposed rulemaking, and applications for licenses, permits, certificates, grants, and financial assistance, shall continue notwithstanding the enactment of this Act or the transfer of the agency to the Department, unless discontinued or modified under the same terms and conditions and to the same extent that such discontinuance could have occurred if such enactment or transfer had not occurred; and

(2) orders issued in such proceedings, and appeals therefrom, and payments made pursuant to such orders, shall issue in the same manner and on the same terms as if this Act had not been enacted or the agency had not been transferred, and any such orders shall continue in effect until amended, modified, superseded, terminated, set aside, or revoked by an officer of the United States or a court of competent jurisdiction, or by operation of law.

(c) PENDING CIVIL ACTIONS.—Subject to the authority of the Secretary under this Act, pending civil actions shall continue notwithstanding the enactment of this Act or the transfer of an agency to the Department, and in such civil actions, proceedings shall be had, appeals taken, and judgments rendered and enforced in the same manner and with the same effect as if such enactment or transfer had not occurred.

(d) REFERENCES.—References relating to an agency that is transferred to the Department in statutes, Executive orders, rules, regulations, directives, or delegations of authority that precede such transfer or the effective date of this Act shall be deemed to refer, as appropriate, to the Department, to its officers, employees, or agents, or to its corresponding organizational units or functions. Statutory reporting requirements that applied in relation to such

an agency immediately before the effective date of this Act shall continue to apply following such transfer if they refer to the agency by name.

(e) EMPLOYMENT PROVISIONS.—(1) Notwithstanding the generality of the foregoing (including subsections (a) and (d)), in and for the Department the Secretary may, in regulations prescribed jointly with the Director of the Office of Personnel Management, adopt the rules, procedures, terms, and conditions, established by statute, rule, or regulation before the effective date of this Act, relating to employment in any agency transferred to the Department pursuant to this Act; and

(2) except as otherwise provided in this Act, or under authority granted by this Act, the transfer pursuant to this Act of personnel shall not alter the terms and conditions of employment, including compensation, of any employee so transferred.

(f) STATUTORY REPORTING REQUIREMENTS.—Any statutory reporting requirement that applied to an agency, transferred to the Department under this Act, immediately before the effective date of this Act shall continue to apply following that transfer if the statutory requirement refers to the agency by name.

SEC. 1513. [6 U.S.C. 553] TERMINATIONS.

Except as otherwise provided in this Act, whenever all the functions vested by law in any agency have been transferred pursuant to this Act, each position and office the incumbent of which was authorized to receive compensation at the rates prescribed for an office or position at level II, III, IV, or V, of the Executive Schedule, shall terminate.

SEC. 1514. [6 U.S.C. 554] NATIONAL IDENTIFICATION SYSTEM NOT AUTHORIZED.

Nothing in this Act shall be construed to authorize the development of a national identification system or card.

SEC. 1515. [6 U.S.C. 555] CONTINUITY OF INSPECTOR GENERAL OVERSIGHT.

Notwithstanding the transfer of an agency to the Department pursuant to this Act, the Inspector General that exercised oversight of such agency prior to such transfer shall continue to exercise oversight of such agency during the period of time, if any, between the transfer of such agency to the Department pursuant to this Act and the appointment of the Inspector General of the Department of Homeland Security in accordance with section 103(b).

SEC. 1516. [6 U.S.C. 556] INCIDENTAL TRANSFERS.

The Director of the Office of Management and Budget, in consultation with the Secretary, is authorized and directed to make such additional incidental dispositions of personnel, assets, and liabilities held, used, arising from, available, or to be made available, in connection with the functions transferred by this Act, as the Director may determine necessary to accomplish the purposes of this Act.

SEC. 1517. [6 U.S.C. 557] REFERENCE.

With respect to any function transferred by or under this Act (including under a reorganization plan that becomes effective under section 1502) and exercised on or after the effective date of

this Act, reference in any other Federal law to any department, commission, or agency or any officer or office the functions of which are so transferred shall be deemed to refer to the Secretary, other official, or component of the Department to which such function is so transferred.

TITLE XVI—TRANSPORTATION SECURITY

Subtitle A—General Provisions

SEC. 1601. [6 U.S.C. 561] DEFINITIONS.

In this title:

(1) ADMINISTRATION.—The term "Administration" means the Transportation Security Administration.

(2) ADMINISTRATOR.—The term "Administrator" means the Administrator of the Transportation Security Administration.

(3) PLAN.—The term "Plan" means the strategic 5-year technology investment plan developed by the Administrator under section 1611.

(4) SECURITY-RELATED TECHNOLOGY.—The term "security-related technology" means any technology that assists the Administration in the prevention of, or defense against, threats to United States transportation systems, including threats to people, property, and information.

Subtitle B—Transportation Security Administration Acquisition Improvements

SEC. 1611. [6 U.S.C. 563] 5-YEAR TECHNOLOGY INVESTMENT PLAN.

(a) IN GENERAL.—The Administrator shall—

(1) not later than 180 days after the date of the enactment of the Transportation Security Acquisition Reform Act, 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, publish the Plan in an unclassified format in the public domain.

(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 industry stakeholder advisory committee established by the Administrator.

(c) APPROVAL.—The Administrator may not publish the Plan under subsection (a)(2) until it has been approved by the Secretary.

(d) CONTENTS OF PLAN.—The Plan shall include—

(1) an analysis of transportation security risks and the associated capability gaps that would be best addressed by secu-

rity-related technology, including consideration of the most recent quadrennial homeland security review under section 707;

(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 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 Administration's acquisition process and provide greater predictability and clarity to small, medium, and large businesses, including the timeline for testing and evaluation;

(10) an assessment of the impact to commercial aviation passengers;

(11) a strategy for consulting airport management, air carrier representatives, and Federal security directors whenever an acquisition will lead to the removal of equipment at airports, and how the strategy for consulting with such officials of the relevant airports will address potential negative impacts on commercial passengers or airport operations; and

(12) in consultation with the National Institutes 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.

(e) LEVERAGING THE PRIVATE SECTOR.—To the extent possible, 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 within 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 to meeting mission needs.

(f) DISCLOSURE.—The Administrator shall include with the Plan a list of nongovernment persons that contributed to the writing of the Plan.

(g)[14] 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 acquired by the Administration since the last issuance or update of the Plan is consistent with the planned technology programs and projects identified under subsection (d)(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.

(h) ADDITIONAL UPDATE REQUIREMENTS.—Updates and reports under subsection (g) shall—

(1) be prepared in consultation with—

(A) the persons described in subsection (b); and

(B) the Surface Transportation Security Advisory Committee established under section 404; 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 life-cycle 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).

(i) NOTICE OF COVERED CHANGES TO PLAN.—

(1) 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

[14] Section 1917(1)(A) of division K of Public Law 115–254 provides for an amendment to strike the matter preceding paragraph (1) and insert new language. The execution of such amendment does not delete the subsection designation and heading in accordance with the probable intent of Congress.

House of Representatives notice of any covered change to the Plan not later than 90 days after the date that the covered change is made.

(2) 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.

SEC. 1612. [6 U.S.C. 563a] ACQUISITION JUSTIFICATION AND REPORTS.

(a) ACQUISITION JUSTIFICATION.—Before the 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 to 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 TO CONGRESS.—

(1) IN GENERAL.—Not later than the end of the 30-day period preceding the award by the 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) EXTENSION 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.

SEC. 1613. [6 U.S.C. 563b] ACQUISITION BASELINE ESTABLISHMENT AND REPORTS.

(a) BASELINE REQUIREMENTS.—

(1) IN GENERAL.—Before the Administration implements any security-related technology acquisition, the appropriate acquisition official of the Department shall establish and document a set of formal baseline requirements.

(2) CONTENTS.—The baseline requirements under paragraph (1) 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.

(3) FEASIBILITY.—In establishing the performance milestones under paragraph (2)(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.

(4) 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 (2)(A);

(B) the necessary and cost-effective combination of laboratory testing, field testing, modeling, simulation, and supporting analysis to ensure that such technologies meet the 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 measure passenger acceptance of and familiarization with the security-related technology.

(5) VERIFICATION AND VALIDATION.—The appropriate acquisition official of the Department—

(A) subject to subparagraph (B), shall utilize independent reviewers to verify and validate the performance milestones and cost estimates developed under paragraph (2) for a security-related technology that pursuant to sec-

tion 1611(d)(2) 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.

(6) 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 acquisitions process for that technology.

(b) REVIEW OF BASELINE REQUIREMENTS AND DEVIATION; REPORT TO CONGRESS.—

(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) TEST AND EVALUATION 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 such excessive costs, delay, or failure; and

(C) a plan for corrective action.

SEC. 1614. [6 U.S.C. 563c] INVENTORY UTILIZATION.

(a) IN GENERAL.—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 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 equipment in the inventory under subsection (a);

(B) the utilization status of security-related technology in the inventory under subsection (a); and

(C) the quantity 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.

SEC. 1615. [6 U.S.C. 563d] SMALL BUSINESS CONTRACTING GOALS.

Not later than 90 days after the date of enactment of the Transportation Security Acquisition Reform Act, and annually thereafter, 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—

(1) the 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 Administration's performance was below the published small-business contracting goals of the Department—

(A) a list of challenges, including deviations from the 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 Administration in furtherance of achieving the Administration's published goal for such 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 such a plan was required.

SEC. 1616. [6 U.S.C. 563e] CONSISTENCY WITH THE FEDERAL ACQUISITION REGULATION AND DEPARTMENTAL POLICIES AND DIRECTIVES.

The Administrator shall execute the responsibilities set forth in this subtitle in a manner consistent with, and not duplicative of,

the Federal Acquisition Regulation and the Department's policies and directives.

SEC. 1617. [6 U.S.C. 563f] DIVERSIFIED SECURITY TECHNOLOGY INDUSTRY MARKETPLACE.

(a) IN GENERAL.—Not later than 120 days after the date of enactment of the TSA Modernization Act, 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 upon which the Administrator can rely to acquire advanced transportation security technologies or capabilities, including by increased participation of small business innovators.

(b) CONTENTS.—The strategy required under subsection (a) shall include the following:

(1) Information on how existing 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 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 within 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 such processes, including when such an innovator lacks adequate resources to participate in such 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 and exempt from tax under section 501(a) of such Code 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.

(c) FEASIBILITY ASSESSMENT.—In conducting the feasibility assessment under subsection (b)(5), the Administrator shall consider the following:

(1) Establishing an organization described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such Code 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 of Homeland Security.

(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed as requiring changes to the Transportation Security Administration standards for security technology.

(e) 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.

Subtitle C—Maintenance of Security-related Technology

SEC. 1621. [6 U.S.C. 565] MAINTENANCE VALIDATION AND OVERSIGHT.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of the TSA Modernization Act, the Administrator shall develop and implement a preventive maintenance validation process for security-related technology deployed to airports.

(b) MAINTENANCE BY ADMINISTRATION PERSONNEL AT AIRPORTS.—For maintenance to be carried out by Administration personnel at airports, the process referred to in subsection (a) shall include the following:

(1) Guidance to Administration personnel at airports specifying how to conduct and document preventive maintenance actions.

(2) Mechanisms for the Administrator to verify compliance with the guidance issued pursuant to paragraph (1).

(c) MAINTENANCE BY CONTRACTORS AT AIRPORTS.—For maintenance to be carried 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 Administration personnel at each airport that includes information on each action to be completed by contractor.

(2) Notification to appropriate 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 any contracts entered into 60 days after the date of enactment of the TSA Modernization Act 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.

TITLE XVII—CONFORMING AND TECHNICAL AMENDMENTS

* * * * * * *

SEC. 1702. EXECUTIVE SCHEDULE.

(a)

* * * * * * *

(b) [5 U.S.C. 5315 note] SPECIAL EFFECTIVE DATE.—Notwithstanding section 4, the amendment made by subsection (a)(5) shall take effect on the date on which the transfer of functions specified under section 441 takes effect.

SEC. 1703. UNITED STATES SECRET SERVICE.

(a)

(b) [3 U.S.C. 202 note] EFFECTIVE DATE.—The amendments made by this section shall take effect on the date of transfer of the United States Secret Service to the Department.

SEC. 1704. COAST GUARD.

(a)

* * * * * * *

(g) [10 U.S.C. 101 note] EFFECTIVE DATE.—The amendments made by this section (other than subsection (f)) shall take effect on the date of transfer of the Coast Guard to the Department.

SEC. 1705. STRATEGIC NATIONAL STOCKPILE AND SMALLPOX VACCINE DEVELOPMENT.

(a)

* * * * * * *

(b) [42 U.S.C. 247d–6b note] EFFECTIVE DATE.—The amendments made by this section shall take effect on the date of transfer of the Strategic National Stockpile of the Department of Health and Human Services to the Department.

SEC. 1706. TRANSFER OF CERTAIN SECURITY AND LAW ENFORCEMENT FUNCTIONS AND AUTHORITIES.

(a)

* * * * * * *

(2) [40 U.S.C. 1315 note] DELEGATION OF AUTHORITY.—The Secretary may delegate authority for the protection of specific buildings to another Federal agency where, in the Secretary's discretion, the Secretary determines it necessary for the protection of that building.

* * * * * * *

SEC. 1708. [50 U.S.C. 1522 note] NATIONAL BIO-WEAPONS DEFENSE ANALYSIS CENTER.

There is established in the Department of Defense a National Bio-Weapons Defense Analysis Center, whose mission is to develop countermeasures to potential attacks by terrorists using weapons of mass destruction.

* * * * * * *

SEC. 1714. [6 U.S.C. 103] Notwithstanding any other provision of this Act, any report, notification, or consultation addressing directly or indirectly the use of appropriated funds and stipulated by this Act to be submitted to, or held with, the Congress or any 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 Act.

TITLE XVIII—EMERGENCY COMMUNICATIONS

SEC. 1801. [6 U.S.C. 571] EMERGENCY COMMUNICATIONS DIVISION.

(a) IN GENERAL.—There is established in the Department an Emergency Communications Division. The Division shall be located in the Cybersecurity and Infrastructure Security Agency.

(b) EXECUTIVE ASSISTANT DIRECTOR.—The head of the Division shall be the Executive Assistant Director for Emergency Communications (in this section referred to as the "Executive Assistant Director"). The Executive Assistant Director shall report to the Director of the Cybersecurity and Infrastructure Security Agency. All decisions of the Executive Assistant Director that entail the exercise of significant authority shall be subject to the approval of the Director of the Cybersecurity and Infrastructure Security Agency.

(c) RESPONSIBILITIES.—The Executive Assistant Director shall—

(1) assist the Secretary in developing and implementing the program described in section 7303(a)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(a)(1)), except as provided in section 314;

(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 manmade 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 use of interoperable emergency communications capabilities;

(7) coordinate with the Regional Administrators regarding the activities of Regional Emergency Communications Coordination Working Groups under section 1805;

(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 such best practices for achieving, maintaining, and enhancing interoperable emergency communications capabilities for such 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 such 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 such plans;

(13) develop and update periodically, as appropriate, a National Emergency Communications Plan under section 1802;

(14) perform such 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 2202(c)(7).

(d) PERFORMANCE OF PREVIOUSLY TRANSFERRED FUNCTIONS.—The Secretary shall transfer to, and administer through, the Executive Assistant Director 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.

(e) COORDINATION.—The Executive Assistant Director shall coordinate—

(1) as appropriate, with the Director of the Office for Interoperability and Compatibility with respect to the responsibilities described in section 314; and

(2) with the Administrator of the Federal Emergency Management Agency with respect to the responsibilities described in this title.

(f) SUFFICIENCY OF RESOURCES PLAN.—

(1) REPORT.—Not later than 120 days after the date of enactment of this section, the Secretary shall submit to Congress a report on the resources and staff necessary to carry out fully the responsibilities under this title.

(2) COMPTROLLER GENERAL REVIEW.—The Comptroller General shall review the validity of the report submitted by the Secretary under paragraph (1). Not later than 60 days after the date on which such report is submitted, the Comptroller General shall submit to Congress a report containing the findings of such review.

(g) REFERENCE.—Any reference to the Assistant Director for Emergency Communications in any 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.

SEC. 1802. [6 U.S.C. 572] NATIONAL EMERGENCY COMMUNICATIONS PLAN.

(a) IN GENERAL.—The Secretary, acting through the Assistant Director for Emergency Communications, and in cooperation with the Department of National Communications System (as appropriate), shall, in cooperation with State, local, and tribal governments, Federal departments and agencies, emergency response providers, and the private sector, develop not later than 180 days after the completion of the baseline assessment under section 1803, 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 1806 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 timeframes 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 7303(g)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(g)(1)).

SEC. 1803. [6 U.S.C. 573] ASSESSMENTS AND REPORTS.

(a) BASELINE ASSESSMENT.—Not later than 1 year after the date of enactment of this section and not less than every 5 years thereafter, the Secretary, acting through the Assistant Director for Emergency Communications, shall conduct an assessment of Federal, State, local, and tribal governments 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 current available capabilities to meet such communications needs;

(4) identifies the gap between such current capabilities and defined requirements; and

(5) includes a national interoperable emergency communications inventory to be completed by the Secretary of Homeland Security, 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, the date of enactment of this title.

(d) PROGRESS REPORTS.—Not later than one year after the date of enactment of this section 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 title, 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

(A) an evaluation of the feasibility and desirability of the Department 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.

SEC. 1804. [6 U.S.C. 574] 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 1802.

(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) such government has not complied with the requirement to submit a Statewide Interoperable Communications Plan as required by section 7303(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(f));

(B) such 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 such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed such 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 1802, 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 with responsibility for standards, shall support the development, promulgation, and updating as necessary of national voluntary consensus standards for interoperable emergency communications.

SEC. 1805. [6 U.S.C. 575] REGIONAL EMERGENCY COMMUNICATIONS COORDINATION.

(a) IN GENERAL.—There is established 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 shall consist of the following:

(1) NON-FEDERAL.—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) FEDERAL.—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 shall 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 1802, on the progress of the region in meeting the goals of such 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.

SEC. 1806. [6 U.S.C. 576] EMERGENCY COMMUNICATIONS PREPAREDNESS CENTER.

(a) ESTABLISHMENT.—There is established the Emergency Communications Preparedness Center (in this section referred to as the "Center").

(b) OPERATION.—The Secretary, the Chairman of the Federal Communications Commission, the Secretary of Defense, the Secretary of Commerce, the Attorney General of the United States, and the heads of other Federal departments and agencies or their designees shall jointly operate the Center in accordance with the Memorandum of Understanding entitled, "Emergency Communications Preparedness Center (ECPC) Charter".

(c) FUNCTIONS.—The 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, on an annual basis, 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 1802; and

(4) perform such other functions as are provided in the Emergency Communications Preparedness Center (ECPC) Charter described in subsection (b)(1).

SEC. 1807. [6 U.S.C. 577] 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 1016 of the National Security Intelligence Reform Act of 2004 (6 U.S.C. 321); and

(3) to be consistent with any applicable State or Urban Area homeland strategy or plan.

SEC. 1808. [6 U.S.C. 578] DEFINITION.

In this title, the term "interoperable" has the meaning given the term "interoperable communications" under section 7303(g)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(g)(1)).

SEC. 1809. [6 U.S.C. 579] 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 title, including ensuring that activities funded by the grant—

(1) comply with the statewide plan for that State required by section 7303(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(f)); and

(2) comply with the National Emergency Communications Plan under section 1802, 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 title V of the Act.

(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 pursuant to section 7303(a)(1)(H) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(a)(1)(H)).

(d) USE OF FUNDS.—A State that receives a grant under this section shall use the grant to implement that State's Statewide Interoperability Plan required under section 7303(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(f)) and approved under subsection (e), 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 Statewide Interoperable Communications Plan required under section 7303(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(f)).

(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 1802.

(3) APPROVAL OF REVISIONS.—The Assistant Director for Emergency Communications may approve revisions to a State's plan if the Assistant Director 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 such actions as necessary 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 1802.

(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 such 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 manmade disasters, including—

(A) the likely need of a jurisdiction within the State to respond to such 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 the following percentage of the total amount appropriated for grants under this section for that fiscal year:

(A) For fiscal year 2008, 0.50 percent.

(B) For fiscal year 2009, 0.50 percent.

(C) For fiscal year 2010, 0.45 percent.

(D) For fiscal year 2011, 0.40 percent.

(E) For fiscal year 2012 and each subsequent fiscal year, 0.35 percent.

(2) TERRITORIES AND POSSESSIONS.—In awarding grants under this section, the Secretary shall ensure that for each fiscal year, American Samoa, the Commonwealth of 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 Statewide Interoperable Communications Plan.

(l) STATE RESPONSIBILITIES.—

(1) AVAILABILITY OF FUNDS TO LOCAL AND TRIBAL GOVERNMENTS.—Not later than 45 days after receiving grant funds, any 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 Statewide 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 Assistant Director for Emergency Communications a report on the progress of the State in implementing that State's Statewide Interoperable Communications Plans required under section 7303(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(f)) and achieving interoperability at the city, county, regional, State, and interstate levels. The Assistant Director 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 deter-

mines 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 such 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.

(o) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for grants under this section—

(1) for fiscal year 2008, such sums as may be necessary;

(2) for each of fiscal years 2009 through 2012, $400,000,000; and

(3) for each subsequent fiscal year, such sums as may be necessary.

SEC. 1810. [6 U.S.C. 580] BORDER INTEROPERABILITY DEMONSTRATION PROJECT.

(a) IN GENERAL.—

(1) ESTABLISHMENT.—The Secretary, acting through the Assistant Director for Emergency Communications (referred to in this section as the "Assistant Director"), and in coordination with the Federal Communications Commission and the Secretary of Commerce, shall establish an International Border Community Interoperable Communications Demonstration Project (referred to in this section as the "demonstration project").

(2) MINIMUM NUMBER OF COMMUNITIES.—The Assistant Director shall select no fewer than 6 communities to participate in a 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, in coordination with the Federal Communications Commission and the Secretary of Commerce, shall ensure that the 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 border 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) PROGRAM REQUIREMENTS.—Consistent with the responsibilities of the Emergency Communications Division under section 1801, the Assistant Director 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 shall—

(1) identify solutions to facilitate interoperable communications across national borders expeditiously;

(2) help ensure that emergency response providers 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 deems appropriate to foster interoperable emergency communications.

(d) DISTRIBUTION OF FUNDS.—

(1) IN GENERAL.—The Secretary shall distribute funds under this section to each community participating in the demonstration project through the State, or States, in which each community is located.

(2) OTHER PARTICIPANTS.—A State shall make the funds available promptly to the local and tribal governments 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 State shall report to the Assistant Director on the status of the distribution of such funds to local and tribal governments.

(e) MAXIMUM PERIOD OF GRANTS.—The Assistant Director may not fund any participant under the demonstration project for more than 3 years.

(f) TRANSFER OF INFORMATION AND KNOWLEDGE.—The Assistant Director 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 the participant in the project.

(g) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for grants under this section such sums as may be necessary.

TITLE XIX—COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE

SEC. 1900. [6 U.S.C. 590] DEFINITIONS.

In this title:

(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 such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(3) OFFICE.—The term "Office" means the Countering Weapons of Mass Destruction Office established under section 1901(a).

(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).

Subtitle A—Countering Weapons of Mass Destruction Office

SEC. 1901. COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE.

(a) [6 U.S.C. 591] ESTABLISHMENT.—There is established in the Department a Countering Weapons of Mass Destruction Office.

(b) ASSISTANT SECRETARY.—The Office shall be headed by an Assistant Secretary for the Countering Weapons of Mass Destruction Office, who shall be appointed by the President.

(c) RESPONSIBILITIES.—The Assistant Secretary shall serve as the Secretary's principal advisor on—

(1) weapons of mass destruction matters and strategies; and

(2) coordinating the efforts of the Department to counter weapons of mass destruction.

(d) DETAILS.—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 heads of other Federal agencies, including elements of the intelligence community, provide for the reimbursable detail of personnel with relevant expertise to the Office.

(e) TERMINATION.—The Office shall terminate on the date that is 5 years after the date of the enactment of the Countering Weapons of Mass Destruction Act of 2018.

Subtitle B—Mission of the Office

SEC. 1921. [6 U.S.C. 591g] MISSION OF THE OFFICE.

The Office shall be 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 such materials, devices, or agents against the people, territory, or interests of the United States.

SEC. 1922. [6 U.S.C. 591h] RELATIONSHIP TO OTHER DEPARTMENT COMPONENTS AND FEDERAL AGENCIES.

(a) IN GENERAL.—The authority of the Assistant Secretary under this title shall not affect or diminish the authority or the responsibility of any officer of the Department or any officer of any

other Federal agency with respect to the command, control, or direction of the functions, personnel, funds, assets, or liabilities of any component of the Department or any other Federal agency.

(b) OFFICE FOR STRATEGY, POLICY, AND PLANS.—Not later than one year after the date of the enactment of the Countering Weapons of Mass Destruction Act of 2018, the Assistant Secretary shall, in coordination with the Under Secretary for Strategy, Policy, and Plans, submit to the appropriate congressional committees a strategy and implementation plan to direct programs within the Office and to integrate those programs with other programs and activities of the Department.

(c) FEDERAL EMERGENCY MANAGEMENT AGENCY.—Nothing in this title or any other provision of law may be construed to affect or reduce the responsibilities of the Federal Emergency Management Agency or the Administrator of the Agency, including the diversion of any asset, function, or mission of the Agency or the Administrator of the Agency.

SEC. 1923. [6 U.S.C. 592] RESPONSIBILITIES.

(a) MISSION.—The Office shall be 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 such devices or materials against the people, territory, or interests of the United States and, to this end, shall—

(1) 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 improve that system over time;

(2) enhance and coordinate the nuclear detection efforts of Federal, State, local, and tribal governments and the private sector to ensure a managed, coordinated response;

(3) 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;

(4) 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—

(A) the Office will be responsible for the implementation of the domestic portion of the global architecture;

(B) the Secretary of Defense will retain responsibility for implementation of Department of Defense requirements within and outside the United States; and

(C) 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;

(5) ensure that the expertise necessary to accurately interpret detection data is made available in a timely manner for all technology deployed by the Office to implement the global nuclear detection architecture;

(6) 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;

(7) 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—

(A) under realistic operational and environmental conditions; and

(B) against realistic adversary tactics and countermeasures;

(8) support and enhance the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments, as well as provide appropriate information to such entities;

(9) further enhance and maintain continuous awareness by analyzing information from all Office mission-related detection systems;

(10) 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;

(11) establish, within 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—

(A) 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

(B) to coordinate and implement the national strategic five-year plan referred to in paragraph (10);

(12) establish a National Nuclear Forensics Expertise Development Program, which—

(A) 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;

(B) 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 1 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—

(I) include, if possible, at least 2 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

(II) 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 Hawaiian Native-serving institutions; and

(C) 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 such employees in areas of critical nuclear forensics and attribution needs of the United States Government, for doctoral education under the scholarship 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 such scholarship is awarded;

(iv) require scholarship recipients to maintain satisfactory academic progress; and

(v) require that—

(I) 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 such recipient is attending, or who voluntarily terminates academic training before graduation from the educational program for which the scholarship was awarded shall be liable to the United States for repayment within 1 year after the date of such default of all scholarship funds paid to such recipient and to the institution of higher education on the behalf of such recipient, provided that the repayment period may be extended by the Secretary if the Secretary determines it necessary, as established by regulation; and

(II) 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 shall be liable to the United States for an amount equal to—

(aa) the total amount of the scholarship received by such recipient under this section; and

(bb) the interest on such amounts which would be payable if at the time the scholarship was received such scholarship was a loan bearing interest at the maximum legally prevailing rate;

(13) provide an annual report to Congress on the activities carried out under paragraphs (10), (11), and (12); and

(14) perform other duties as assigned by the Secretary.

(b) DEFINITIONS.—In this section:

(1) 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).

(2) 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).

(3) HAWAIIAN NATIVE-SERVING[15] INSTITUTION.—The term "Hawaiian native-serving[15] institution" has the meaning given the term in section 317 of the Higher Education Act of 1965 (20 U.S.C. 1059d).

(4) HISPANIC-SERVING INSTITUTION.—The term "Hispanic-serving institution" has the meaning given that term in section 502 of the Higher Education Act of 1965 (20 U.S.C. 1101a).

(5) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term "historically Black college or university" has the meaning given the term "part B institution" in section 322(2) of the Higher Education Act of 1965 (20 U.S.C. 1061(2)).

(6) TRIBAL COLLEGE OR UNIVERSITY.—The term "Tribal College or University" has the meaning given that term in section 316(b) of the Higher Education Act of 1965 (20 U.S.C. 1059c(b)).

SEC. 1924. [6 U.S.C. 593] HIRING AUTHORITY.

In hiring personnel for the Office, the Secretary shall have the hiring and management authorities provided in section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note). The term of appointments for employees under subsection (c)(1) of such section may not exceed 5 years before granting any extension under subsection (c)(2) of such section.

SEC. 1925. [6 U.S.C. 594] TESTING AUTHORITY.

(a) IN GENERAL.—The Director 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 missions identified in section 1923. Any such 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, the provisions of section 309. The Office may direct that private sector entities utilizing Government facilities in accordance with this section pay an appropriate fee to the agency that owns or operates those facilities to defray additional costs to the Government resulting from such 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 in-

[15] The reference for the term "Hawaiian native-serving" in both the heading and the text of section 1902(b)(3) probably should be to "Native Hawaiian-serving".

direct 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 such services.

SEC. 1926. [6 U.S.C. 596] CONTRACTING AND GRANT MAKING AUTHORITIES.

The Secretary, acting through the Assistant Secretary, in carrying out the responsibilities under section 1923, 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 1923 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 1 or more federally funded research and development centers to provide independent analysis of homeland security issues and carry out other responsibilities under this title.

SEC. 1927. [6 U.S.C. 596a] JOINT ANNUAL INTERAGENCY REVIEW OF GLOBAL NUCLEAR DETECTION ARCHITECTURE.

(a) 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 such 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 of nuclear or radiological detection technologies under the global nuclear detection architecture by that agency, office, or entity;

(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;

(ii) attaches, as an appendix to the Joint Interagency Annual Review, the most current version of such strategy and plan; and

(iii) includes 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.

(b) 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 (a) 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.

(c) DEFINITION.—In this section, the term "global nuclear detection architecture" means the global nuclear detection architecture developed under section 1923.

SEC. 1928. [6 U.S.C. 596b] SECURING THE CITIES PROGRAM.

(a) ESTABLISHMENT.—The Secretary, through the Assistant Secretary, shall establish a program, to be known as the "Securing the Cities" or "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 operations, 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 high-risk urban areas under section 2003.

(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 any change to a jurisdiction previously designated under that paragraph.

(d) ACCOUNTABILITY.—

(1) IMPLEMENTATION PLAN.—

(A) IN GENERAL.—The Secretary shall develop, in consultation 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 one year after the date of the enactment of the Countering Weapons of Mass Destruction Act of 2018, the Secretary shall submit to the appropriate congressional committees and the Comptroller General of the United States the implementation plan required by subparagraph (A).

(2) REPORT REQUIRED.—Not later than one 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)(ii); and

(B) proposals for any 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 any 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 of the United States shall submit to the appropriate congressional committees 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 any changes to the structure or requirements of the STC program, the Assistant Secretary shall—

(A) consult with the 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.

Subtitle C—Chief Medical Officer

SEC. 1931. [6 U.S.C. 597] CHIEF MEDICAL OFFICER.

(a) IN GENERAL.—There is in the Office a Chief Medical Officer, who shall be appointed by the President. The Chief Medical Officer shall report to the Assistant Secretary.

(b) QUALIFICATIONS.—The individual appointed as Chief Medical Officer shall be a licensed physician possessing a demonstrated ability in and knowledge of medicine and public health.

(c) RESPONSIBILITIES.—The Chief Medical Officer shall have the responsibility within 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 the 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 such other duties relating to such responsibilities as the Secretary may require.

SEC. 1932. [6 U.S.C. 597a] MEDICAL COUNTERMEASURES.

(a) 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.

(b) OVERSIGHT.—The Secretary, acting through the Chief Medical Officer of the Department, shall—

(1) provide programmatic oversight of the medical countermeasures program established under subsection (a); 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.

(c) MEDICAL COUNTERMEASURES WORKING GROUP.—The Secretary, acting through the Chief Medical Officer of the Department, 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.

(d) MEDICAL COUNTERMEASURES MANAGEMENT.—Not later than 120 days after the date on which appropriations are made available to carry out subsection (a), 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 such methodology shall be reevaluated;

(2) a replenishment plan; and

(3) inventory tracking, reporting, and reconciliation procedures for existing stockpiles and new medical countermeasure purchases.

(e) TRANSFER.—Not later than 120 days after the date of enactment of this section, the Secretary shall transfer all medical countermeasures-related programmatic and personnel resources from the Under Secretary for Management to the Chief Medical Officer.

(f) STOCKPILE ELEMENTS.—In determining the types and quantities of medical countermeasures to stockpile under subsection (d), the Secretary, acting through the Chief Medical Officer of the Department—

(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.

(g) BRIEFING.—Not later than 180 days after the date of enactment of this section, 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 (d); and

(2) implementation of the requirements of this section.

(h) DEFINITION.—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.

TITLE XX—HOMELAND SECURITY GRANTS

SEC. 2001. [6 U.S.C. 601] DEFINITIONS.

In this title, the following definitions shall apply:

(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) any 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)(I) that is located on or near an international border or a coastline bordering an ocean (including the Gulf of Mexico) or international waters;

(II) that is located within 10 miles of a system or asset included on the prioritized critical infrastructure list established under section 2214(a)(2) or has such a system or asset within its territory;

(III) that is located within or contiguous to 1 of the 50 most populous metropolitan statistical areas in the United States; or

(IV) the jurisdiction of which includes not less than 1,000 square miles of Indian country, as that term is defined in section 1151 of title 18, United States Code; and

(iv) that certifies to the Secretary that a State has not provided funds under section 2003 or 2004 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 2003(b)(3)(A).

(7) INDIAN TRIBE.—The term "Indian tribe" has the meaning given that term in section 4(e) of the Indian Self-Determination 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 210A(j)), 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 209; 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 646(a) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 746(a)).

(14) TRIBAL GOVERNMENT.—The term "tribal government" means the government of an Indian tribe.

Subtitle A—Grants to States and High-Risk Urban Areas

SEC. 2002. [6 U.S.C. 603] HOMELAND SECURITY GRANT PROGRAMS.

(a) GRANTS AUTHORIZED.—The Secretary, through the Administrator, may award grants under sections 2003, 2004, and 2009 to State, local, and tribal governments.

(b) PROGRAMS NOT AFFECTED.—This subtitle 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.

(4) Grants to protect critical infrastructure, including port security grants authorized under section 70107 of title 46, United States Code, and the grants authorized under title XIV and XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 and the amendments made by such titles.

(5) The Metropolitan Medical Response System authorized under section 635 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 723).

(6) The Interoperable Emergency Communications Grant Program authorized under title XVIII.

(7) Grant programs other than those administered by the Department.

(c) RELATIONSHIP TO OTHER LAWS.—

(1) IN GENERAL.—The grant programs authorized under sections 2003 and 2004 shall supercede 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 section 2003 or 2004 shall be governed by the terms of this subtitle and not by any other provision of law.

SEC. 2003. [6 U.S.C. 604] URBAN AREA SECURITY INITIATIVE.

(a) ESTABLISHMENT.—There is established an 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 Administrator 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 Administrator 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 2007(a)(1); 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 Administrator 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) DESIGNATION.—

(i) IN GENERAL.—For each fiscal year, after conducting the initial assessment under paragraph (2), and based on that assessment, the Administrator shall designate high-risk urban areas that may submit applications for grants under this section.

(ii) ADDITIONAL AREAS.—Notwithstanding paragraph (2), the Administrator may—

(I) in any case where an eligible metropolitan area consists of more than 1 metropolitan division (as that term is defined by the Office of Management and Budget) designate more than 1 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 Administrator of the rel-

ative threat, vulnerability, and consequences from acts of terrorism faced by the area.

(iii) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed to require the Administrator to—

(I) designate all eligible metropolitan areas that submit information to the Administrator 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) IN GENERAL.—In designating high-risk urban areas under subparagraph (A), the Administrator shall determine which jurisdictions, at a minimum, shall be included in each high-risk urban area.

(ii) ADDITIONAL JURISDICTIONS.—A high-risk urban area designated by the Administrator may, in consultation with the State or States in which such 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) such information in support of the application as the Administrator 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 such 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 Administrator, 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 Administrator 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 Administrator approves the application of a high-risk urban area for a grant under this section, the Administrator 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 that 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 Administrator shall distribute to each such 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 Administrator 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 Administrator that the State has made available to the applicable high-risk urban area the required funds under paragraph (2).

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for grants under this section—

(1) $850,000,000 for fiscal year 2008;

(2) $950,000,000 for fiscal year 2009;

(3) $1,050,000,000 for fiscal year 2010;

(4) $1,150,000,000 for fiscal year 2011;

(5) $1,300,000,000 for fiscal year 2012; and

(6) such sums as are necessary for fiscal year 2013, and each fiscal year thereafter.

SEC. 2004. [6 U.S.C. 605] STATE HOMELAND SECURITY GRANT PROGRAM.

(a) ESTABLISHMENT.—There is established 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 such information in support of the application as the Administrator may reasonably require.

(2) MINIMUM CONTENTS OF APPLICATION.—The Administrator 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 Administrator 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 Administrator extend the period under paragraph (1) for an additional period of time. The Administrator may approve such a request if the Administrator 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) shall not apply to the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of 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 such distribution may petition the Administrator 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, such States shall submit to the Administrator 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 Administrator shall ensure that—

(A) except as provided in subparagraph (B), each State receives, from the funds appropriated for the State Homeland Security Grant Program established under this section, not less than an amount equal to—

(i) 0.375 percent of the total funds appropriated for grants under this section and section 2003 in fiscal year 2008;

(ii) 0.365 percent of the total funds appropriated for grants under this section and section 2003 in fiscal year 2009;

(iii) 0.36 percent of the total funds appropriated for grants under this section and section 2003 in fiscal year 2010;

(iv) 0.355 percent of the total funds appropriated for grants under this section and section 2003 in fiscal year 2011; and

(v) 0.35 percent of the total funds appropriated for grants under this section and section 2003 in fiscal year 2012 and in each fiscal year thereafter; and

(B) for each fiscal year, American Samoa, the Commonwealth of 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 2003.

(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.

(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for grants under this section—

(1) $950,000,000 for each of fiscal years 2008 through 2012; and

(2) such sums as are necessary for fiscal year 2013, and each fiscal year thereafter.

SEC. 2005. [6 U.S.C. 606] GRANTS TO DIRECTLY ELIGIBLE TRIBES.

(a) IN GENERAL.—Notwithstanding section 2004(b), the Administrator may award grants to directly eligible tribes under section 2004.

(b) TRIBAL APPLICATIONS.—A directly eligible tribe may apply for a grant under section 2004 by submitting an application to the Administrator that includes, as appropriate, the information required for an application by a State under section 2004(b).

(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 2004 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 such 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 Administrator, in writing, of that fact; and

(B) provide an explanation of the reason for not supporting the application.

(d) FINAL AUTHORITY.—The Administrator shall have final authority to approve any application of a directly eligible tribe. The Administrator 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 Administrator shall allocate funds to directly eligible tribes in accordance with the factors applicable to allocating funds among States under section 2007.

(f) DISTRIBUTION OF AWARDS TO DIRECTLY ELIGIBLE TRIBES.—If the Administrator awards funds to a directly eligible tribe under this section, the Administrator 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 Administrator 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 2004, not less than an amount equal to 0.1 percent of the total funds appropriated for grants under sections 2003 and 2004.

(2) EXCEPTION.—This subsection shall not apply in any fiscal year in which the Administrator—

(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 2004 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 2004 may receive funds for other purposes under a grant from the State or States within the boundaries of which any part of such 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 shall be responsible for allocating grant funds received under section 2004 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 2004, 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 2004.

(k) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to affect the authority of an Indian tribe that receives funds under this subtitle.

SEC. 2006. [6 U.S.C. 607] TERRORISM PREVENTION.

(a) LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM.—

(1) IN GENERAL.—The Administrator shall ensure that not less than 25 percent of the total combined funds appropriated for grants under sections 2003 and 2004 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 210A(i);

(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 Administrator.

(3) PARTICIPATION OF UNDERREPRESENTED COMMUNITIES IN FUSION CENTERS.—The Administrator shall ensure that grant funds described in paragraph (1) are used to support the participation, as appropriate, of law enforcement and other emergency response providers from rural and other underrepresented communities at risk from acts of terrorism in fusion centers.

(b) OFFICE FOR STATE AND LOCAL LAW ENFORCEMENT.—

(1) ESTABLISHMENT.—There is established in the Policy Directorate of the Department an Office for State and Local Law Enforcement, which shall be headed by an Assistant Secretary for State and Local Law Enforcement.

(2) QUALIFICATIONS.—The Assistant Secretary for State and Local Law Enforcement 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 506(c)(2), 821, and 888(d), 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 manmade 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 Administrator to ensure that law enforcement and terrorism-focused grants to State, local, and tribal government agencies, including grants under sections 2003 and 2004, 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 Science and Technology Directorate, 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 Administrator, 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, supercede, or replace the responsibilities, authorities, or role of the Administrator.

SEC. 2007. [6 U.S.C. 608] PRIORITIZATION.

(a) IN GENERAL.—In allocating funds among States and high-risk urban areas applying for grants under section 2003 or 2004, 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 Administrator 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 Administrator; 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 Administrator 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) Such other types of threat determined relevant by the Administrator.

SEC. 2008. [6 U.S.C. 609] USE OF FUNDS.

(a) PERMITTED USES.—The Administrator shall permit the recipient of a grant under section 2003 or 2004 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(3) of the Energy Policy Act of 2005 (42 U.S.C. 15801(3))), 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 section 512 of this Act and section 648 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 748);

(3) protecting a system or asset included on the prioritized critical infrastructure list established under section 2214(a)(2);

(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 210A(i);

(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 such analysts are current or new full-time employees or contract employees;

(12) paying expenses directly related to administration of the grant, except that such expenses may not exceed 3 percent of the amount of the grant;

(13) 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 any online service (as defined in section 3 of the DOTGOV Online Trust in Government Act of 2020) to the.gov internet domain; and

(15) any other appropriate activity, as determined by the Administrator.

(b) LIMITATIONS ON USE OF FUNDS.—

(1) IN GENERAL.—Funds provided under section 2003 or 2004 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 2003 or 2004 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 2003 or 2004, the Administrator 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 2003 or 2004 for personnel costs in accordance with paragraph (2) of this subsection, the Administrator may not—

(i) impose a limit on the amount of the award that may be used to pay for personnel, or personnel-re-

lated, 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 2003 or 2004 are used for paying salary or benefits of a qualified intelligence analyst under subsection (a)(10), the Administrator shall make such amounts available without time 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 2003 or 2004 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 2003 or 2004 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 such buildings secure against acts of terrorism.

(ii) REQUIREMENTS FOR EXCEPTION.—No grant awarded under section 2003 or 2004 may be used for a purpose described in clause (i) unless—

(I) specifically approved by the Administrator;

(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 subtitle may not be used for recreational or social purposes.

(c) MULTIPLE-PURPOSE FUNDS.—Nothing in this subtitle shall be construed to prohibit State, local, or tribal governments from using grant funds under sections 2003, 2004, and 2009 in a manner that enhances preparedness for disasters unrelated to acts of terrorism, if such use assists such 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 2003 or 2004 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 subtitle. Any such 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 2003 or 2004 may petition the Administrator 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.—Upon request by the recipient of a grant under section 2003, 2004, or 2009, the Administrator may authorize the grant recipient to transfer all or part of the grant funds from uses specified in the grant agreement to other uses authorized under this section, if the Administrator determines that such transfer is in the interests of homeland security.

(f) EQUIPMENT STANDARDS.—If an applicant for a grant under section 2003 or 2004 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 647 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 747), the applicant shall include in its application an explanation of why such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed such standards.

SEC. 2009. [6 U.S.C. 609a] NONPROFIT SECURITY GRANT PROGRAM.

(a) ESTABLISHMENT.—There is established in the Department a program to be known as 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 such 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 and exempt from tax under section 501(a) of such Code; 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 such grant for any of the following uses:

(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) PERIOD OF PERFORMANCE.—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 2022 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 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 the date of enactment of this subsection, the Administrator shall ensure that within 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 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 provide 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 identify and 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) PAPERWORK REDUCTION ACT.—Chapter 35 of title 44, United States Code (commonly known as the "Paperwork Reduction Act"), 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 for grants under this section, of which—

(A) $180,000,000 each such fiscal year shall be for recipients in high-risk urban areas that receive funding under section 2003; and

(B) $180,000,000 each such fiscal year shall be for recipients in jurisdictions that do not so receive such funding.

(2) OPERATIONS 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.

Subtitle B—Grants Administration

SEC. 2021. [6 U.S.C. 611] 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, title IV, or title V of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et seq., and 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, title IV, or title V of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et seq., and 5191 et seq.)) that include or substantially affect parts or all of more than 1 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 2003 or 2004 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, as the case may be, and to assist in determining effective funding priorities for grants under such sections.

(2) COMPOSITION.—

(A) IN GENERAL.—The State planning committees and urban area working groups referred to in paragraph (1) shall include at least one representative from each of the following significant stakeholders:

(i) Local or tribal government officials.

(ii) Emergency response providers, which shall include representatives of the 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 education.

(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, as the case may be, shall be a representative group of individuals from the counties, cities, towns, and Indian tribes within 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, as the case may be, 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.

(c) SENSE OF CONGRESS.—It is the sense of Congress that, in order to ensure that the Nation is most effectively able to prevent, prepare for, protect against, and respond to all hazards, including natural disasters, acts of terrorism, and other man-made disasters—

(1) the Department should administer a coherent and coordinated system of both terrorism-focused and all-hazards grants;

(2) there should be a continuing and appropriate balance between funding for terrorism-focused and all-hazards preparedness, as reflected in the authorizations of appropriations for grants under the amendments made by titles I and II, as applicable, of the Implementing Recommendations of the 9/11 Commission Act of 2007; and

(3) with respect to terrorism-focused grants, it is necessary to ensure both that the target capabilities of the highest risk areas are achieved quickly and that basic levels of preparedness, as measured by the attainment of target capabilities, are achieved nationwide.

SEC. 2022. [6 U.S.C. 612] 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 Administrator a copy of the organization-wide financial and compliance audit report required under chapter 75 of title 31, United States Code.

(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 related to any grant administered by the Department.

(C) IMPROPER PAYMENTS.—Consistent with subchapter IV of chapter 33 of title 31, United States Code, for each of the grant programs under sections 2003 and 2004 of this title and section 662 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 762), the Administrator shall specify policies and procedures for—

(i) identifying activities funded under any such 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.—Not less than once every 2 years, the Administrator shall 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., and 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 Administrator, there are authorized to be appropriated to the Administrator for reviews under this paragraph—

(i) $8,000,000 for each of fiscal years 2008, 2009, and 2010; and

(ii) such sums as are necessary for fiscal year 2011, and each fiscal year thereafter.

(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 Administrator shall—

(A) ensure that any such State or high-risk urban area conducts or participates in exercises under section 648(b) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 748(b));

(B) use performance metrics in accordance with the comprehensive assessment system under section 649 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 749) and ensure that any such State or high-risk urban area regularly tests its progress against such metrics through the exercises required under subparagraph (A);

(C) use the remedial action management program under section 650 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 750); 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 652(c) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 752(c)).

(4) CONSIDERATION OF ASSESSMENTS.—In conducting program reviews and performance audits under paragraph (2), the Administrator and the Inspector General of the Department shall take into account the performance assessment elements required under paragraph (3).

(5) RECOVERY AUDITS.—The Administrator shall conduct a recovery audit under section 3352(i) of title 31, United States Code, for any grant administered by the Department with a total value of not less than $1,000,000, if the Administrator 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 Administrator finds that a recipient of a grant under this title has failed to substantially comply with any provision of law or with any regulations or guidelines of the Department regarding eligible expenditures, the Administrator 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 such other action as the Administrator determines appropriate.

(B) DURATION OF PENALTY.—The Administrator shall apply an appropriate penalty under subparagraph (A) until such time as the Administrator 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 2003 or 2004, 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 Ad-

ministrator 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 2003 or 2004 in that quarter;

(ii) the amount of funds received and expended under section 2003 or 2004 by that recipient in that quarter; and

(iii) a summary description of expenditures made by that recipient using such funds, and the purposes for which such 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 all such funds expended in compliance with section 2021(a)(1) 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) how the funds were used by each recipient or subgrantee during that fiscal year.

(2) ANNUAL REPORT.—Any State applying for a grant under section 2004 shall submit to the Administrator annually a State preparedness report, as required by section 652(c) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 752(c)).

(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 652(a) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 752(a)).

(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 such variable;

(ii) an explanation of how each such variable, as weighted, correlates to risk, and the basis for concluding there is such a correlation; and

(iii) any change in the methodologies from the previous fiscal year, including changes in variables considered, weighting of those variables, and computational methods.

(B) CLASSIFIED ANNEX.—The information required under subparagraph (A) shall be provided in unclassified form to the greatest extent possible, and may include a classified annex if necessary.

(C) DEADLINE.—For each fiscal year, the information required under subparagraph (A) shall be provided on the earlier of—

(i) October 31; or

(ii) 30 days before the issuance of any program guidance for grants administered by the Department.

(3) TRIBAL FUNDING REPORT.—At the end of each fiscal year, the Administrator shall submit to the appropriate committees of Congress a report setting forth the amount of funding provided during that fiscal year to Indian tribes under any grant program administered by the Department, whether provided directly or through a subgrant from a State or high-risk urban area.

SEC. 2023. [6 U.S.C. 613] IDENTIFICATION OF REPORTING REDUNDANCIES AND DEVELOPMENT OF PERFORMANCE METRICS.

(a) DEFINITION.—In this section, the term "covered grants" means grants awarded under section 2003, grants awarded under section 2004, and any other grants specified by the Administrator.

(b) INITIAL REPORT.—Not later than 90 days after the date of enactment of the Redundancy Elimination and Enhanced Performance for Preparedness Grants Act, the Administrator shall submit to the appropriate committees of Congress a report that includes—

(1) an assessment of redundant reporting requirements imposed by the Administrator on State, local, and tribal governments in connection with the awarding of grants, including—

(A) a list of each discrete item of data requested by the Administrator from grant recipients as part of the process of administering covered grants;

(B) identification of the items of data from the list described in subparagraph (A) that are required to be submitted by grant recipients on multiple occasions or to multiple systems; and

(C) identification of the items of data from the list described in subparagraph (A) that are not necessary to be collected in order for the Administrator to effectively and efficiently administer the programs under which covered grants are awarded;

(2) a plan, including a specific timetable, for eliminating any redundant and unnecessary reporting requirements identified under paragraph (1); and

(3) 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 1 year after the date on which the initial report is required to be submitted under subsection (b), and once every 2 years thereafter, the Administrator 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)(2);

(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)(3);

(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 649 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 749); 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, section 2022(a)(4), and section 649 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 749);

(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.—

(1) IN GENERAL.—Not later than 30 days after the enactment of Redundancy Elimination and Enhanced Performance for Preparedness Grants Act, the Administrator shall enter into a contract with the National Academy of Public Administration under which the National Academy of Public Administration shall assist the Administrator in studying, developing, and implementing—

(A) quantifiable performance measures and metrics to assess the effectiveness of grants administered by the Department, as required under this section and section 649

of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 749); and

(B) the plan required under subsection (b)(3).

(2) REPORT.—Not later than 1 year after the date on which the contract described in paragraph (1) is awarded, the Administrator shall submit to the appropriate committees of Congress a report that describes the findings and recommendations of the study conducted under paragraph (1).

(3) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Administrator such sums as may be necessary to carry out this subsection.

TITLE XXI—CHEMICAL FACILITY ANTI–TERRORISM STANDARDS

SEC. 2101. [6 U.S.C. 621] DEFINITIONS.

In this title—

(1) 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 2107;

(2) 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 thereto, at a threshold quantity set pursuant to relevant risk-related security principles; and

(B) is not an excluded facility;

(3) the term "covered chemical facility" means a facility that—

(A) the Secretary—

(i) identifies as a chemical facility of interest; and

(ii) based upon review of the facility's Top-Screen, determines meets the risk criteria developed under section 2102(e)(2)(B); and

(B) is not an excluded facility;

(4) 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 Safe Drinking Water 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) 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; 6 U.S.C. 121 note) that is in effect on the day before the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014; and

(B) a Federal Register notice or other published guidance relating to section 550 of the Department of Homeland Security Appropriations Act, 2007 that is in effect on the day before the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014;

(6) 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 2102(c)(4);

(7) 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 the 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) the term "guidance for expedited approval facilities" means the guidance issued under section 2102(c)(4)(B)(i);

(9) the term "risk assessment" means the Secretary's application of relevant risk criteria identified in section 2102(e)(2)(B);

(10) the term "terrorist screening database" means the terrorist screening database maintained by the Federal Government Terrorist Screening Center or its successor;

(11) the term "tier" has the meaning given the term in section 27.105 of title 6, Code of Federal Regulations, or any successor thereto;

(12) 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) the term "Top-Screen" has the meaning given the term in section 27.105 of title 6, Code of Federal Regulations, or any successor thereto; and

(14) the term "vulnerability assessment" means the identification of weaknesses in the security of a chemical facility of interest.

SEC. 2102. [6 U.S.C. 622] CHEMICAL FACILITY ANTI-TERRORISM STANDARDS PROGRAM.

(a) PROGRAM ESTABLISHED.—

(1) IN GENERAL.—There is in the Department a Chemical Facility Anti-Terrorism Standards Program, which shall be located in the Cybersecurity and Infrastructure Security Agency.

(2) REQUIREMENTS.—In carrying out the Chemical Facility Anti-Terrorism Standards Program, the Secretary shall—

(A) identify—

(i) chemical facilities of interest; and

(ii) covered chemical facilities;

(B) 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;

(C) establish risk-based performance standards designed to address high levels of security risk at covered chemical facilities; and

(D) require each covered chemical facility to—

(i) submit a security vulnerability assessment; and

(ii) 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 assessment 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)(2)(C).

(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 deter-

mines 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) 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 title.

(B) PREVIOUSLY APPROVED PLANS.—In the case of a covered chemical facility for which the Secretary approved a site security plan before the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, the Secretary may not require the facility to resubmit the site security plan solely by reason of the enactment of this title.

(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)(2)(D) 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.—Not later than 180 days after the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, 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 such security measure meets the risk-based performance standards.

(iii) APPLICABILITY OF OTHER LAWS TO DEVELOPMENT AND ISSUANCE OF INITIAL GUIDANCE.—During the period before the Secretary has met the deadline under clause (i), 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, United States Code;

(II) subchapter I of chapter 35 of title 44, United States Code; or

(III) section 2107(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 title and part 27 of title 6, Code of Federal Regulations, or any successor thereto, and the site security plan being submitted;

(ii) the site security plan includes the security measures required by subsection (b);

(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 of 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) IN GENERAL.—Not later than 120 days after the date described in clause (ii), 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).

(ii) DATE.—The date described in this clause is—

(I) for an expedited approval facility that was assigned to tier 3 or 4 under existing CFATS regulations before the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, the date that is 210 days after the date of enactment of that Act; 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 the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014.

(iii) 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 title, the Secretary may enforce compliance in accordance with section 2104.

(F) AMENDMENTS TO SITE SECURITY PLAN.—

(i) REQUIREMENT.—

(I) IN GENERAL.—If the owner or operator of an expedited approval facility amends a site secu-

rity plan submitted under subparagraph (A), the owner or operator shall submit the amended site security plan and a certification 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) 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, not later than 120 days after the date on which the owner or operator receives notice under subsection (e)(3).

(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 fa-

cility 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 2104(a)(1)(B).

(bb) EFFECT OF REVOCATION.—If the Secretary revokes the certification of an expedited approval facility under item (aa) by issuing an order under section 2104(a)(1)(B)—

(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 review under subsection (c)(1); 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 subsection (c)(1); 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)(2)(C) 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 DEVELOPMENT AND ISSUANCE OF INITIAL SITE SECURITY PLAN TEMPLATES AND RELATED GUIDANCE.—During the period before the Secretary has met the deadline under subparagraph (B)(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, United States Code;

(II) subchapter I of chapter 35 of title 44, United States Code; or

(III) section 2107(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.—Not later than 18 months after the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, 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.—Not later than 18 months after the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, 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)(2)(D);

(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) the term "nondepartmental"—

(I) with respect to personnel, means personnel that is 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; and

(ii) the term "nongovernmental"—

(I) with respect to personnel, means personnel that is 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 title 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 title.

(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 within 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 within 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 within 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 or certifications necessary to handle chemical-terrorism vulnerability in-

formation (as defined in section 27.105 of title 6, Code of Federal Regulations, or any successor thereto);

(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 such 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.—

(A) PERSONNEL SURETY PROGRAM.—For purposes of this title, 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 such feedback is necessary for the facility to be in compliance with regulations promulgated under this title; 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 such vetting by a covered chemical facility, or its designated representative, was inaccurate.

(B) PERSONNEL SURETY PROGRAM IMPLEMENTATION.—To the extent that a risk-based performance standard established under subsection (a) 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 such a 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 assessment of the threat posed by acceptance of such 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 title, 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 title, 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 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 title.

(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 the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, and not less frequently than once every 6 months thereafter, 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 2101(3) 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.

SEC. 2103. [6 U.S.C. 623] PROTECTION AND SHARING OF INFORMATION.

(a) IN GENERAL.—Notwithstanding any other provision of law, information developed under this title, 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, United States Code.

(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 title, 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 title, provided that such 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 210A(j)(1)) 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 such 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 title, and related vulnerability or security information, shall be treated as if the information were classified information.

(e) AVAILABILITY OF INFORMATION.—Notwithstanding any other provision of law (including section 552(b)(3) of title 5, United States Code), section 552 of title 5, United States Code (commonly known as the "Freedom of Information Act") shall not apply to information protected from public disclosure pursuant to subsection (a) of this section.

(f) SHARING OF INFORMATION WITH MEMBERS OF CONGRESS.—Nothing in this section shall prohibit the Secretary from disclosing information developed under this title to a Member of Congress in response to a request by a Member of Congress.

SEC. 2104. [6 U.S.C. 624] CIVIL ENFORCEMENT.

(a) NOTICE OF NONCOMPLIANCE.—

(1) NOTICE.—If the Secretary determines that a covered chemical facility is not in compliance with this title, the Secretary shall—

(A) provide the owner or operator of the facility with—

(i) not later than 14 days after 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 title 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 title, 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 title shall be liable for a civil penalty under section 70119(a) of title 46, United States Code.

(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 title or the CFATS regulations shall be liable for a civil penalty under section 70119(a) of title 46, United States Code.

(c) EMERGENCY ORDERS.—

(1) IN GENERAL.—Notwithstanding subsection (a) or any site security plan or alternative security program approved under this title, if the Secretary determines that there is an imminent threat of death, serious illness, or severe personal injury, due to a violation of this title 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 that paragraph 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 title confers upon any person 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 title.

SEC. 2105. [6 U.S.C. 625] WHISTLEBLOWER PROTECTIONS.

(a) PROCEDURE FOR REPORTING PROBLEMS.—

(1) ESTABLISHMENT OF A REPORTING PROCEDURE.—Not later than 180 days after the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, 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 title.

(2) CONFIDENTIALITY.—The Secretary shall keep confidential the identity of an individual who submits a report under paragraph (1) and any such 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 2104 of this title if necessary to address any substantiated violation of a requirement under this title identified in the report.

(5) DUE PROCESS FOR FACILITY OWNER OR OPERATOR.—

(A) IN GENERAL.—If, upon the review described in paragraph (4), the Secretary determines that a violation of

a provision of this title, or a regulation prescribed under this title, has occurred, the Secretary may—

(i) institute a civil enforcement under section 2104(a) of this title; or

(ii) if the Secretary makes the determination under section 2104(c), 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 such 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 title 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, United States Code;

(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 title.

(d) PROTECTED INFORMATION.—All information contained in a report made under this subsection (a) shall be protected in accordance with section 2103.

SEC. 2106. [6 U.S.C. 626] RELATIONSHIP TO OTHER LAWS.

(a) OTHER FEDERAL LAWS.—Nothing in this title 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 title.

(b) STATES AND POLITICAL SUBDIVISIONS.—This title shall not preclude or deny any right of any State or political subdivision thereof 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 section, 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.

SEC. 2107. [6 U.S.C. 627] CFATS REGULATIONS.

(a) GENERAL AUTHORITY.—The Secretary may, in accordance with chapter 5 of title 5, United States Code, promulgate regulations or amend existing CFATS regulations to implement the provisions under this title.

(b) EXISTING CFATS REGULATIONS.—

(1) IN GENERAL.—Notwithstanding section 4(b) of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, each existing CFATS regulation shall remain in effect unless the Secretary amends, consolidates, or repeals the regulation.

(2) REPEAL.—Not later than 30 days after the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, the Secretary shall repeal any existing CFATS regulation that the Secretary determines is duplicative of, or conflicts with, this title.

(c) AUTHORITY.—The Secretary shall exclusively rely upon authority provided under this title in—

(1) determining compliance with this title;

(2) identifying chemicals of interest; and

(3) determining security risk associated with a chemical facility.

SEC. 2108. [6 U.S.C. 628] SMALL COVERED CHEMICAL FACILITIES.

(a) DEFINITION.—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 title.

(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 development of physical security best practices.

SEC. 2109. [6 U.S.C. 629] OUTREACH TO CHEMICAL FACILITIES OF INTEREST.

Not later than 90 days after the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, 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.

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

SEC. 2200. [6 U.S.C. 650] DEFINITIONS.

Except as otherwise specifically provided, in this title:

(1) AGENCY.—The term "Agency" means the Cybersecurity and Infrastructure Security Agency.

(2) 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.

(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 thereto.

(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—

(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 any critical infrastructure or protected system to resist such 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 thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such 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 communications that appear to be transmitted for the purpose of gathering technical information related 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 such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

(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, dis-

closure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

(B) does not include any 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 First Amendment to the Constitution of the United States, 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 by, 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 such information system not owned by—

(i) the private entity, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501), operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(10) DIRECTOR.—The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency.

(11) HOMELAND SECURITY ENTERPRISE.—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, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

(13) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "Information Sharing and Analysis Organization"

means any 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 related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(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, a compromise, or an incapacitation problem related 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, State, local, and Federal Governments, or any 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, United States Code; 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 the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(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" a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such 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;

(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such 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" has the meaning given the term in section 11103 of title 40, United States Code.

(22) RANSOMWARE 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 any such 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" (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

(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 thereof.

(28) SUPPLY CHAIN COMPROMISE.—The term "supply chain compromise" means an incident within the supply chain of an information system that an adversary can leverage, or does leverage, to jeopardize 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.

Subtitle A—Cybersecurity and Infrastructure Security

SEC. 2201. [6 U.S.C. 651] DEFINITION.

In this subtitle, the term "Cybersecurity Advisory Committee" means the advisory committee established under section 2219(a).

SEC. 2202. [6 U.S.C. 652] CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) REDESIGNATION.—

(1) IN GENERAL.—The National Protection and Programs Directorate of the Department shall, on and after the date of the enactment of this subtitle, be known as the "Cybersecurity and Infrastructure Security Agency".

(2) REFERENCES.—Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department.

(b) DIRECTOR.—

(1) IN GENERAL.—The Agency shall be headed by the Director, who shall report to the Secretary.

(2) QUALIFICATIONS.—

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

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

(ii) not fewer than five 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) as in effect on the day be-

fore the date of enactment of this subtitle in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Director of the Cybersecurity and Infrastructure Security Agency.

(c) RESPONSIBILITIES.—The Director shall—

(1) lead cybersecurity and critical infrastructure security programs, operations, and associated policy for the Agency, including national cybersecurity asset response activities;

(2) coordinate with Federal entities, including Sector-Specific Agencies, and non-Federal entities, including international entities, to carry out the cybersecurity and critical infrastructure activities of the Agency, as appropriate;

(3) 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, United States Code, and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113)), including by carrying out a periodic strategic assessment of the related programs and activities of the Agency to ensure such programs and activities contemplate the innovation of information systems and changes in cybersecurity risks and cybersecurity threats;

(4) coordinate a national effort to secure and protect against critical infrastructure risks, consistent with subsection (e)(1)(E);

(5) upon 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-Specific Agencies and other Federal departments and agencies;

(6) develop and utilize mechanisms for active and frequent collaboration between the Agency and Sector-Specific Agencies to ensure appropriate coordination, situational awareness, and communications with Sector-Specific Agencies;

(7) 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 Act;

(8) develop, coordinate, and implement—

(A) comprehensive strategic plans for the activities of the Agency; and

(B) risk assessments by and for the Agency;

(9) carry out emergency communications responsibilities, in accordance with title XVIII;

(10) carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate that outreach and engagement with critical infrastructure Sector-Specific Agencies, as appropriate; [16]

[16] Section 1717(a)(1)(A)(i) of Public Law 116-283 amends section 2202(c)(10) by striking "and" at the end. The amendment could not be carried out as such text does not appear in law. Section 1719(b) of such Public Law attempts to amend paragraph (10) in the same manner as section 1717(a)(1)(A)(i).

(11) 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;

(12) appoint a Cybersecurity State Coordinator in each State, as described in section 2217;

(13) carry out the duties and authorities relating to the.gov internet domain, as described in section 2215; and

(14) carry out such other duties and powers prescribed by law or delegated by the Secretary.

(d) DEPUTY DIRECTOR.—There shall be in the Agency a Deputy Director of the Cybersecurity and Infrastructure Security Agency who shall—

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

(2) report to the Director.

(e) CYBERSECURITY AND INFRASTRUCTURE SECURITY AUTHORITIES OF THE SECRETARY.—

(1) IN GENERAL.—The responsibilities of the Secretary relating to cybersecurity and infrastructure security shall include the following:

(A) To access, receive, and analyze 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 to integrate that information, in support of the mission responsibilities of the Department, in order 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) 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 those attacks and the feasibility and potential efficacy of various countermeasures to those attacks. At the discretion of the Secretary, such assessments may be carried out in coordination with Sector-Specific Agencies.

(C) To integrate 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) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this title, including obtaining that information from other Federal Government agencies.

(E) To develop, in coordination with the Sector-Specific 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 those systems.

(F) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government agencies, including Sector-Specific Agencies, and in cooperation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities.

(G) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information relating to homeland security within the Federal Government and between Federal Government agencies and State, local, tribal, and territorial government agencies and authorities.

(H) To disseminate, as appropriate, information analyzed by the Department within 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 in order to assist in the deterrence, prevention, or preemption of, or response to, terrorist attacks against the United States.

(I) To consult 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) To ensure that any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties.

(K) To request 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 such information.

(L) To establish and utilize, in conjunction with the Chief Information Officer of the Department, a secure com-

munications 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.

(M) To coordinate 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, 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.

(N) To coordinate with Federal, State, local, tribal, and territorial law enforcement agencies, and the private sector, as appropriate.

(O) To exercise the authorities and oversight of the functions, personnel, assets, and liabilities of those components transferred to the Department pursuant to section 201(g).

(P) To carry out the functions of the national cybersecurity and communications integration center under section 2209.

(Q) To carry out the requirements of the Chemical Facility Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate program established under subtitle J of title VIII, or any successor programs.

(R) To encourage and build cybersecurity awareness and competency across the United States and to develop, attract, and retain 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 sections 2203(b) and 2204(b), consistent with the responsibilities provided in paragraph (1), upon certifying to and briefing the appropriate congressional committees, and making available 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.—In order 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 described in this subparagraph 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-Specific Agencies; and

(viii) any other agency of the Federal Government that 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) BASIS.—The detail of personnel under this paragraph may be on a reimbursable or non-reimbursable basis.

(f) COMPOSITION.—The Agency shall be composed of the following divisions:

(1) The Cybersecurity Division, headed by an Executive Assistant Director.

(2) The Infrastructure Security Division, headed by an Executive Assistant Director.

(3) The Emergency Communications Division under title XVIII, headed by an Executive Assistant Director.

(g) CO-LOCATION.—

(1) IN GENERAL.—To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence.

(2) COORDINATION.—When establishing the central locations described in paragraph (1), the Director shall coordinate with component heads and the Under Secretary for Management to co-locate or partner on any new real property leases, renewing any occupancy agreements for existing leases, or agreeing to extend or newly occupy any Federal space or new construction.

(h) PRIVACY.—

(1) IN GENERAL.—There shall be a Privacy Officer of the Agency with primary responsibility for privacy policy and compliance for the Agency.

(2) RESPONSIBILITIES.—The responsibilities of the Privacy Officer of the Agency shall include—

(A) assuring 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;

(B) assuring that personal information contained in systems of records of the Agency is handled in full compliance as specified in section 552a of title 5, United States Code (commonly known as the "Privacy Act of 1974");

(C) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Agency; and

(D) 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.

(i) SAVINGS.—Nothing in this title may be construed as affecting in any manner the authority, existing on the day before the date of enactment of this title, 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 (6 U.S.C. 121 note; Public Law 114–94).

SEC. 2203. [6 U.S.C. 653] CYBERSECURITY DIVISION.

(a) ESTABLISHMENT.—

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

(2) EXECUTIVE ASSISTANT DIRECTOR.—The Cybersecurity Division shall be headed by an Executive Assistant Director for Cybersecurity (in this section referred to as the "Assistant Director"), who shall—

(A) be at the level of Assistant Secretary within 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 Director for Cybersecurity in any 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.

(b) FUNCTIONS.—The Executive Assistant Director shall—

(1) direct the cybersecurity efforts of the Agency;

(2) carry out activities, at the direction of the Director, related to the security of Federal information and Federal information systems consistent with law, including subchapter II of chapter 35 of title 44, United States Code, and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113));

(3) fully participate in the mechanisms required under section 2202(c)(7); and

(4) carry out such other duties and powers as prescribed by the Director.

SEC. 2204. [6 U.S.C. 654] INFRASTRUCTURE SECURITY DIVISION.

(a) ESTABLISHMENT.—

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

(2) EXECUTIVE ASSISTANT DIRECTOR.—The Infrastructure Security Division shall be headed by an Executive Assistant Director for Infrastructure Security (in this section referred to as the "Assistant Director"), who shall—

(A) be at the level of Assistant Secretary within 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 Director for Infrastructure Security in any 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.

(b) FUNCTIONS.—The Executive Assistant Director shall—

(1) direct the critical infrastructure security efforts of the Agency;

(2) carry out, at the direction of the Director, the Chemical Facilities Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate program established under subtitle J of title VIII, or any successor programs;

(3) fully participate in the mechanisms required under section 2202(c)(7); and

(4) carry out such other duties and powers as prescribed by the Director.

SEC. 2205. [6 U.S.C. 655] ENHANCEMENT OF FEDERAL AND NON-FEDERAL CYBERSECURITY.

In carrying out the responsibilities under section 2202, the Director of the Cybersecurity and Infrastructure Security Agency shall—

(1) as appropriate, provide to State and local government entities, and upon 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) in coordination with the Under Secretary for Emergency Preparedness and Response, crisis management support in response to threats to, or attacks on, critical information systems;

(2) as appropriate, provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, 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, United States Code.

SEC. 2206. [6 U.S.C. 656] NET GUARD.

The Director of the Cybersecurity and Infrastructure Security Agency 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.

SEC. 2207. [6 U.S.C. 657] CYBER SECURITY ENHANCEMENT ACT OF 2002.

(a) SHORT TITLE.—This section may be cited as the "Cyber Security Enhancement Act of 2002".

(b) AMENDMENT OF SENTENCING GUIDELINES RELATING TO CERTAIN COMPUTER CRIMES.—

(1) DIRECTIVE TO THE UNITED STATES SENTENCING COMMISSION.—Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this subsection, the United States Sentencing Commission shall review and, if appropriate, amend its guidelines and its policy statements applicable to persons convicted of an offense under section 1030 of title 18, United States Code.

(2) REQUIREMENTS.—In carrying out this subsection, the Sentencing Commission shall—

(A) ensure that the sentencing guidelines and policy statements reflect the serious nature of the offenses described in paragraph (1), the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses;

(B) consider the following factors and the extent to which the guidelines may or may not account for them—

(i) the potential and actual loss resulting from the offense;

(ii) the level of sophistication and planning involved in the offense;

(iii) whether the offense was committed for purposes of commercial advantage or private financial benefit;

(iv) whether the defendant acted with malicious intent to cause harm in committing the offense;

(v) the extent to which the offense violated the privacy rights of individuals harmed;

(vi) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;

(vii) whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and

(viii) whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person;

(C) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(D) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(E) make any necessary conforming changes to the sentencing guidelines; and

(F) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18, United States Code.

(c) STUDY AND REPORT ON COMPUTER CRIMES.—Not later than May 1, 2003, the United States Sentencing Commission shall submit a brief report to Congress that explains any actions taken by the Sentencing Commission in response to this section and includes any recommendations the Commission may have regarding statutory penalties for offenses under section 1030 of title 18, United States Code.

(d) EMERGENCY DISCLOSURE EXCEPTION.—

(1)

* * * * * * *

(2) REPORTING OF DISCLOSURES.—A government entity that receives a disclosure under section 2702(b) of title 18, United States Code, shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after the date of enactment of this Act.

* * * * * * *

SEC. 2208. [6 U.S.C. 658] CYBERSECURITY 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 meaning given that term in section 7103(a)(8) of title 5, United States Code.

(3) EXCEPTED SERVICE.—The term "excepted service" has the meaning given that term in section 2103 of title 5, United States Code.

(4) PREFERENCE ELIGIBLE.—The term "preference eligible" has the meaning given that term in section 2108 of title 5, United States Code.

(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 meaning given that term in section 2101a of title 5, United States Code.

(b) GENERAL AUTHORITY.—

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

(A) GENERAL AUTHORITY.—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, United States Code; 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 the provisions of 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 such employees by law or regulation.

(B) PREVAILING RATE SYSTEMS.—The Secretary may, consistent with section 5341 of title 5, United States Code, 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 that title.

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

(A) ADDITIONAL COMPENSATION BASED ON TITLE 5 AUTHORITIES.—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, United States Code.

(B) ALLOWANCES IN NONFOREIGN AREAS.—An employee in a qualified position whose rate of basic pay is fixed under paragraph (2)(A) shall be eligible for an allowance under section 5941 of title 5, United States Code, on the same basis and to the same extent as if the employee was an employee covered by such section 5941, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

(4) PLAN FOR EXECUTION OF AUTHORITIES.—Not later than 120 days after the date of enactment of this section, 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 1 year after the date of enactment of this section, and every year thereafter for 4 years, 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 such 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 within 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 shall be 3 years.

(e) INCUMBENTS OF EXISTING COMPETITIVE SERVICE POSITIONS.—

(1) IN GENERAL.—An individual serving in a position on the date of enactment of this section that is selected to be converted to a position in the excepted service under this section shall have the right to refuse such 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) STUDY AND REPORT.—Not later than 120 days after the date of enactment of this section, the National Protection and Programs Directorate 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, United States Code) 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.

SEC. 2209. [6 U.S.C. 659] NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITION.—The term "cybersecurity vulnerability" has the meaning given the term "security vulnerability" in section 2200.

(b) CENTER.—There is in the Department a national cybersecurity and communications integration center (referred to in this section as the "Center") to carry out certain responsibilities of the Di-

rector. The Center shall be located in the Cybersecurity and Infrastructure Security Agency. The head of the Center shall report to the Executive Assistant Director for Cybersecurity.

(c) 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 related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including the implementation of title I of the Cybersecurity Act of 2015;

(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 related 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 or could have consequential impacts across multiple sectors;

(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cyber threat indicators, defensivemeasures, cybersecurity risks, and incidents;

(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n), 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) upon 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, cybersecurityrisks, 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 related 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 related 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 of the Department, 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 such 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 in section 2240) submitted by covered entities (as defined in section 2240) and reports related to ransom payments (as defined in section 2240) submitted by covered entities (as defined in section 2240) in furtherance of the activities specified in sections 2202(e), 2203, and 2241, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.

(d) COMPOSITION.—

(1) IN GENERAL.—The Center shall be composed of—

(A) appropriate representatives of Federal entities, such as—

(i) sector-specific 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 within 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.

(e) PRINCIPLES.—In carrying out the functions under subsection (c), 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 222 to ensure that the Center follows the policies and procedures specified in subsections (b) and (d)(5)(C) of section 105 of the Cybersecurity Act of 2015.

(f) 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 upon 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.

(g) 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.

(2) CERTAIN ASSISTANCE OR INFORMATION.—The provision of certain assistance or information to, or inclusion in the Center, or any team or activity of the Center, of, one governmental or private entity 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.

(h) 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 title I of the Cybersecurity Act of 2015.

(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). Such reports shall be required until such capabilities are fully implemented.

(i) VOLUNTARY INFORMATION SHARING PROCEDURES.—

(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 any such 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 such a 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 such is appropriate for national security.

(2) VOLUNTARY INFORMATION SHARING RELATIONSHIPS.—A voluntary information sharing relationship under this subsection may be characterized as an agreement described in this paragraph.

(A) STANDARD AGREEMENT.—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) NEGOTIATED AGREEMENT.—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) EXISTING AGREEMENTS.—An agreement between the Center and a non-Federal entity that is entered into before the date of enactment of this subsection, or such an agreement that is in effect before such date, shall be deemed in compliance with the requirements of this subsection, notwithstanding any other provision or require-

ment 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.

(j) 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.

(k) REPORTS ON INTERNATIONAL COOPERATION.—Not later than 180 days after the date of enactment of this subsection, and periodically thereafter, the Secretary of Homeland Security 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 (c)(8).

(l) OUTREACH.—Not later than 60 days after the date of enactment of this subsection, 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 such sharing.

(m) CYBERSECURITY OUTREACH.—

(1) IN GENERAL.—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.

(2) DEFINITIONS.—For purposes of this subsection, the terms "small business concern" and "small business development center" have the meaning given such terms, respectively, under section 3 of the Small Business Act.

(n) 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.

(o) 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 such vulnerabilities exist because software or hardware is no longer supported by a vendor.

(p) SUBPOENA AUTHORITY.—

(1) DEFINITION.—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; and

(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 such 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 such covered device or system, the Director may issue a subpoena for the production of information necessary to identify and notify such entity at risk, in order to carry out a function authorized under subsection (c)(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, United States Code; and

(ii) for not more than 20 covered devices or systems.

(C) LIABILITY PROTECTIONS FOR DISCLOSING PROVIDERS.—The provisions of section 2703(e) of title 18, United States Code, shall apply to any 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 any such subpoena with the Department of Justice, including the Federal Bureau of Investigation, pursuant to inter-agency procedures which the Director, in coordination with the Attorney General, shall develop not later than 60 days after the date of the enactment of this subsection.

(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 (c)(12); and

(ii) subject to the limitations specified in this subsection.

(4) NONCOMPLIANCE.—If any person, partnership, corporation, association, or entity fails to comply with any duly served subpoena issued pursuant to this subsection, the Director may

request that the Attorney General seek enforcement of such subpoena in any judicial district in which such person, partnership, corporation, association, or entity resides, is found, or transacts business.

(5) NOTICE.—Not later than seven 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 such subpoena regarding such subpoena and the identified vulnerability.

(6) AUTHENTICATION.—

(A) IN GENERAL.—Any 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 such subpoena was issued by the Agency and has not been altered or modified since such issuance.

(B) INVALID IF NOT AUTHENTICATED.—Any 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 such subpoena.

(7) PROCEDURES.—Not later than 90 days after the date of the enactment of this subsection, 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 such a subpoena, including a requirement that the Agency not disseminate nonpublic information obtained through such a subpoena that identifies the party that is subject to such 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 such 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 such entity, which relates to the vulnerability which led to the issuance of such subpoena;

(ii) the Director determines that sharing the nonpublic information with another Federal department or agency is necessary to allow such 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 such 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 en-

forcement interests, consistent with such 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 such a subpoena for a cybersecurity purpose.

(C) The retention and destruction of nonpublic information obtained through such a subpoena, including—

(i) destruction of such information that the Director determines is unrelated to critical infrastructure immediately upon 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 such a 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 such a subpoena and each entity identified by information obtained under such a 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 Act.

(9) REVIEW OF PROCEDURES.—Not later than 1 year after the date of the enactment of this subsection, the Privacy Officer of the Agency shall—

(A) review the internal procedures established pursuant to paragraph (7) to ensure that—

(i) such procedures are consistent with fair information practices; and

(ii) the operations of the Agency comply with such 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) Such 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 such 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 so 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 pursuant to 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 THE 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 such paragraph.

(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 any other Federal department or agency for any purpose other than a cybersecurity purpose or for the purpose of enforcing a subpoena issued pursuant to this subsection.

(q) 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.

(r) COORDINATION ON CYBERSECURITY FOR SLTT ENTITIES.—

(1) COORDINATION.—The Center shall, upon 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—

(A) conduct exercises with SLTT entities;

(B) provide operational and technical cybersecurity training to SLTT entities to address cybersecurity risks or incidents, with or without reimbursement, related to—

(i) cyber threat indicators;

(ii) defensive measures;

(iii) cybersecurity risks;

(iv) vulnerabilities; and

(v) incident response and management;

(C) in order 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—

(i) cyber threat indicators;

(ii) defensive measures;

(iii) information about cybersecurity risks; and

(iv) information about incidents;

(D) provide SLTT entities notifications containing specific incident and malware information that may affect them or their residents;

(E) provide to, and periodically update, SLTT entities via an easily accessible platform and other means—

(i) information about tools;

(ii) information about products;

(iii) resources;

(iv) policies;

(v) guidelines;

(vi) controls; and

(vii) other cybersecurity standards and best practices and procedures related to information security, including, as appropriate, information produced by other Federal agencies;

(F) 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;

(G) provide operational and technical assistance to SLTT entities to implement tools, products, resources, policies, guidelines, controls, and procedures on information security;

(H) assist SLTT entities in developing policies and procedures for coordinating vulnerability disclosures consistent with international and national standards in the information technology industry; and

(I) promote cybersecurity education and awareness through engagements with Federal agencies and non-Federal entities.

(s) REPORT.—Not later than 1 year after the date of enactment of this subsection, 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.

SEC. 2210. [6 U.S.C. 660] CYBERSECURITY PLANS.

(a) DEFINITIONS.—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 such plan as necessary.

(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of De-

fense, a national security system, or an element of the intelligence community.

(c) CYBER INCIDENT RESPONSE PLAN.—The Director of the Cybersecurity and Infrastructure Security Agency 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 such 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) REQUIREMENT.—Not later than one year after the date of the enactment of this subsection, the Secretary, acting through the Director, shall, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, and other stakeholders, 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 (as such term is defined in section 2209).

(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 under section 502 of title 40, United States Code;

(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 such 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 44, United States Code (commonly known as the "Paperwork Reduction Act"), shall not apply to any action to implement this subsection.

SEC. 2211. [6 U.S.C. 661] CYBERSECURITY STRATEGY.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this section, the Secretary shall develop a departmental strategy to carry out cybersecurity responsibilities as set forth in 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 2209 (relating to the national cybersecurity and communications integration center).

(B) Cybersecurity investigations capabilities.

(C) Cybersecurity research and development.

(D) Engagement with international cybersecurity partners.

(c) 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 707; and

(2) include information on the roles and responsibilities of components and offices of the Department, to the extent practicable, to carry out such 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 such tasks.

(3) Metrics to evaluate performance of such tasks.

(e) CONGRESSIONAL OVERSIGHT.—The Secretary shall submit to Congress for assessment the following:

(1) A copy of the strategy required under subsection (a) upon issuance.

(2) A copy of the implementation plan required under subsection (d) upon 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.

SEC. 2212. [6 U.S.C. 662] CLEARANCES.

The Secretary shall make available the process of application for security clearances under Executive Order 13549 (75 Fed. Reg. 162; relating to a classified national security information program) 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 that the Secretary determines appropriate.

SEC. 2213. [6 U.S.C. 663] FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.

(a) DEFINITIONS.—In this section—

(1) the term "agency" has the meaning given the term in section 3502 of title 44, United States Code;

(2) the term "agency information" means information collected or maintained by or on behalf of an agency;

(3) the term "agency information system" has the meaning given the term in section 2210; and

(b) REQUIREMENT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, 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 prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such 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 such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency

from disclosing such 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 such 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.—Not later than 1 year after the date of enactment of this section, the Privacy Officer appointed under section 222, 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.

SEC. 2214. [6 U.S.C. 664] 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, any State, or any 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 such 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 any data submissions recommended by the official for inclusion in the database established under subsection (a)(1);

(D) examining the contents and identifying any submissions made by such an 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 such contents shall include the categorization of the contents—

(A) according to the sectors listed in 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 any 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 any other department or agency under this section by a Sector Risk Management Agency, including the assignment of a level of classification of such information, shall be binding on Congress, the Department, and that other Federal agency.

(d) REPORTS.—

(1) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, and annually 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 database established under subsection (a)(1) and the list established under subsection (a)(2).

(2) CONTENTS OF REPORT.—Each such 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 such 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 such 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 such list or in such database.

(E) If appropriate, the extent to which such database and such 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 any entity of the Department that meets with representatives of private sector industries for purposes of such coordination, for the purpose of ensuring the accuracy of such database and such list.

(G) Any 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 a consortium to be known as the "National Infrastructure Protection Consortium". The Consortium may advise the Secretary on the best way to identify, generate, organize, and maintain any 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 such database or such list.

SEC. 2215. [6 U.S.C. 665] DUTIES AND AUTHORITIES RELATING TO.GOV INTERNET DOMAIN.

(a) DEFINITION.—In this section, the term "agency" has the meaning given the term in section 3502 of title 44, United States Code.

(b) AVAILABILITY OF.GOV INTERNET DOMAIN.—The Director shall make.gov internet domain name registration services, as well as any supporting services described in subsection (e), 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 (c);

(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 (c); and

(3) without conditioning registration on participation in any separate service offered by the Director or any other Federal entity.

(c) 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 any purpose other than the administration of the.gov internet domain, the services described in subsection (e), and the requirements for establishing a.gov inventory described in subsection (h).

(d) 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 IDEA Act (44 U.S.C. 3501 note) and implementation guidance issued pursuant to that Act.

(e) SUPPORTING SERVICES.—

(1) IN GENERAL.—The Director may provide services to the entities described in subsection (b)(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 (b)(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.

(f) FEES.—

(1) IN GENERAL.—The Director may provide any service relating to the availability of the.gov internet domain program, including.gov internet domain name registration services described in subsection (b) and supporting services described in subsection (e), to entities described in subsection (b)(1) with or without reimbursement, including variable pricing.

(2) LIMITATION.—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.

(g) 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 (c), in particular on matters of privacy, accessibility, transparency, and technology modernization.

(h) .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) data may be collected 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, United States Code;

(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 Fed-

eral 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 the date of enactment of this section, 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.

SEC. 2216. [6 U.S.C. 665b] JOINT CYBER PLANNING OFFICE.

(a) ESTABLISHMENT OF OFFICE.—There is established in the Agency an office for joint cyber planning (in this section 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. The Office shall be headed by a senior official of the Agency selected by the Director.

(b) PLANNING AND EXECUTION.—In leading the development of plans for cyber defense operations pursuant to subsection (a), the head of the Office shall—

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

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

(3) 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 such entities have comparative advantages in limiting, mitigating, or defending against a cybersecurity risk or incident or coordinated, malicious cyber operation;

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

(5) 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;

(6) 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

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

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

(1) a central planning staff; and

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

(A) the Department;

(B) United States Cyber Command;

(C) the National Security Agency;

(D) the Federal Bureau of Investigation;

(E) the Department of Justice; and

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

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

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

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

(3) owners and operators of critical information systems;

(4) private entities; and

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

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

(f) DEFINITIONS.—In this section, the term "cyber defense operation" means the defensive activities performed for a cybersecurity purpose.

SEC. 2217. [6 U.S.C. 665c] CYBERSECURITY STATE COORDINATOR.

(a) 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.

(b) DUTIES.—The duties of a Cybersecurity State Coordinator appointed under subsection (a) 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, 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 within 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.

(c) 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.

SEC. 2218. [6 U.S.C. 665d] SECTOR RISK MANAGEMENT AGENCIES.

(a) 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—

(1) provide specialized sector-specific expertise to critical infrastructure owners and operators within its designated critical infrastructure sector or subsector of such sector; and

(2) support programs and associated activities of such sector or subsector of such sector.

(b) IMPLEMENTATION.—In carrying out this section, Sector Risk Management Agencies shall—

(1) coordinate with the Department and, as appropriate, other relevant Federal departments and agencies;

(2) collaborate with critical infrastructure owners and operators within the designated critical infrastructure sector or subsector of such sector; and

(3) coordinate with independent regulatory agencies, and State, local, Tribal, and territorial entities, as appropriate.

(c) 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 such sector and authorities under applicable law to—

(1) support sector risk management, in coordination with the Director, including—

(A) establishing and carrying out programs to assist critical infrastructure owners and operators within the designated sector or subsector of such sector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets, or within a region, sector, or subsector of such sector; and

(B) recommending security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets;

(2) assess sector risk, in coordination with the Director, including—

(A) identifying, assessing, and prioritizing risks within the designated sector or subsector of such sector, considering physical security and cybersecurity threats, vulnerabilities, and consequences; and

(B) supporting national risk assessment efforts led by the Department;

(3) sector coordination, including—

(A) serving as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities and responsibilities under this title;

(B) serving as the Federal Government coordinating council chair for the designated sector or subsector of such sector; and

(C) participating in cross-sector coordinating councils, as appropriate;

(4) facilitating, in coordination with the Director, the sharing with the Department and other appropriate Federal department of information regarding physical security and cybersecurity threats within the designated sector or subsector of such sector, including—

(A) 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 2209;

(B) facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators in the designated sector or subsector of such sector, in coordination with the Director of National Intelligence and the heads of other Federal departments and agencies, as appropriate;

(C) providing the Director, and facilitating awareness within the designated sector or subsector of such sector, of ongoing, and where possible, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of such sector or subsector of such sector; and

(D) supporting the reporting requirements of the Department under applicable law by providing, on an annual basis, sector-specific critical infrastructure information;

(5) supporting incident management, including—

(A) supporting, in coordination with the Director, incident management and restoration efforts during or following a security incident; and

(B) supporting the Director, upon request, in national cybersecurity asset response activities for critical infrastructure; and

(6) contributing to emergency preparedness efforts, including—

(A) coordinating with critical infrastructure owners and operators within the designated sector or subsector of such 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;

(B) 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 within the designated sector or subsector of such sector; and

(C) 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 or such sector.

SEC. 2219. [6 U.S.C. 665e] CYBERSECURITY ADVISORY COMMITTEE.

(a) ESTABLISHMENT.—The Secretary shall establish within the Agency a Cybersecurity Advisory Committee (referred to in this section as the "Advisory Committee").

(b) DUTIES.—

(1) IN GENERAL.—The 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.

(2) RECOMMENDATIONS.—

(A) IN GENERAL.—The 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.

(B) RECOMMENDATIONS OF SUBCOMMITTEES.—Recommendations agreed upon by subcommittees established under subsection (d) for any year shall be approved by the Advisory Committee before the Advisory Committee submits to the Director the annual report under paragraph (4) for that year.

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

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

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

(4) ANNUAL REPORT.—

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

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

(5) FEEDBACK.—Not later than 90 days after receiving any recommendation submitted by the Advisory Committee under paragraph (2), (3), or (4), the Director shall respond in writing to the Advisory Committee with feedback on the recommendation. Such a response shall include—

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

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

(6) CONGRESSIONAL NOTIFICATION.—Not less frequently than once per year after the date of enactment of this section, the Director shall provide to the Committee on Homeland Se-

curity 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 Advisory Committee.

(7) GOVERNANCE RULES.—The Director shall establish rules for the structure and governance of the Advisory Committee and all subcommittees established under subsection (d).

(c) MEMBERSHIP.—

(1) APPOINTMENT.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of the Cybersecurity Advisory Committee Authorization Act of 2020, the Director shall appoint the members of the Advisory Committee.

(B) COMPOSITION.—The membership of the Advisory Committee shall consist of not more than 35 individuals.

(C) REPRESENTATION.—

(i) IN GENERAL.—The membership of the Advisory Committee 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:

(aa) Defense.

(bb) Education.

(cc) Financial services and insurance.

(dd) Healthcare.

(ee) Manufacturing.

(ff) Media and entertainment.

(gg) Chemicals.

(hh) Retail.

(ii) Transportation.

(jj) Energy.

(kk) Information Technology.

(ll) Communications.

(mm) Other relevant fields identified by the Director.

(ii) PROHIBITION.—Not fewer than one member nor more than three members may represent any one category under clause (i)(III).

(iii) PUBLICATION OF MEMBERSHIP LIST.—The 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.

(2) TERM OF OFFICE.—

(A) TERMS.—The term of each member of the Advisory Committee shall be two years, except that a member may continue to serve until a successor is appointed.

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

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

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

(4) MEETINGS.—

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

(B) PUBLIC MEETINGS.—At least one of the meetings referred to in subparagraph (A) shall be open to the public.

(C) ATTENDANCE.—The Advisory Committee shall maintain a record of the persons present at each meeting.

(5) MEMBER ACCESS TO CLASSIFIED INFORMATION.—

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

(B) ACCESS.—Access to classified materials shall be managed in accordance with Executive Order No. 13526 of December 29, 2009 (75 Fed. Reg. 707), or any subsequent corresponding Executive Order.

(C) PROTECTIONS.—A member of the Advisory Committee shall protect all classified information in accordance with the applicable requirements for the particular level of classification of such information.

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

(6) CHAIRPERSON.—The Advisory Committee shall select, from among the members of the Advisory Committee—

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

(B) a member to serve as chairperson of each subcommittee of the Advisory Committee established under subsection (d).

(d) SUBCOMMITTEES.—

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

(A) Information exchange.

(B) Critical infrastructure.

(C) Risk management.

(D) Public and private partnerships.

(2) MEETINGS AND REPORTING.—Each subcommittee shall meet not less frequently than semiannually, and submit to the

Advisory Committee for inclusion in the annual report required under subsection (b)(4) information, including activities, findings, and recommendations, regarding subject matter considered by the subcommittee.

(3) SUBJECT MATTER EXPERTS.—The chair of the 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.

SEC. 2220. [6 U.S.C. 665f] CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Cybersecurity Education and Training Assistance Program (referred to in this section as "CETAP") is established within the Agency.

(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.

(b) REQUIREMENTS.—In carrying out CETAP, the Director shall—

(1) ensure that the program—

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

(B) conducts professional development sessions for teachers;

(C) develops resources for the teaching of cybersecurity-focused curricula described in subparagraph (A);

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

(E) 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;

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

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

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

(I) any other activity the Director determines necessary to meet the purpose described in subsection (a)(2); and

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

(c) BRIEFINGS.—

(1) 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.

(2) CONTENTS.—Each briefing conducted under paragraph (1) shall include—

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

(B) information on outreach and engagement efforts, including the activities described in subsection (b)(1)(E);

(C) information on any grants or cooperative agreements made pursuant to subsection (e), including how any such grants or cooperative agreements are being used to enhance cybersecurity education for underserved populations or communities;

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

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

(d) 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 to recruit and retain Agency personnel.

(e) 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 such 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—

(1) carry out the purposes of CETAP; and

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

SEC. 2220A. [6 U.S.C. 665g] STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

(a) DEFINITIONS.—In this section:

(1) CYBERSECURITY PLAN.—The term "Cybersecurity Plan" means a plan submitted by an eligible entity under subsection (e)(1).

(2) ELIGIBLE ENTITY.—The term "eligible entity" means a—

(A) State; or

(B) Tribal government.

(3) MULTI-ENTITY GROUP.—The term "multi-entity group" means a group of 2 or more eligible entities desiring a grant under this section.

(4) ONLINE SERVICE.—The term "online service" means any internet-facing service, including a website, email, virtual private network, or custom application.

(5) RURAL AREA.—The term "rural area" has the meaning given the term in section 5302 of title 49, United States Code.

(6) STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.—The term "State and Local Cybersecurity Grant Program" means the program established under subsection (b).

(7) TRIBAL GOVERNMENT.—The term "Tribal government" means the recognized governing body of any 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).

(b) ESTABLISHMENT.—

(1) IN GENERAL.—There is established within 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.

(2) 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.

(c) ADMINISTRATION.—The State and Local Cybersecurity Grant Program shall be administered in the same office of the Department that administers grants made under sections 2003 and 2004.

(d) USE OF FUNDS.—An eligible entity that receives a grant under this section and a local government that receives funds from a grant under this section, 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.

(e) CYBERSECURITY PLANS.—

(1) IN GENERAL.—An eligible entity applying for a grant under this section shall submit to the Secretary a Cybersecurity Plan for review in accordance with subsection (i).

(2) REQUIRED ELEMENTS.—A Cybersecurity Plan of an eligible entity shall—

(A) incorporate, to the extent practicable—

(i) 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

(ii) 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;

(B) describe, to the extent practicable, how the eligible entity will—

(i) 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;

(ii) 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;

(iii) 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;

(iv) 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;

(v) 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) cyber chain supply chain risk management best practices identified by the National Institute of Standards and Technology; and

(III) knowledge bases of adversary tools and tactics;

(vi) 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;

(vii) ensure continuity of operations of the eligible entity and, if the eligible entity is a State, local gov-

ernments 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;

(viii) 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;

(ix) 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;

(x) 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;

(xi) 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;

(xii) leverage cybersecurity services offered by the Department;

(xiii) implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;

(xiv) 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—

(aa) eligible entities that neighbor the jurisdiction of the eligible entity or, as appro-

priate, members of an Information Sharing and Analysis Organization; and

(bb) countries that neighbor the jurisdiction of the eligible entity;

(xv) ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the jurisdiction of the eligible entity; and

(xvi) distribute funds, items, services, capabilities, or activities to local governments under subsection (n)(2)(A), including the fraction of that distribution the eligible entity plans to distribute to rural areas under subsection (n)(2)(B);

(C) assess the capabilities of the eligible entity relating to the actions described in subparagraph (B);

(D) 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;

(E) outline, to the extent practicable, the necessary resources and a timeline for implementing the plan; and

(F) describe the metrics the eligible entity will use to measure progress towards—

(i) implementing the plan; and

(ii) 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.

(3) DISCRETIONARY ELEMENTS.—In drafting a Cybersecurity Plan, an eligible entity may—

(A) consult with the Multi-State Information Sharing and Analysis Center;

(B) 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

(C) 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.

(f) MULTI-ENTITY GRANTS.—

(1) 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.

(2) SATISFACTION OF OTHER REQUIREMENTS.—In order to be eligible for a multi-entity grant under this subsection, each eligible entity that comprises a multi-entity group shall have—

(A) a Cybersecurity Plan that has been reviewed by the Secretary in accordance with subsection (i); and

(B) a cybersecurity planning committee established in accordance with subsection (g).

(3) APPLICATION.—

(A) IN GENERAL.—A multi-entity group applying for a multi-entity grant under paragraph (1) shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(B) MULTI-ENTITY PROJECT PLAN.—An application for a grant under this section of a multi-entity group under subparagraph (A) shall include a plan describing—

(i) the division of responsibilities among the eligible entities that comprise the multi-entity group;

(ii) the distribution of funding from the grant among the eligible entities that comprise the multi-entity group; and

(iii) how the eligible entities that comprise the multi-entity group will work together to implement the Cybersecurity Plan of each of those eligible entities.

(g) PLANNING COMMITTEES.—

(1) IN GENERAL.—An eligible entity that receives a grant under this section shall establish a cybersecurity planning committee to—

(A) assist with the development, implementation, and revision of the Cybersecurity Plan of the eligible entity;

(B) approve the Cybersecurity Plan of the eligible entity; and

(C) assist with the determination of effective funding priorities for a grant under this section in accordance with subsections (d) and (j).

(2) COMPOSITION.—A committee of an eligible entity established under paragraph (1) shall—

(A) be comprised of representatives from—

(i) the eligible entity;

(ii) if the eligible entity is a State, counties, cities, and towns within the jurisdiction of the eligible entity; and

(iii) institutions of public education and health within the jurisdiction of the eligible entity; and

(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

(3) CYBERSECURITY EXPERTISE.—Not less than one-half of the representatives of a committee established under paragraph (1) shall have professional experience relating to cybersecurity or information technology.

(4) RULE OF CONSTRUCTION REGARDING EXISTING PLANNING COMMITTEES.—Nothing in this subsection 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—

(A) meets the requirements of this subsection; or

(B) may be expanded or leveraged to meet the requirements of this subsection, including through the formation of a cybersecurity planning subcommittee.

(5) RULE OF CONSTRUCTION REGARDING CONTROL OF INFORMATION SYSTEMS OF ELIGIBLE ENTITIES.—Nothing in this subsection shall be construed to permit a cybersecurity planning committee of an eligible entity that meets the requirements of this subsection to make decisions relating to information systems owned or operated by, or on behalf of, the eligible entity.

(h) SPECIAL RULE FOR TRIBAL GOVERNMENTS.—With respect to any requirement under subsection (e) or (g), the Secretary, in consultation with the Secretary of the Interior and Tribal governments, may prescribe an alternative substantively similar requirement 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 section.

(i) REVIEW OF PLANS.—

(1) REVIEW AS CONDITION OF GRANT.—

(A) IN GENERAL.—Subject to paragraph (3), before an eligible entity may receive a grant under this section, the Secretary, acting through the Director, shall—

(i) review the Cybersecurity Plan of the eligible entity, including any revised Cybersecurity Plans of the eligible entity; and

(ii) determine that the Cybersecurity Plan reviewed under clause (i) satisfies the requirements under paragraph (2).

(B) DURATION OF DETERMINATION.—In the case of a determination under subparagraph (A)(ii) that a Cybersecurity Plan satisfies the requirements under paragraph (2), the determination shall be effective for the 2-year period beginning on the date of the determination.

(C) ANNUAL RENEWAL.—Not later than 2 years after the date on which the Secretary determines under subparagraph (A)(ii) that a Cybersecurity Plan satisfies the requirements under paragraph (2), and annually thereafter, the Secretary, acting through the Director, shall—

(i) determine whether the Cybersecurity Plan and any revisions continue to meet the criteria described in paragraph (2); and

(ii) renew the determination if the Secretary, acting through the Director, makes a positive determination under clause (i).

(2) PLAN REQUIREMENTS.—In reviewing a Cybersecurity Plan of an eligible entity under this subsection, the Secretary, acting through the Director, shall ensure that the Cybersecurity Plan—

(A) satisfies the requirements of subsection (e)(2); and

(B) has been approved by—

(i) the cybersecurity planning committee of the eligible entity established under subsection (g); and

(ii) the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity.

(3) EXCEPTION.—Notwithstanding subsection (e) and paragraph (1) of this subsection, 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—

(A) the activities that will be supported by the grant are—

(i) integral to the development of the Cybersecurity Plan of the eligible entity; or

(ii) necessary to assist with activities described in subsection (d)(4), as confirmed by the Director; and

(B) the eligible entity will submit to the Secretary a Cybersecurity Plan for review under this subsection by September 30, 2023.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to provide authority to the Secretary to—

(A) 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

(B) condition the receipt of grants under this section on—

(i) participation in a particular Federal program; or

(ii) the use of a specific product or technology.

(j) LIMITATIONS ON USES OF FUNDS.—

(1) IN GENERAL.—Any entity that receives funds from a grant under this section may not use the grant—

(A) to supplant State or local funds;

(B) for any recipient cost-sharing contribution;

(C) to pay a ransom;

(D) for recreational or social purposes; or

(E) for any 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.

(2) 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 section uses the grant for the purposes for which the grant is awarded.

(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1)(A) shall be construed to prohibit the use of funds from a grant under this section awarded to a State, local, or Tribal government for otherwise permissible uses under this section 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.

(k) OPPORTUNITY TO AMEND APPLICATIONS.—In considering applications for grants under this section, 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.

(l) APPORTIONMENT.—For fiscal year 2022 and each fiscal year thereafter, the Secretary shall apportion amounts appropriated to carry out this section among eligible entities as follows:

(1) BASELINE AMOUNT.—The Secretary shall first apportion—

(A) 0.25 percent of such amounts to each of American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the United States Virgin Islands;

(B) 1 percent of such amounts to each of the remaining States; and

(C) 3 percent of such amounts to Tribal governments.

(2) REMAINDER.—The Secretary shall apportion the remainder of such amounts to States as follows:

(A) 50 percent of such remainder in the ratio that the population of each State, bears to the population of all States; and

(B) 50 percent of such 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) APPORTIONMENT AMONG TRIBAL GOVERNMENTS.—In determining how to apportion amounts to Tribal governments under paragraph (1)(C), the Secretary shall consult with the Secretary of the Interior and Tribal governments.

(4) MULTI-ENTITY GRANTS.—An amount received from a multi-entity grant awarded under subsection (f)(1) by a State or Tribal government that is a member of the multi-entity group shall qualify as an apportionment for the purpose of this subsection.

(m) FEDERAL SHARE.—

(1) IN GENERAL.—The Federal share of the cost of an activity carried out using funds made available with a grant under this section may not exceed—

(A) in the case of a grant to an eligible entity—

(i) for fiscal year 2022, 90 percent;

(ii) for fiscal year 2023, 80 percent;

(iii) for fiscal year 2024, 70 percent; and

(iv) for fiscal year 2025, 60 percent; and

(B) in the case of a grant to a multi-entity group—

(i) for fiscal year 2022, 100 percent;

(ii) for fiscal year 2023, 90 percent;

(iii) for fiscal year 2024, 80 percent; and

(iv) for fiscal year 2025, 70 percent.

(2) WAIVER.—

(A) IN GENERAL.—The Secretary may waive or modify the requirements of paragraph (1) if an eligible entity or multi-entity group demonstrates economic hardship.

(B) GUIDELINES.—The Secretary shall establish and publish guidelines for determining what constitutes economic hardship for the purposes of this subsection.

(C) CONSIDERATIONS.—In developing guidelines under subparagraph (B), the Secretary shall consider, with respect to the jurisdiction of an eligible entity—

(i) changes in rates of unemployment in the jurisdiction from previous years;

(ii) 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

(iii) any other factors the Secretary considers appropriate.

(3) WAIVER FOR TRIBAL GOVERNMENTS.—Notwithstanding paragraph (2), the Secretary, in consultation with the Secretary of the Interior and Tribal governments, may waive or modify the requirements of paragraph (1) for 1 or more Tribal governments if the Secretary determines that the waiver is in the public interest.

(n) RESPONSIBILITIES OF GRANTEES.—

(1) CERTIFICATION.—Each eligible entity or multi-entity group that receives a grant under this section shall certify to the Secretary that the grant will be used—

(A) for the purpose for which the grant is awarded; and

(B) in compliance with subsections (d) and (j).

(2) AVAILABILITY OF FUNDS TO LOCAL GOVERNMENTS AND RURAL AREAS.—

(A) IN GENERAL.—Subject to subparagraph (C), not later than 45 days after the date on which an eligible entity or multi-entity group receives a grant under this section, 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, consistent with the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multi-entity group—

(i) not less than 80 percent of funds available under the grant;

(ii) 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

(iii) with the consent of the local governments, grant funds combined with other items, services, capabilities, or activities having the total value of not less than 80 percent of the amount of the grant.

(B) AVAILABILITY TO RURAL AREAS.—In obligating funds, items, services, capabilities, or activities to local governments under subparagraph (A), 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 not less than—

(i) 25 percent of the amount of the grant awarded to the eligible entity;

(ii) 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

(iii) grant funds combined with other items, services, capabilities, or activities having the total value of not less than 25 percent of the grant awarded to the eligible entity.

(C) EXCEPTIONS.—This paragraph shall not apply to—

(i) any grant awarded under this section that solely supports activities that are integral to the development or revision of the Cybersecurity Plan of the eligible entity; or

(ii) the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the United States Virgin Islands, or a Tribal government.

(3) 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 paragraph (2).

(4) EXTENSION OF PERIOD.—

(A) IN GENERAL.—An eligible entity or multi-entity group may request in writing that the Secretary extend the period of time specified in paragraph (2) for an additional period of time.

(B) APPROVAL.—The Secretary may approve a request for an extension under subparagraph (A) 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.

(5) DIRECT FUNDING.—If an eligible entity does not make a distribution to a local government required under paragraph (2) in a timely fashion, the local government may petition the Secretary to request the Secretary to provide funds directly to the local government.

(6) LIMITATION ON CONSTRUCTION.—A grant awarded under this section may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities.

(7) CONSULTATION IN ALLOCATING FUNDS.—An eligible entity applying for a grant under this section 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 section.

(8) PENALTIES.—In addition to other remedies available to the Secretary, if an eligible entity violates a requirement of this subsection, the Secretary may—

(A) terminate or reduce the amount of a grant awarded under this section to the eligible entity; or

(B) distribute grant funds previously awarded to the eligible entity—

(i) 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

(ii) 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.

(o) CONSULTATION WITH STATE, LOCAL, AND TRIBAL REPRESENTATIVES.—In carrying out this section, 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 section, including guidance for Cybersecurity Plans;

(2) the study of risk-based formulas required under subsection (q)(4);

(3) the development of guidelines required under subsection (m)(2)(B); and

(4) any modifications described in subsection (q)(2)(D).

(p) 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 section, including an announcement to the eligible entity, the Secretary shall provide to the appropriate congressional committees notice of the announcement.

(q) REPORTS, STUDY, AND REVIEW.—

(1) ANNUAL REPORTS BY GRANT RECIPIENTS.—

(A) IN GENERAL.—Not later than 1 year after the date on which an eligible entity receives a grant under this section 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—

(i) implementing the Cybersecurity Plan of the eligible entity; and

(ii) 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.

(B) 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 section, 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—

(i) develop or revise a Cybersecurity Plan; or

(ii) assist with the activities described in subsection (d)(4).

(2) ANNUAL REPORTS TO CONGRESS.—Not less frequently than annually, the Secretary, acting through the Director, shall submit to Congress a report on—

(A) the use of grants awarded under this section;

(B) the proportion of grants used to support cybersecurity in rural areas;

(C) the effectiveness of the State and Local Cybersecurity Grant Program;

(D) any necessary modifications to the State and Local Cybersecurity Grant Program; and

(E) any progress made toward—

(i) developing, implementing, or revising Cybersecurity Plans; and

(ii) 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 section.

(3) PUBLIC AVAILABILITY.—

(A) IN GENERAL.—The Secretary, acting through the Director, shall make each report submitted under paragraph (2) publicly available, including by making each report available on the website of the Agency.

(B) REDACTIONS.—In making each report publicly available under subparagraph (A), 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, United States Code (commonly referred to as the "Freedom of Information Act").

(4) STUDY OF RISK-BASED FORMULAS.—

(A) 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 section, including—

(i) 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 section;

(ii) potential sources of data and information necessary for the implementation of a risk-based formula;

(iii) any obstacles to implementing a risk-based formula, including obstacles that require a legislative solution;

(iv) 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

(v) 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.

(B) INAPPLICABILITY OF PAPERWORK REDUCTION ACT.—The requirements of chapter 35 of title 44, United States Code (commonly referred to as the "Paperwork Reduction Act"), shall not apply to any action taken to carry out this paragraph.

(5) TRIBAL CYBERSECURITY NEEDS REPORT.—Not later than 2 years after the date of enactment of this section, the Secretary, acting through the Director, shall submit to Congress a report that—

(A) describes the cybersecurity needs of Tribal governments, which shall be determined in consultation with the Secretary of the Interior and Tribal governments; and

(B) includes any recommendations for addressing the cybersecurity needs of Tribal governments, including any necessary modifications to the State and Local Cybersecurity Grant Program to better serve Tribal governments.

(6) GAO REVIEW.—Not later than 3 years after the date of enactment of this section, the Comptroller General of the United States shall conduct a review of the State and Local Cybersecurity Grant Program, including—

(A) the grant selection process of the Secretary; and

(B) a sample of grants awarded under this section.

(r) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There are authorized to be appropriated for activities under this section—

(A) for fiscal year 2022, $200,000,000;

(B) for fiscal year 2023, $400,000,000;

(C) for fiscal year 2024, $300,000,000; and

(D) for fiscal year 2025, $100,000,000.

(2) TRANSFERS AUTHORIZED.—

(A) 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 paragraph (1) 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 section.

(B) ADDITIONAL APPROPRIATIONS.—Any funds transferred under subparagraph (A) shall be in addition to any funds appropriated to the Department or the components described in subparagraph (A) for salaries, expenses, and other administrative costs.

(s) TERMINATION.—

(1) IN GENERAL.—Subject to paragraph (2), the requirements of this section shall terminate on September 30, 2025.

(2) EXCEPTION.—The reporting requirements under subsection (q) shall terminate on the date that is 1 year after the date on which the final funds from a grant under this section are expended or returned.

SEC. 2220B. [6 U.S.C. 665h] NATIONAL CYBER EXERCISE PROGRAM.

(a) ESTABLISHMENT OF PROGRAM.—

(1) IN GENERAL.—There is established in the Agency the National Cyber Exercise Program (referred to in this section as the "Exercise Program") to evaluate the National Cyber Incident Response Plan, and other related plans and strategies.

(2) REQUIREMENTS.—

(A) 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.

(B) 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 such governments and private entities with the design, implementation, and evaluation of exercises that—

(I) conform to the requirements described in subparagraph (A);

(II) are consistent with any applicable national, State, local, or Tribal strategy or plan; and

(III) provide for systematic evaluation of readiness.

(3) 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.

(b) DEFINITIONS.—In this section:

(1) STATE.—The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

(2) PRIVATE ENTITY.—The term "private entity" has the meaning given such term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(c) 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 section 648 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 748).

SEC. 2220C.[17] [6 U.S.C. 665i] CYBERSENTRY PROGRAM.

(a) ESTABLISHMENT.—There is established 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, upon request and subject to the consent of such owner or operator.

(b) 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 such systems and detection of cybersecurity risks to such industrial control systems and other cybersecurity services, as appropriate, based on and subject to the agreement and consent of such 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 which could be exploited by adversaries attempting to gain access to such industrial control systems, and work with owners and operators to remediate such 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.

(c) PRIVACY REVIEW.—Not later than 180 days after the date of enactment of this section, the Privacy Officer of the Agency under section 2202(h) shall—

(1) review the policies, guidelines, and activities of CyberSentry for compliance with all applicable privacy laws, including such laws governing the acquisition, interception, retention, use, and disclosure of communities; and

[17] Section 2220C was added to the end of title XXII of this Act by section 1548(a) of division A of Public Law 117–81. Such amendment should have added this section at the end of subtitle A of title XXII. It's been placed here to reflect the probable intent of Congress.

(2) 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 such privacy laws.

(d) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this section, 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.

(e) SAVINGS.—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 under section 2702 of title 18, United States Code.

(f) DEFINITION.—In this section, the term "industrial control system" means an information system used to monitor and/or control industrial processes such as manufacturing, product handling, production, and distribution, including supervisory control and data acquisition (SCADA) systems used to monitor and/or control geographically dispersed assets, distributed control systems (DCSs), Human-Machine Interfaces (HMIs), and programmable logic controllers that control localized processes.

(g) TERMINATION.—The authority to carry out a program under this section shall terminate on the date that is seven years after the date of the enactment of this section.

SEC. 2220D. [6 U.S.C. 665k] 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") within 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) PAPERWORK REDUCTION ACT.—Chapter 35 of title 44, United States Code (commonly known as the "Paper-

work Reduction Act"), shall not apply to any rulemaking or information collection required under this section.

(B) FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.) 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 in section 8101 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 upon 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 COMMISSION RECOMMENDATIONS.—The Clearinghouse shall present, as determined in consultation with the of-

ficers 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 such 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 nongovernmental organizations, including organizations representing parents of elementary and secondary school students, representative from 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 with identifying relevant Clearinghouse resources related to supporting the implementation of Clearinghouse evidence-based practices and recommendations.

SEC. 2220E. [6 U.S.C. 665n] INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY TRAINING INITIATIVE.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Industrial Control Systems Cybersecurity Training Initiative (in this section referred to as the "Initiative") is established within the Agency.

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

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

(1) ensure the Initiative includes—

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

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

(C) 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 control systems technology; and

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

(2) engage in—

(A) collaboration with the National Laboratories of the Department of Energy in accordance with section 309;

(B) consultation with Sector Risk Management Agencies;

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

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

(c) REPORTS.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this section and annually thereafter, the Director 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.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include 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 such courses.

(C) The number of participants in each course.

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

(E) Information on the participation in such 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.

Subtitle B—Critical Infrastructure Information

SEC. 2221. [6 U.S.C. 101 note] SHORT TITLE.

This subtitle may be cited as the "Critical Infrastructure Information Act of 2002".

SEC. 2222. [6 U.S.C. 671] DEFINITIONS.

In this subtitle:

(1) AGENCY.—The term "agency" has the meaning given it in section 551 of title 5, United States Code.

(2) COVERED FEDERAL AGENCY.—The term "covered Federal agency" means the Department of Homeland Security.

(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term "critical infrastructure information" has the meaning given the term in section 2200.

(4) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.—The term "critical infrastructure protection program" means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.

(5) PROTECTED SYSTEM.—The term "protected system"—

(A) means any 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 any 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 any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency's exercise of legal authority to compel access to or submission of such 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 any action brought under the securities laws as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))—

(I) does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to sec-

tion 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(I)); and

(II) with respect to the submittal of critical infrastructure information, does not include any 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.

SEC. 2223. [6 U.S.C. 672] 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 of Homeland Security.

SEC. 2224. [6 U.S.C. 673] PROTECTION OF VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.

(a) PROTECTION.—

(1) IN GENERAL.—Notwithstanding any other provision of 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 (2)—

(A) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);

(B) shall not be subject to any 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 such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;

(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this subtitle, 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, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

(E) shall not, if provided to a State or local government or government agency—

(i) be made available pursuant to any State or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such 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 any applicable privilege or protection provided under law, such as trade secret protection.

(2) EXPRESS STATEMENT.—For purposes of paragraph (1), 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 provisions of 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.

(b) LIMITATION.—No communication of critical infrastructure information to a covered Federal agency made pursuant to this subtitle shall be considered to be an action subject to the requirements of chapter 10 of title 5, United States Code.

(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 any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law. For purposes of this section a permissible use of independently obtained information includes the disclosure of such information under section 2302(b)(8) of title 5, United States Code.

(d) TREATMENT OF VOLUNTARY SUBMITTAL OF INFORMATION.—The voluntary submittal to the Government of information or records that are protected from disclosure by this subtitle shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other provision of law.

(e) PROCEDURES.—

(1) IN GENERAL.—The Secretary of the Department of Homeland Security 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. The procedures shall be established not later than 90 days after the date of the enactment of this subtitle.

(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 such information as voluntarily submitted to the Government for purposes of and subject to the provisions of this subtitle;

(C) the care and storage of such information; and

(D) the protection and maintenance of the confidentiality of such information so as to permit the sharing of such 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 such manner as 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, and 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 subtitle coming to him in the course of this employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, 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 any 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 2223, to enter into a voluntary agreement to promote critical infrastructure security, including with any 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. App. 2158).

SEC. 2225. [6 U.S.C. 674] NO PRIVATE RIGHT OF ACTION.

Nothing in this subtitle may be construed to create a private right of action for enforcement of any provision of this Act.

Subtitle C—Declaration of a Significant Incident

SEC. 2231. [6 U.S.C. 677] SENSE OF CONGRESS.

It is the sense of Congress that—

(1) the purpose of this subtitle is to authorize the Secretary to declare that a significant incident has occurred and to establish the authorities that are provided under the declaration to respond to and recover from the significant incident; and

(2) the authorities established under this subtitle are intended to enable the Secretary to provide voluntary assistance to non-Federal entities impacted by a significant incident.

SEC. 2232. [6 U.S.C. 677a] DEFINITIONS.

For the purposes of this subtitle:

(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 2233(a)(1).

(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, United States Code.

(5) FUND.—The term "Fund" means the Cyber Response and Recovery Fund established under section 2234(a).

(6) INCIDENT.—The term "incident" has the meaning given the term in section 3552 of title 44, United States Code.

(7) RENEWAL.—The term "renewal" means a renewal of a declaration under section 2233(d).

(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, United States Code); or

(ii) an information system described in paragraph (2) or (3) of section 3553(e) of title 44, United States Code.

SEC. 2233. [6 U.S.C. 677b] 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 subtitle if the Secretary determines that—

(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.—Upon 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 upon 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) IN GENERAL.—Not later than 72 hours after a declaration or a renewal, the Secretary shall publish the declaration or renewal in the Federal Register.

(2) PROHIBITION.—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.—Any expenditure from the Fund for the purpose of paragraph (1)(B) shall be made from amounts available in the Fund, and amounts available in the Fund shall be in addition to any other appropriations available to the Cybersecurity and Infrastructure Security Agency for such purpose.

SEC. 2234. [6 U.S.C. 677c] CYBER RESPONSE AND RECOVERY FUND.

(a) IN GENERAL.—There is established a Cyber Response and Recovery Fund, which shall be available for—

(1) the coordination of activities described in section 2233(b);

(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 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 2233(f)(1)(B).

(b) DEPOSITS AND EXPENDITURES.—

(1) IN GENERAL.—Amounts shall be deposited into 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 such reimbursement.

(2) EXPENDITURES.—Any expenditure from the Fund for the purposes of this subtitle shall be made from amounts available in the Fund from a deposit described in paragraph (1), and amounts available in the Fund shall be in addition to any other appropriations available to the Cybersecurity and Infrastructure Security Agency for such purposes.

(c) SUPPLEMENT NOT SUPPLANT.—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.

SEC. 2235. [6 U.S.C. 677d] NOTIFICATION AND REPORTING.

(a) NOTIFICATION.—Upon 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;

(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 2233(b) that the Secretary anticipates the Director to 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, United States Code (commonly 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 (commonly known as the "Paperwork Reduction Act") 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.

SEC. 2236. [6 U.S.C. 677e] RULE OF CONSTRUCTION.

Nothing in this subtitle 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.

SEC. 2237. [6 U.S.C. 677f] AUTHORIZATION OF APPROPRIATIONS.

There are 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.

SEC. 2238. [6 U.S.C. 677g] SUNSET.

The authorities granted to the Secretary or the Director under this subtitle shall expire on the date that is 7 years after the date of enactment of this subtitle.

Subtitle D—Cyber Incident Reporting

SEC. 2240. [6 U.S.C. 681] DEFINITIONS.

In this subtitle:

(1) CENTER.—The term "Center" means the center established under section 2209.

(2) COUNCIL.—The term "Council" means the Cyber Incident Reporting Council described in section 2246.

(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 to section 2242(b).

(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 to section 2242(b).

(5) CYBER INCIDENT.—The term "cyber incident"—

(A) has the meaning given the term "incident" in section 2209; 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 2200.

(7) FEDERAL ENTITY The term "Federal entity" has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(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 CURRENCY ADDRESS.—The term "virtual currency address" means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.

SEC. 2241. [6 U.S.C. 681a] CYBER INCIDENT REVIEW.

(a) ACTIVITIES.—The Center shall—

(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and 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 to section 2245;

(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, 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 such 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 section 2242(a) and 2243 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 within 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 in section 2245, 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 with section 2245 and 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 to section 2243, or information received pursuant to a request for information or subpoena under section 2244, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

(b) INTERAGENCY 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 BRIEFING.—Not later than 60 days after the effective date of the final rule required under section 2242(b), and on the first 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 under sections 2242 and 2243 during 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 under sections 2242 and 2243, 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 under sections 2242 and 2243; and

(4) include an unclassified portion, but may include a classified component.

SEC. 2242. [6 U.S.C. 681b] 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 such date that such 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 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 of section 104(a) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, the requirements under paragraphs (1), (2), and (3) shall not apply to a covered entity required by law, regulation, or contract 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 to section 104(a) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

(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 paragraph;

(II) prevent the Agency from contacting an entity submitting information to another Federal agency that is provided to the Agency pursuant to section 104 of the Cyber Incident Reporting for Critical Infrastructure Act of 2022; 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 24 months after the date of enactment of this section, 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 is authorized to 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 under chapter 5 of title 5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

(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 such 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 such a 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 such a 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 in section 2240(14)(A).

(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 subtitle 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 such 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 such 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 such 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 such covered entity, or, where applicable, the service provider of such 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 subtitle.

(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 such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, that covered entity to assist with compliance with the requirements of this subtitle.

(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 such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such 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 thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

(B) the Agency to carry out—

(i) the enforcement provisions of section 2244, 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 to section 105(b) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(b)) and 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 pay-

ment, 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 under section 2244 when 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 subtitle.

(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 under section 871;

(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 44, United States Code, shall 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; relating to improving the nation's cybersecurity), 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.

SEC. 2243. [6 U.S.C. 681c] 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) of section 2242(a), 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) of section 2242(a) information that is not required to be included, but may enhance the situational awareness of cyber threats.

(c) APPLICATION OF SECTION 2245.—Section 2245 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 2242.

SEC. 2244. [6 U.S.C. 681d] NONCOMPLIANCE WITH REQUIRED REPORTING.

(a) PURPOSE.—In the event that a covered entity that is required to submit a report under section 2242(a) fails 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 such 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) of section 2241(a), that a covered entity has experienced a covered cyber incident or made a ransom payment but failed to report such cyber incident or payment to the Agency in accordance with section 2242(a), 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 in section 2242 including that section 2245 shall apply to such

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 2242.

(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 such information was requested, or received an inadequate response, the Director may issue to such covered entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2242 and any implementing regulations, and 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 such 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 such subpoena was issued by the Agency and has not been altered or modified since such 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 such subpoena.

(d) PROVISION OF CERTAIN INFORMATION TO ATTORNEY GENERAL.—

(1) IN GENERAL.—Notwithstanding section 2245(a)(5) and paragraph (b)(2) of this section, 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 such information to the Attorney General or the head of the appropriate Federal regu-

latory agency, who may use such 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 THE 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.

SEC. 2245. [6 U.S.C. 681e] INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

(a) DISCLOSURE, RETENTION, AND USE.—

(1) AUTHORIZED ACTIVITIES.—Information provided to the Agency pursuant to section 2242 or 2243 may 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 to section 2242 or 2243 or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

(2) AGENCY ACTIONS AFTER RECEIPT.—

(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon 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 such 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 to section 2242 shall 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 to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and 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 to section 2242, 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 subtitle 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) CLARIFICATION.—A report submitted to the Agency pursuant to section 2242 or 2243 may, 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 such systems.

(b) PROTECTIONS FOR REPORTING ENTITIES AND INFORMATION.—Reports describing covered cyber incidents or ransom payments submitted to the Agency by entities in accordance with section 2242, as well as voluntarily-submitted cyber incident reports submitted to the Agency pursuant to section 2243, 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 under section 552(b)(3) of title 5, United States Code (commonly known as the "Freedom of Information Act"), 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 shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 2242(a) that is submitted in conformance with this subtitle and the rule promulgated under section 2242(b), except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 2244(c)(2).

(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 subtitle or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such 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 thereof, provided that nothing in this subtitle 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 such report.

(d) SHARING WITH NON-FEDERAL ENTITIES.—The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 2242 available to critical infrastructure owners and operators and the general public.

(e) STORED COMMUNICATIONS ACT.—Nothing in this subtitle 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 under chapter 121 of title 18, United States Code (commonly known as the "Stored Communications Act").

SEC. 2246. [6 U.S.C. 681f] 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.