115TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
115–198

DEPARTMENT OF HOMELAND SECURITY AUTHORIZATION ACT OF 2017

JUNE 28, 2017.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. MCCAUL, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 2825]

The Committee on Homeland Security, to whom was referred the bill (H.R. 2825) to amend the Homeland Security Act of 2002 to make certain improvements in the laws administered by the Secretary of Homeland Security, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

The amendment is as follows:
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Department of Homeland Security Authorization Act of 2017" or the "DHS Authorization Act of 2017".

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

TITLE I—DEPARTMENT OF HOMELAND SECURITY HEADQUARTERS

Subtitle A—Headquarters Operations

SEC. 101. HOMELAND SECURITY ENTERPRISE DEFINED.

Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended—

(1) by redesignating paragraphs (9) through (20) as paragraphs (10) through (21), respectively; and

(2) by inserting after paragraph (8) the following new paragraph (9):

"(9) The term 'homeland security enterprise' means any relevant governmental or nongovernmental entity involved in homeland security, including a

Federal, State, or local government official, private sector representative, academic, or other policy expert.".

SEC. 102. FUNCTIONS AND COMPONENTS OF HEADQUARTERS OF DEPARTMENT OF HOMELAND SECURITY.

Section 102 of the Homeland Security Act of 2002 (6 U.S.C. 112) is amended—

(1) in subsection (c)—

(A) in the matter preceding paragraph (1), by striking "through the Office of State and Local Coordination (established under section 801)" and inserting "through the Office of Partnership and Engagement";

(B) in paragraph (2), by striking "and" after the semicolon at the end;

(C) in paragraph (3), by striking the period and inserting "; and"; and

(D) by adding at the end the following:

"(4) entering into agreements with governments of other countries, in consultation with the Secretary of State, and international nongovernmental organizations in order to achieve the missions of the Department."; and

(2) by adding at the end the following new subsection:

"(h) HEADQUARTERS.—

"(1) COMPONENTS.—There is in the Department a Headquarters. The Department Headquarters shall include each of the following:

"(A) The Office of the Secretary.

"(B) The Office of the Deputy Secretary.

"(C) The Executive Secretary.

"(D) The Management Directorate, including the Office of the Chief Financial Officer.

"(E) The Office of Strategy, Policy, and Plans.

"(F) The Office of the General Counsel.

"(G) The Office of the Chief Privacy Officer.

"(H) The Office for Civil Rights and Civil Liberties.

"(I) The Office of Operations Coordination.

"(J) The Office of Intelligence and Analysis.

"(K) The Office of Legislative Affairs.

"(L) The Office of Public Affairs.

"(M) The Office of the Inspector General.

"(N) The Office of the Citizenship and Immigration Services Ombudsman.

"(2) FUNCTIONS.—The Secretary, acting through the appropriate official of the Headquarters, shall—

"(A) establish an overall strategy to successfully further the mission of the Department;

"(B) establish initiatives that improve Department-wide operational performance;

"(C) establish mechanisms to—

"(i) ensure that components of the Department comply with Department policies and fully implement the strategies and initiatives of the Secretary; and

"(ii) require the head of each component of the Department and component chief officers to comply with such policies and implement such strategies and initiatives;

"(D) establish annual operational and management objectives to evaluate the performance of the Department;

"(E) ensure that the Department successfully meets operational and management performance objectives through conducting oversight of component agencies;

"(F) ensure that the strategies, priorities, investments, and workforce of Department components align with Department objectives;

"(G) establish and implement policies related to Department ethics and compliance standards;

"(H) establish and implement, in consultation with the Office of Civil Rights and Civil Liberties, policies which preserve individual liberty, fairness, and equality under the law;

"(I) manage and encourage shared services across Department components;

"(J) lead and coordinate interaction with Congress and other external organizations; and

"(K) carry out other such functions as the Secretary determines are appropriate.".

SEC. 103. REPEAL OF DIRECTOR OF SHARED SERVICES AND OFFICE OF COUNTERNARCOTICS ENFORCEMENT OF DEPARTMENT OF HOMELAND SECURITY.

(a) ABOLISHMENT OF DIRECTOR OF SHARED SERVICES.—

(1) ABOLISHMENT.—The position of Director of Shared Services of the Department of Homeland Security is abolished.

(2) CONFORMING AMENDMENT.—The Homeland Security Act of 2002 is amended by striking section 475 (6 U.S.C. 295).

(3) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 475.

(b) ABOLISHMENT OF THE OFFICE OF COUNTERNARCOTICS ENFORCEMENT.—

(1) ABOLISHMENT.—The Office of Counternarcotics Enforcement is abolished.

(2) CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 is amended—

(A) in subparagraph (B) of section 843(b)(1) (6 U.S.C. 413(b)(1)), by striking "by—" and all that follows through the end of that subparagraph and inserting "by the Secretary; and"; and

(B) by striking section 878 (6 U.S.C. 112).

(3) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 878.

SEC. 104. RESPONSIBILITIES AND FUNCTIONS OF CHIEF PRIVACY OFFICER.

(a) IN GENERAL.—Section 222 of the Homeland Security Act of 2002 (6 U.S.C. 142) is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1)—

(i) by inserting "to be the Chief Privacy Officer of the Department," after "in the Department,"; and

(ii) by striking "to the Secretary, to assume" and inserting "to the Secretary. Such official shall have";

(B) in paragraph (5), by striking "and" at the end;

(C) by striking paragraph (6); and

(D) by inserting after paragraph (5) the following new paragraphs:

"(6) developing guidance to assist components of the Department in developing privacy policies and practices;

"(7) establishing a mechanism to ensure such components are in compliance with Federal, regulatory, statutory, and Department privacy requirements, mandates, directives, and policies;

"(8) working with the Chief Information Officer of the Department to identify methods for managing and overseeing the records, management policies, and procedures of the Department;

"(9) working with components and offices of the Department to ensure that information sharing activities incorporate privacy protections;

"(10) serving as the Chief FOIA Officer of the Department for purposes of subsection (j) of section 552 of title 5, United States Code (popularly known as the Freedom of Information Act), to manage and process requests related to such section;

"(11) developing guidance on procedures to be followed by individuals making requests for information under section 552 of title 5, United States Code;

"(12) overseeing the management and processing of requests for information under section 552 of title 5, United States Code, within Department Headquarters and relevant Department component offices;

"(13) identifying and eliminating unnecessary and duplicative actions taken by the Department in the course of processing requests for information under section 552 of title 5, United States Code;

"(14) preparing an annual report to Congress that includes—

"(A) a description of the activities of the Department that affect privacy during the fiscal year covered by the report, including complaints of privacy violations, implementation of section 552a of title 5, United States Code (popularly known as the Privacy Act of 1974), internal controls, and other matters; and

"(B) the number of new technology programs implemented in the Department during the fiscal year covered by the report, the number of such programs that the Chief Privacy Officer has evaluated to ensure that privacy protections are considered and implemented, the number of such programs that effectively implemented privacy protections into new technology programs, and an explanation of why any new programs did not effectively implement privacy protections; and

"(15) carrying out such other responsibilities as the Secretary determines are appropriate, consistent with this section."; and

(2) by adding at the end the following new subsection:

"(f) REASSIGNMENT OF FUNCTIONS.—Notwithstanding subsection (a)(10), the Secretary may reassign the functions related to managing and processing requests for

information under section 552 of title 5, United States Code, to another officer within the Department, consistent with requirements of that section.".

SEC. 105. RESPONSIBILITIES OF CHIEF FINANCIAL OFFICER.

Section 702 of the Homeland Security Act of 2002 (6 U.S.C. 342) is amended—

(1) by redesignating subsections (b) and (c) as subsections (c) and (d), respectively; and

(2) by inserting after subsection (a) the following new subsection (b):

"(b) RESPONSIBILITIES.—The Chief Financial Officer, in consultation with the Under Secretary for Management and the Under Secretary for Intelligence and Analysis, as appropriate, shall—

"(1) oversee Department budget formulation and execution;

"(2) lead and provide guidance on performance-based budgeting practices for the Department to ensure that the Department and its components are meeting missions and goals;

"(3) lead cost-estimating practices for the Department, including the development of policies on cost estimating and approval of life cycle cost estimates;

"(4) coordinate with the Office of Strategy, Policy, and Plans to ensure that the development of the budget for the Department is compatible with the long-term strategic plans, priorities, and policies of the Secretary;

"(5) develop financial management policy for the Department and oversee the implementation of such policy, including the establishment of effective internal controls over financial reporting systems and processes throughout the Department;

"(6) provide guidance for and over financial system modernization efforts throughout the Department;

"(7) lead the efforts of the Department related to financial oversight, including identifying ways to streamline and standardize business processes;

"(8) oversee the costs of acquisition programs and related activities to ensure that actual and planned costs are in accordance with budget estimates and are affordable, or can be adequately funded, over the lifecycle of such programs and activities;

"(9) fully implement a common accounting structure to be used across the entire Department by fiscal year 2020; and

"(10) track, approve, oversee, and make public information on expenditures by components of the Department for conferences, as appropriate, including by requiring each component to—

"(A) report to the Inspector General of the Department the expenditures by such component for each conference hosted or attended by Department employees for which the total expenditures of the Department exceed $20,000, within 15 days after the date of the conference; and

"(B) with respect to such expenditures, provide to the Inspector General—

"(i) the information described in subsections (a), (b), and (c) of section 739 of title VII of division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Public Law 113–235); and

"(ii) documentation of such expenditures.".

SEC. 106. CHIEF INFORMATION OFFICER.

(a) IN GENERAL.—Section 703 of the Homeland Security Act of 2002 (6 U.S.C. 343) is amended—

(1) in subsection (a), by adding at the end the following new sentence: "In addition to the functions under section 3506(a)(2) of title 44, United States Code, the Chief Information Officer shall perform the functions set forth in this section and such other functions as may be assigned by the Secretary.";

(2) by redesignating subsection (b) as subsection (d); and

(3) by inserting after subsection (a) the following new subsections:

"(b) RESPONSIBILITIES.—In addition to performing the functions under section 3506 of title 44, United States Code, the Chief Information Officer shall serve as the lead technical authority for information technology programs of the Department and Department components and, in consultation with the Under Secretary for Management, shall—

"(1) advise and assist the Secretary, heads of the components of the Department, and other senior officers in carrying out the responsibilities of the Department for all activities relating to the budgets, programs, security, and operations of the information technology functions of the Department;

"(2) to the extent delegated by the Secretary, exercise leadership and authority over Department information technology management and establish the information technology priorities, policies, processes, standards, guidelines, and procedures of the Department to ensure interoperability and standardization of information technology;

"(3) maintain a consolidated inventory of the mission critical and mission essential information systems of the Department, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems;

"(4) maintain the security, visibility, reliability, integrity, and availability of data and information technology of the Department;

"(5) establish and implement policies and procedures to effectively monitor and manage vulnerabilities in the supply chain for purchases of information technology, in consultation with the Chief Procurement Officer of the Department;

"(6) review contracts and interagency agreements associated with major information technology investments and information technology investments that have had cost, schedule, or performance challenges in the past;

"(7) assess the risk of all major information technology investments and publically report the risk rating to the Office of Management and Budget; and

"(8) carry out any other responsibilities delegated by the Secretary consistent with an effective information system management function.

"(c) STRATEGIC PLANS.—In coordination with the Chief Financial Officer, the Chief Information Officer shall develop an information technology strategic plan every five years and report to 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 on the extent to which—

"(1) the budget of the Department aligns with priorities specified in the information technology strategic plan;

"(2) the information technology strategic plan informs the budget process of the Department;

"(3) information technology priorities were or were not funded and the reasons for not funding all priorities in a given fiscal year;

"(4) the Department has identified and addressed skills gaps needed to implement the information technology strategic plan; and

"(5) unnecessary duplicate information technology within and across the components of the Department has been eliminated.".

(b) SOFTWARE LICENSING.—

(1) SOFTWARE INVENTORY.—Not later than 180 days after the date of the enactment of this Act and every two years thereafter until 2022, the Chief Information Officer of the Department of Homeland Security, in consultation with Department component chief information officers, shall—

(A) conduct a Department-wide inventory of all existing software licenses held by the Department, including utilized and unutilized licenses;

(B) assess the needs of the Department and the components of the Department for software licenses for the subsequent two fiscal years;

(C) examine how the Department can achieve the greatest possible economies of scale and cost savings in the procurement of software licenses;

(D) determine how the use of shared cloud-computing services will impact the needs for software licenses for the subsequent two fiscal years;

(E) establish plans and estimated costs for eliminating unutilized software licenses for the subsequent two fiscal years; and

(F) submit a copy of each inventory conducted under subparagraph (A) to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(2) PLAN TO REDUCE SOFTWARE LICENSES.—If the Chief Information Officer determines through the inventory conducted under paragraph (1) that the number of software licenses held by the Department and the components of the Department exceed the needs of the Department, not later than 90 days after the date on which the inventory is completed, the Secretary of Homeland Security shall establish a plan for reducing the number of such software licenses to meet needs of the Department.

(3) PROHIBITION ON PROCUREMENT OF NEW SOFTWARE LICENSES.—

(A) IN GENERAL.—Except as provided in subparagraph (B), upon completion of a plan under paragraph (2), no additional resources may be obligated for the procurement of new software licenses for the Department until such time as the need of the Department exceeds the number of used and unused licenses held by the Department.

(B) EXCEPTION.—The Chief Information Officer may authorize the purchase of additional licenses and amend the number of needed licenses as necessary.

(c) COMPTROLLER GENERAL REVIEW.—Not later than fiscal year 2019, the Comptroller General of the United States shall review the extent to which the Chief Information Officer fulfilled all requirements established in this section and the amendment made by this section.

(d) COMPLETION OF FIRST DEFINITION OF CAPABILITIES.—Not later than one year after the date of the enactment of this Act, the Chief Information Officer shall complete the first information technology strategic plan required under subsection (c) of section 701 of the Homeland Security Act of 2002, as added by subsection (a) of this section.

SEC. 107. QUADRENNIAL HOMELAND SECURITY REVIEW.

(a) IN GENERAL.—Section 707 of the Homeland Security Act of 2002 (6 U.S.C. 347) is amended—

(1) in subsection (a)(3)—

(A) in subparagraph (B), by striking "and" at the end;

(B) by redesignating subparagraph (C) as subparagraph (D); and

(C) by inserting after subparagraph (B) the following new subparagraph (C):

"(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";

(2) in subsection (b)—

(A) in paragraph (2), by inserting before the semicolon at the end the following: "based on the risk assessment required pursuant to subsection (c)(2)(B)";

(B) in paragraph (3)—

(i) by inserting ", to the extent practicable," after "describe"; and

(ii) by striking "budget plan" and inserting "resources required";

(C) in paragraph (4)—

(i) by inserting ", to the extent practicable," after "identify";

(ii) by striking "budget plan required to provide sufficient resources to successfully" and inserting "resources required to"; and

(iii) by striking the semicolon at the end and inserting ", including any resources identified from redundant, wasteful, or unnecessary capabilities and capacities that can be redirected to better support other existing capabilities and capacities, as the case may be; and";

(D) in paragraph (5), by striking "; and" and inserting a period; and

(E) by striking paragraph (6);

(3) in subsection (c)—

(A) in paragraph (1), by striking "December 31 of the year" and inserting "60 days after the date of the submittal of the President's budget for the fiscal year after the fiscal year";

(B) in paragraph (2)—

(i) in subparagraph (B), by striking "description of the threats to" and inserting "risk assessment of";

(ii) in subparagraph (C), by inserting ", as required under subsection (b)(2)" before the semicolon at the end;

(iii) in subparagraph (D)—

(I) by inserting "to the extent practicable," before "a description"; and

(II) by striking "budget plan" and inserting "resources required";

(iv) in subparagraph (F)—

(I) by inserting "to the extent practicable," before "a discussion"; and

(II) by striking "the status of";

(v) in subparagraph (G)—

(I) by inserting "to the extent practicable," before "a discussion";

(II) by striking "the status of";

(III) by inserting "and risks" before "to national homeland"; and

(IV) by inserting "and" after the semicolon at the end;

(vi) by striking subparagraph (H); and

(vii) by redesignating subparagraph (I) as subparagraph (H);

(C) by redesignating paragraph (3) as paragraph (4); and

(D) by inserting after paragraph (2) the following new paragraph (3):

"(3) DOCUMENTATION.—The Secretary shall retain and, upon request, provide to Congress the following documentation regarding the quadrennial homeland security review:

"(A) Records regarding the consultation carried out the pursuant to subsection (a)(3), including—

"(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; and

"(ii) information on how feedback received by the Secretary informed the quadrennial homeland security review.

"(B) Information regarding the risk assessment, as required under subsection (c)(2)(B), including—

"(i) the risk model utilized to generate the risk assessment;

"(ii) information, including data used in the risk model, utilized to generate the risk assessment;

"(iii) sources of information, including other risk assessments, utilized to generate the risk assessment; and

"(iv) information on assumptions, weighing factors, and subjective judgments utilized to generate the risk assessment, together with information on the rationale or basis thereof."; and

(4) by redesignating subsection (d) as subsection (e); and

(5) by inserting after subsection (c) the following new subsection (d):

"(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 covered by the report were integrated into the acquisition strategy and expenditure plans for the Department.".

(b) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to a quadrennial homeland security review conducted after December 31, 2017.

SEC. 108. OFFICE OF STRATEGY, POLICY, AND PLANS.

(a) IN GENERAL.—Section 709 of the Homeland Security Act of 2002 (6 U.S.C. 349) is amended—

(1) in subsection (a), by adding at the end the following: "The Office of Strategy, Policy, and Plans shall include the following components:

"(1) The Office of Partnership and Engagement.

"(2) The Office of International Affairs.

"(3) The Office of Cyber, Infrastructure, and Resilience Policy.

"(4) The Office of Strategy, Planning, Analysis, and Risk.

"(5) The Office of Threat Prevention and Security Policy.

"(6) The Office of Border, Immigration, and Trade Policy.";

(2) by redesignating subsections (e) through (g) as subsections (f) through (h), respectively; and

(3) by inserting after subsection (d) the following new subsection (e):

"(e) ASSISTANT SECRETARIES AND DIRECTORS.—

"(1) ASSISTANT SECRETARY FOR PARTNERSHIP AND ENGAGEMENT.—The Office of Partnership and Engagement shall be led by an Assistant Secretary for Partnership and Engagement appointed by the Secretary. The Assistant Secretary shall—

"(A) lead the efforts of the Department to incorporate external feedback from stakeholders into policy and strategic planning efforts, as appropriate, in consultation with the Office for Civil Rights and Civil Liberties;

"(B) conduct the activities specified in section 2006(b);

"(C) advise the Secretary on the effects of the policies, regulations, processes, and actions of the Department on the private sector and create and foster strategic communications with the private sector to enhance the primary mission of the Department to protect the homeland;

"(D) coordinate the activities of the Department relating to State and local government;

"(E) provide State and local governments with regular information, research, and technical support to assist local efforts at securing the homeland; and

"(F) perform such other functions as are established by law or delegated by the Under Secretary for Policy.

"(2) ASSISTANT SECRETARY FOR INTERNATIONAL AFFAIRS.—The Office of International Affairs shall be led by an Assistant Secretary for International Affairs appointed by the Secretary. The Assistant Secretary shall—

"(A) coordinate international activities within the Department, including activities carried out by the components of the Department, in consultation with other Federal officials with responsibility for counterterrorism and homeland security matters;

"(B) advise, inform, and assist the Secretary with respect to the development and implementation of the policy priorities of the Department, including strategic priorities for the deployment of assets, including personnel, outside the United States;

"(C) develop, in consultation with the Under Secretary for Management, guidance for selecting, assigning, training, and monitoring overseas deployments of Department personnel, including minimum standards for pre-deployment training;

"(D) maintain awareness regarding the international travel of senior officers of the Department and their intent to pursue negotiations with foreign government officials, and review resulting draft agreements; and

"(E) perform such other functions as are established by law or delegated by the Under Secretary for Policy.".

(b) ABOLISHMENT OF OFFICE OF INTERNATIONAL AFFAIRS.—

(1) IN GENERAL.—The Office of International Affairs within the Office of the Secretary of Homeland Security is abolished.

(2) TRANSFER OF ASSETS AND PERSONNEL.—The functions authorized to be performed by such office as of the day before the date of the enactment of this Act, and the assets and personnel associated with such functions, are transferred to the head of the Office of International Affairs provided for by section 709 of the Homeland Security Act of 2002, as amended by this section.

(3) CONFORMING AMENDMENT.—The Homeland Security Act of 2002 is amended by striking section 879 (6 U.S.C. 459).

(4) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 879.

(c) TRANSFER OF FUNCTIONS, ASSETS, AND PERSONNEL OF OFFICE FOR STATE AND LOCAL LAW ENFORCEMENT.—The functions authorized to be performed by the Office for State and Local Law Enforcement of the Department of Homeland Security as of the day before the date of the enactment of this Act, and the assets and personnel associated with such functions, are transferred to the head of the Office of Partnership and Engagement provided for by section 709 of the Homeland Security Act of 2002, as amended by this section.

(d) ABOLISHMENT OF OFFICE FOR STATE AND LOCAL GOVERNMENT COORDINATION.—

(1) IN GENERAL.—The Office for State and Local Government Coordination of the Department of Homeland Security is abolished.

(2) TRANSFER OF FUNCTIONS AND ASSETS.—The functions authorized to be performed by such office immediately before the enactment of this Act, and the assets and personnel associated with such functions, are transferred to the head of Office of Partnership and Engagement provided for by section 709 of the Homeland Security Act of 2002, as amended by this section.

(3) CONFORMING AMENDMENT.—The Homeland Security Act of 2002 is amended by striking section 801 (6 U.S.C. 631).

(4) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 801.

(e) ABOLISHMENT OF SPECIAL ASSISTANT TO SECRETARY OF HOMELAND SECURITY.—

(1) IN GENERAL.—The Special Assistant to the Secretary authorized by section 102(f) of the Homeland Security Act of 2002 (6 U.S.C. 112(f)), as in effect immediately before the enactment of this Act, is abolished.

(2) TRANSFER OF FUNCTIONS AND ASSETS.—The functions authorized to be performed by such Special Assistant to the Secretary immediately before the enactment of this Act, and the assets and personnel associated with such functions, are transferred to the head of the Office of Partnership and Engagement provided for by section 709 of the Homeland Security Act of 2002, as amended by this section.

(3) CONFORMING AMENDMENT.—Section 102 of the Homeland Security Act of 2002 (6 U.S.C. 112) is amended by striking subsection (f).

(f) CONFORMING AMENDMENTS RELATING TO ASSISTANT SECRETARIES.—Subsection (a) of section 103 of the Homeland Security Act of 2002 (6 U.S.C. 113) is amended—

(1) in the subsection heading, by inserting "; ASSISTANT SECRETARIES" after "UNDER SECRETARIES";

(2) in paragraph (1), by striking subparagraph (I) and redesignating subparagraphs (J) and (K) as subparagraphs (I) and (J), respectively; and

(3) by amending paragraph (2) to read as follows:

"(2) ASSISTANT SECRETARIES AND OTHER OFFICIALS.—

"(A) ADVICE AND CONSENT APPOINTMENTS.—The Department shall have the following officials appointed by the President, by and with the advice and consent of the Senate:

"(i) The Assistant Secretary, U.S. Immigration and Customs Enforcement.

"(ii) The Administrator, Transportation Security Administration.

"(B) OTHER PRESIDENTIAL APPOINTMENTS.—The Department shall have the following Assistant Secretaries appointed by the President:

"(i) The Assistant Secretary, Infrastructure Protection.

"(ii) The Assistant Secretary, Office of Public Affairs.

"(iii) The Assistant Secretary, Office of Legislative Affairs.

"(C) SECRETARIAL APPOINTMENTS.—The Department shall have the following Assistant Secretaries appointed by the Secretary:

"(i) The Assistant Secretary, Office of Cybersecurity and Communications.

"(ii) The Assistant Secretary for International Affairs.

"(iii) The Assistant Secretary for Partnership and Engagement.

"(iv) The Assistant Secretary for Threat Prevention and Security Policy.

"(v) The Assistant Secretary for Border, Immigration, and Trade Policy.

"(vi) The Assistant Secretary for Cyber, Infrastructure, and Resilience Policy.

"(vii) The Assistant Secretary for Strategy, Planning, Analysis, and Risk.

"(viii) The Assistant Secretary for State and Local Law Enforcement."; and

(4) by adding at the end the following new paragraphs:

"(3) ASSISTANT SECRETARY, LEGISLATIVE AFFAIRS.—The Assistant Secretary, Legislative Affairs shall oversee one internal reporting structure for engaging with authorizing and appropriating congressional committees.

"(4) LIMITATION ON CREATION OF POSITIONS.—No Assistant Secretary position may be created in addition to the positions provided for by this section unless such position is authorized by a statute enacted after the date of the enactment of the Department of Homeland Security Authorization Act of 2017.".

(g) HOMELAND SECURITY ADVISORY COUNCIL.—Subsection (b) of section 102 of the Homeland Security Act of 2002 (6 U.S.C. 112) is amended—

(1) in paragraph (2), by striking "and" at the end;

(2) in paragraph (3), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following new paragraph:

"(4) shall establish a Homeland Security Advisory Council to provide advice and recommendations on homeland security-related matters, including advice with respect to the preparation of the Quadrennial Homeland Security Review.".

(h) PROHIBITION ON NEW OFFICES.—No new office may be created to perform functions transferred by this section, other than as provided in section 709 of the Homeland Security Act of 2002, as amended by this Act.

(i) DEFINITIONS.—In this section each of the terms "functions", "assets", and "personnel" has the meaning given each such term under section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(j) DUPLICATION REVIEW.—

(1) REVIEW REQUIRED.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall complete a review of the functions and responsibilities of each Department of Homeland Security component responsible for international affairs to identify and eliminate areas of unnecessary duplication.

(2) SUBMITTAL TO CONGRESS.—Not later than 30 days after the completion of the review required under paragraph (1), the Secretary shall provide the results of the review to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(3) ACTION PLAN.—Not later than one year after the date of the enactment of this Act, the Secretary shall submit to the congressional homeland security committees an action plan, including corrective steps and an estimated date of completion, to address areas of duplication, fragmentation, and overlap and opportunities for cost savings and revenue enhancement, as identified by the Government Accountability Office based on the annual report of the Government

Accountability Office entitled "Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits".

SEC. 109. CHIEF PROCUREMENT OFFICER.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.) is amended by adding at the end the following new section:

"SEC. 710. CHIEF PROCUREMENT OFFICER.

"(a) IN GENERAL.—There is in the Department a Chief Procurement Officer, who shall serve as a senior business advisor to agency officials on procurement-related matters and report directly to the Under Secretary for Management. The Chief Procurement Officer is the senior procurement executive for purposes of subsection (c) of section 1702 of title 41, United States Code, and shall perform procurement functions as specified in such subsection.

"(b) RESPONSIBILITIES.—The Chief Procurement Officer shall—

"(1) delegate or retain contracting authority, as appropriate;

"(2) issue procurement policies and oversee the heads of contracting activity of the Department to ensure compliance with those policies;

"(3) serve as the main liaison of the Department to industry on procurement-related issues;

"(4) account for the integrity, performance, and oversight of Department procurement and contracting functions;

"(5) ensure that procurement contracting strategies and plans are consistent with the intent and direction of the Acquisition Review Board;

"(6) oversee a centralized acquisition workforce certification and training program using, as appropriate, existing best practices and acquisition training opportunities from the Federal Government, private sector, or universities and colleges to include training on how best to identify actions that warrant referrals for suspension or debarment;

"(7) provide input on the periodic performance reviews of each head of contracting activity of the Department;

"(8) collect baseline data and use such data to establish performance measures on the impact of strategic sourcing initiatives on the private sector, including small businesses;

"(9) establish and implement policies and procedures to effectively monitor and manage vulnerabilities in the supply chain for all Department purchases;

"(10) ensure that a fair proportion of the value of Federal contracts and subcontracts are awarded to small businesses (in accordance with the procurement contract goals under section 15(g) of the Small Business Act (15 U.S.C. 644(g)), maximize opportunities for small business participation in such contracts, and ensure, to the extent practicable, small businesses that achieve qualified vendor status for security-related technologies are provided an opportunity to compete for contracts for such technology;

"(11) conduct oversight of implementation of administrative agreements to resolve suspension or debarment proceedings and, upon request, provide information to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate about the effectiveness of such agreements at improving contractor responsibility; and

"(12) carry out any other procurement duties that the Under Secretary for Management may designate.

"(c) HEAD OF CONTRACTING ACTIVITY DEFINED.—In this section the term 'head of contracting activity' means an official responsible for the creation, management, and oversight of a team of procurement professionals properly trained, certified, and warranted to accomplish the acquisition of products and services on behalf of the designated components, offices, and organizations of the Department, and as authorized, other government entities.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 709 the following new item:

"Sec. 710. Chief Procurement Officer.".

SEC. 110. CHIEF SECURITY OFFICER.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.) is further amended by inserting after the item relating to section 710, as added by this Act, the following new section:

"SEC. 711. CHIEF SECURITY OFFICER.

"(a) IN GENERAL.—There is in the Department a Chief Security Officer, who shall report directly to the Under Secretary for Management.

"(b) RESPONSIBILITIES.—The Chief Security Officer shall—

"(1) develop and implement the security policies, programs, and standards of the Department;

"(2) identify training and provide education to Department personnel on security-related matters; and

"(3) provide support to Department components on security-related matters.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by inserting after the item relating to section 710, as added by this Act, the following new item:

"Sec. 711. Chief Security Officer.".

SEC. 111. OFFICE OF INSPECTOR GENERAL.

(a) SENSE OF CONGRESS.—

(1) FINDINGS.—Congress finds the following:

(A) The Inspector General Act of 1978 mandates that Inspectors General are to conduct audits and investigations relating to the programs and operations of Federal departments to promote economy, efficiency, and effectiveness in the administration of programs and operations, and to prevent and detect fraud and abuse in such programs and operations.

(B) The Inspector General Act of 1978 mandates that Inspectors General are to provide a means for keeping Federal departments and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action.

(C) The Office of the Inspector General of the Department of Homeland Security detects, investigates, and prevents instances of waste, fraud, abuse, and mismanagement within the Department, and offers solutions for response.

(D) The Office of the Inspector General of the Department of Homeland Security consistently produces high-value, high-impact work that enhances the security and safety of the homeland.

(E) The Inspector General of the Department of Homeland Security provides the leadership and accountability within the Office of the Inspector General to oversee a cabinet-level agency.

(F) The Inspector General of the Department of Homeland Security stands as a leader within the Inspector General community through consistent exemplary service.

(G) The Office of Inspector General of the Department of Homeland Security offers the Federal Government and American taxpayers an impressive return on investment, measured in dollars spent versus dollars saved.

(H) The Office of the Inspector General of the Department of Homeland Security enhances the Department's ability to effectively and efficiently administer laws.

(2) SENSE OF CONGRESS.—It is the sense of Congress that the Inspector General of the Department of Homeland Security plays a vital role in fulfilling the Department's daily missions.

(b) NOTIFICATION.—The heads of offices and components of the Department of Homeland Security shall promptly advise the Inspector General of the Department of all allegations of misconduct with respect to which the Inspector General has investigative authority under the Inspector General Act of 1978. The Inspector General may waive the notification requirement under this subsection with respect to any category or subset of allegations of misconduct.

(c) RULE OF CONSTRUCTION.—Nothing in this section may be construed as affecting the authority of the Secretary of Homeland Security under subsection (a) of section 8I of the Inspector General Act of 1978 (5 U.S.C. App. 8I).

SEC. 112. OFFICE FOR CIVIL RIGHTS AND CIVIL LIBERTIES.

(a) IN GENERAL.—Section 705 of the Homeland Security Act of 2002 (6 U.S.C. 345) is amended—

(1) in the section heading, by striking "**ESTABLISHMENT OF OFFICER FOR**";

(2) by redesignating subsection (b) as subsection (c); and

(3) by inserting after subsection (a) the following new subsection:

"(b) OFFICE FOR CIVIL RIGHTS AND CIVIL LIBERTIES.—There is in the Department an Office for Civil Rights and Civil Liberties. Under the direction of the Officer for Civil Rights and Civil Liberties, the Office shall support the Officer in the following:

"(1) Integrating civil rights and civil liberties into activities of the Department by conducting programs and providing policy advice and other technical assistance.

"(2) Investigating allegations of violations of civil rights and civil liberties from the public.

"(3) Carrying out the Department's equal employment opportunity and diversity policies and programs, including complaint management and adjudication.

"(4) Communicating with individuals and communities whose civil rights and civil liberties may be affected by Department activities.

"(5) Any other activities as assigned by the Officer.".

(b) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $22,571,000 for each of fiscal years 2018 and 2019 to carry out section 705 of the Homeland Security Act of 2002, as amended by subsection (a) of this section.

SEC. 113. DEPARTMENT OF HOMELAND SECURITY ROTATION PROGRAM.

(a) ENHANCEMENTS TO THE ROTATION PROGRAM.—Section 844 of the Homeland Security Act of 2002 (6) U.S.C. 414) is amended—

(1) by striking "(a) ESTABLISHMENT.—";

(2) by redesignating paragraphs (1) through (5) as subsections (a) through (e), respectively, and adjusting the margins accordingly;

(3) in subsection (a), as so redesignated—

(A) by striking "Not later than 180 days after the date of enactment of this section, the" and inserting "The"; and

(B) by striking "for employees of the Department" and inserting "for certain personnel within the Department";

(4) in subsection (b), as so redesignated—

(A) by redesignating subparagraphs (A) through (G) as paragraphs (3) through (9), respectively, and adjusting the margins accordingly;

(B) by inserting before paragraph (3), as so redesignated, the following new paragraphs:

"(1) seek to foster greater departmental integration and unity of effort;

"(2) seek to help enhance the knowledge, skills, and abilities of participating personnel with respect to the programs, policies, and activities of the Department;";

(C) in paragraph (4), as so redesignated, by striking "middle and senior level"; and

(D) in paragraph (7), as so redesignated, by inserting before "invigorate" the following: "seek to improve morale and retention throughout the Department and";

(5) in subsection (c), as redesignated by paragraph (2)—

(A) by redesignating subparagraphs (A) and (B) as paragraphs (1) and (2), respectively, and adjusting the margins accordingly; and

(B) in paragraph (2), as so redesignated—

(i) by striking clause (iii); and

(ii) by redesignating clauses (i), (ii), and (iv) through (viii) as subparagraphs (A) through (G), respectively, and adjusting the margins accordingly;

(6) by redesignating subsections (d) and (e), as redesignated by paragraph (2), as subsections (e) and (f), respectively;

(7) by inserting after subsection (c) the following new subsection:

"(d) ADMINISTRATIVE MATTERS.—In carrying out the Rotation Program the Secretary shall—

"(1) before selecting employees for participation in the Rotation Program, disseminate information broadly within the Department about the availability of the Rotation Program, qualifications for participation in the Rotation Program, including full-time employment within the employing component or office not less than one year, and the general provisions of the Rotation Program;

"(2) require as a condition of participation in the Rotation Program that an employee—

"(A) is nominated by the head of the component or office employing the employee; and

"(B) is selected by the Secretary, or the Secretary's designee, solely on the basis of relative ability, knowledge, and skills, after fair and open competition that assures that all candidates receive equal opportunity;

"(3) ensure that each employee participating in the Rotation Program shall be entitled to return, within a reasonable period of time after the end of the period of participation, to the position held by the employee, or a corresponding or higher position, in the component or office that employed the employee prior to the participation of the employee in the Rotation Program;

"(4) require that the rights that would be available to the employee if the employee were detailed from the employing component or office to another Federal agency or office remain available to the employee during the employee participation in the Rotation Program; and

"(5) require that, during the period of participation by an employee in the Rotation Program, performance evaluations for the employee—

"(A) shall be conducted by officials in the office or component employing the employee with input from the supervisors of the employee at the component or office in which the employee is placed during that period; and

"(B) shall be provided the same weight with respect to promotions and other rewards as performance evaluations for service in the office or component employing the employee."; and

(8) by adding at the end the following new subsection:

"(g) INTELLIGENCE ROTATIONAL ASSIGNMENT PROGRAM.—

"(1) ESTABLISHMENT.—The Secretary shall establish an Intelligence Rotational Assignment Program as part of the Rotation Program under subsection (a).

"(2) ADMINISTRATION.—The Chief Human Capital Officer, in conjunction with the Chief Intelligence Officer, shall administer the Intelligence Rotational Assignment Program established pursuant to paragraph (1).

"(3) ELIGIBLITY.—The Intelligence Rotational Assignment Program established pursuant to paragraph (1) shall be open to employees serving in existing analyst positions within the Department's Intelligence Enterprise and other Department employees as determined appropriate by the Chief Human Capital Officer and the Chief Intelligence Officer.

"(4) COORDINATION.—The responsibilities specified in subsection (c)(2) that apply to the Rotation Program under such subsection shall, as applicable, also apply to the Intelligence Rotational Assignment Program under this subsection.".

(b) CONGRESSIONAL NOTIFICATION AND OVERSIGHT.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security 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 about the status of the Homeland Security Rotation Program authorized by section 844 of the Homeland Security Act of 2002, as amended by subsection (a) of this section.

SEC. 114. FUTURE YEARS HOMELAND SECURITY PROGRAM.

(a) IN GENERAL.—Section 874 of the Homeland Security Act of 2002 (6 U.S.C. 454) is amended—

(1) in the section heading, by striking "**YEAR**" and inserting "**YEARS**";

(2) by striking subsection (a) and inserting the following:

"(a) IN GENERAL.—Not later than 60 days after the date on which the budget of the President is submitted to Congress under section 1105(a) of title 31, United States Code, 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 (referred to in this section as the 'appropriate committees') a Future Years Homeland Security Program that covers the fiscal year for which the budget is submitted and the 4 succeeding fiscal years."; and

(3) by striking subsection (c) and inserting the following new subsections:

"(c) PROJECTION OF ACQUISITION ESTIMATES.—On and after February 1, 2018, each Future Years Homeland Security Program shall project—

"(1) acquisition estimates for the fiscal year for which the budget is submitted and the four succeeding fiscal years, with specified estimates for each fiscal year, for all major acquisitions by the Department and each component of the Department; and

"(2) estimated annual deployment schedules for all physical asset major acquisitions over the five-fiscal-year period described in paragraph (1) and the full operating capability for all information technology major acquisitions.

"(d) SENSITIVE AND CLASSIFIED INFORMATION.—The Secretary may include with each Future Years Homeland Security Program a classified or other appropriately controlled document containing any information required to be submitted under this section that is restricted from public disclosure in accordance with Federal law or any Executive Order.

"(e) AVAILABILITY OF INFORMATION TO THE PUBLIC.—The Secretary shall make available to the public in electronic form the information required to be submitted to the appropriate committees under this section, other than information described in subsection (d).".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by striking the item relating to section 874 and inserting the following new item:

"874. Future Years Homeland Security Program.".

SEC. 115. FIELD EFFICIENCIES PLAN.

(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and Committee on Homeland Security and Governmental Affairs of the Senate a field efficiencies plan that—

(A) examines the facilities and administrative and logistics functions of components of the Department of Homeland Security located within designated geographic areas; and

(B) provides specific recommendations and an associated cost-benefit analysis for the consolidation of the facilities and administrative and logistics functions of components of the Department within each designated geographic area.

(2) CONTENTS.—The field efficiencies plan submitted under paragraph (1) shall include the following:

(A) An accounting of leases held by the Department or its components that have expired in the current fiscal year or will be expiring in the next fiscal year, that have begun or been renewed in the current fiscal year, or that the Department or its components plan to sign or renew in the next fiscal year.

(B) For each designated geographic area—

(i) An evaluation of specific facilities at which components, or operational entities of components, of the Department may be closed or consolidated, including consideration of when leases expire or facilities owned by the government become available.

(ii) An evaluation of potential consolidation with facilities of other Federal, State, or local entities, including—

(I) offices;
(II) warehouses;
(III) training centers;
(IV) housing;
(V) ports, shore facilities, and airfields;
(VI) laboratories; and
(VII) other assets as determined by the Secretary.

(iii) An evaluation of the potential for the consolidation of administrative and logistics functions, including—

(I) facility maintenance;
(II) fleet vehicle services;
(III) mail handling and shipping and receiving;
(IV) facility security;
(V) procurement of goods and services;
(VI) information technology and telecommunications services and support; and
(VII) additional ways to improve unity of effort and cost savings for field operations and related support activities as determined by the Secretary.

(C) An implementation plan, including—

(i) near-term actions that can co-locate, consolidate, or dispose of property within 24 months;

(ii) identifying long-term occupancy agreements or leases that cannot be changed without a significant cost to the Government; and

(iii) how the Department can ensure it has the capacity, in both personnel and funds, needed to cover up-front costs to achieve consolidation and efficiencies.

(D) An accounting of any consolidation of the real estate footprint of the Department or any component of the Department, including the co-location of personnel from different components, offices, and agencies within the Department.

SEC. 116. SUBMISSION TO CONGRESS OF INFORMATION REGARDING REPROGRAMMING OR TRANSFER OF DEPARTMENT OF HOMELAND SECURITY RESOURCES TO RESPOND TO OPERATIONAL SURGES.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 is further amended by adding at the end the following new section:

"SEC. 712. ANNUAL SUBMITTAL TO CONGRESS OF INFORMATION ON REPROGRAMMING OR TRANSFERS OF FUNDS TO RESPOND TO OPERATIONAL SURGES.

"For each fiscal year until fiscal year 2023, the Secretary of Homeland Security 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, together with the annual budget request for the Department, information on—

"(1) any circumstance during the year covered by the report in which the Secretary exercised the authority to reprogram or transfer funds to address unforeseen costs, including costs associated with operational surges; and

"(2) any circumstance in which any limitation on the transfer or reprogramming of funds affected the ability of the Secretary to address such unforeseen costs.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by inserting after the item relating to section 711, as added by this Act, the following new item:

"712. Annual submittal to Congress of information on reprogramming or transfers of funds to respond to operational surges.".

SEC. 117. REPORT TO CONGRESS ON COST SAVINGS AND EFFICIENCY.

(a) IN GENERAL.—Not later than two years after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Under Secretary of Homeland Security for Management, shall submit to the congressional homeland security committees a report that includes each of the following:

(1) A detailed accounting of the management and administrative expenditures and activities of each component of the Department of Homeland Security and identifies potential cost savings, avoidances, and efficiencies for those expenditures and activities.

(2) An examination of major physical assets of the Department, as defined by the Secretary;

(3) A review of the size, experience level, and geographic distribution of the operational personnel of the Department.

(4) Recommendations for adjustments in the management and administration of the Department that would reduce deficiencies in the capabilities of the Department, reduce costs, and enhance efficiencies.

(b) FORM OF REPORT.—The report required under subsection (a) shall be submitted in unclassified form but may include a classified annex.

SEC. 118. RESEARCH AND DEVELOPMENT AND CBRNE ORGANIZATIONAL REVIEW.

(a) DEPARTMENT OF HOMELAND SECURITY RESEARCH AND DEVELOPMENT ACTIVITIES.—

(1) IN GENERAL.—The Secretary of Homeland Security shall assess the organization and management of the Department of Homeland Security's research and development activities, and shall develop and submit to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, not later than six months after the date of the enactment of this Act, a proposed organizational structure for the management of such research and development activities.

(2) ORGANIZATIONAL JUSTIFICATION.—The proposed organizational structure for the management of the Department of Homeland Security's research and development activities included in the assessment required under paragraph (1) shall include the following:

(A) A discussion of the methodology for determining such proposed organizational structure.

(B) A comprehensive inventory of research and development activities of the Department, and the proposed location of each activity under such proposed organizational structure.

(C) Information relating to how such proposed organizational structure will facilitate and promote enhanced coordination and better collaboration between the Under Secretary for Science and Technology of the Department and the offices and components of the Department, including a specific description of operational challenges resulting from the current organizational structure and a detailed explanation of how the proposed organizational structure will address such challenges.

(D) Information relating to how such proposed organizational structure will support the development of research and development priorities and capabilities across the Department.

(E) A discussion of any resulting cost savings and efficiencies from such proposed organizational structure.

(F) Recommendations for any necessary statutory changes, an explanation of why no statutory or organizational changes are necessary, or a request for additional time to complete the organizational justification.

(b) DEPARTMENT OF HOMELAND SECURITY CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND EXPLOSIVES ACTIVITIES.—

(1) IN GENERAL.—The Secretary of Homeland Security shall assess the organization and management of the Department of Homeland Security's chemical, biological, radiological, nuclear, and explosives activities, and shall develop and submit to 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 six months after the date of the enactment of this Act, a proposed organizational structure to ensure enhanced coordination and provide strengthened chemical, biological, radiological, nuclear, and explosives capabilities in support of homeland security.

(2) ORGANIZATIONAL JUSTIFICATION.—The proposed organizational structure for the management of the Department of Homeland Security's chemical, biological, radiological, nuclear, and explosives activities included in the assessment required under paragraph (1) shall include the following:

(A) A discussion of the methodology for determining such proposed organizational structure.

(B) A comprehensive inventory of chemical, biological, radiological, nuclear, and explosives activities of the Department, and the proposed location of each activity under such proposed organizational structure.

(C) Information relating to how such proposed organizational structure will enhance the development of chemical, biological, radiological, nuclear, and explosives priorities and capabilities across the Department, including a specific description of operational challenges resulting from the current organizational structure and a detailed explanation of how the proposed organizational structure will address such challenges.

(D) A discussion of any resulting cost savings and efficiencies from such proposed organizational structure.

(E) Recommendations for any necessary statutory changes, an explanation of why no statutory or organizational changes are necessary, or a request for additional time to complete the organizational justification.

(c) REVIEW REQUIRED.—Not later than three months after the submission of the proposed organizational justifications required under subsections (a)(1) and (b)(1), the Comptroller General of the United States shall submit to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a review of the organizational justifications. The review shall consider how the proposed organizational realignment, or lack thereof, of research and development activities and chemical, biological, radiological, nuclear, and explosives activities will improve or impede the Department's ongoing efforts is such mission areas, including an assessment of—

(1) any potential cost savings or additional costs incurred as a result of any proposed organizational realignment;

(2) an assessment of the comparison of benefits and costs of the proposed organizational structure;

(3) the extent to which the organizational justification submitted pursuant to subsections (a)(1) and (b)(1) fully assesses, documents, and addresses any potential problems that could result from any proposed organizational realignment;

(4) the extent to which the organizational justification identifies specific deficiencies in operations resulting from the existing organizational structure of the Department and an explanation of how any proposed realignment will address such deficiencies;

(5) the extent to which the Department solicited and incorporated the feedback of its workforce in the proposed organizational structure; and

(6) the extent to which the Department conducted and incorporated stakeholder outreach in developing the proposed organizational structure.

SEC. 119. ACTIVITIES RELATED TO CHILDREN.

Paragraph (6) of subsection (c) of section 708 of the Homeland Security Act of 2002 (6 U.S.C. 349(c)), as redesignated by section 410 of this Act, is amended by inserting ", including feedback from organizations representing the needs of children," after "stakeholder feedback".

Subtitle B—Human Resources and Other Matters

SEC. 121. CHIEF HUMAN CAPITAL OFFICER RESPONSIBILITIES.

Section 704 of the Homeland Security Act of 2002 (6 U.S.C. 344) is amended—

(1) in subsection (b)—

(A) in paragraph (1)—

(i) by inserting ", including with respect to leader development and employee engagement," after "policies";

(ii) by striking "and in line" and inserting ", in line"; and

(iii) by inserting "and informed by best practices within the Federal government and the private sector," after "priorities,";

(B) in paragraph (2), by striking "develop performance measures to provide a basis for monitoring and evaluating" and inserting "evaluate, on an ongoing basis,";

(C) in paragraph (3), by inserting "that, to the extent practicable, are informed by employee feedback," after "policies";

(D) in paragraph (4), by inserting "including leader development and employee engagement programs," before "in coordination";

(E) in paragraph (5), by inserting before the semicolon at the end the following: "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 non-supervisory roles across the Department and appropriate workforce planning initiatives";

(F) by redesignating paragraphs (9) and (10) as paragraphs (11) and (12), respectively; and

(G) by inserting after paragraph (8) the following new paragraphs:

"(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;";

(2) by redesignating subsections (d) and (e) as subsections (e) and (f), respectively;

(3) by inserting after subsection (c) the following new subsection:

"(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."; and

(4) in subsection (e), as so redesignated—

(A) by redesignating paragraphs (2), (3), and (4) as paragraphs (5), (6), and (7), respectively; and

(B) by inserting after paragraph (1) the following new paragraphs:

"(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 Department-wide 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 710(a), including the number of meeting, types of materials developed and distributed, and recommendations made to the Secretary;".

SEC. 122. EMPLOYEE ENGAGEMENT STEERING COMMITTEE AND ACTION PLAN.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.) is amended by adding at the end the following new section:

"SEC. 714. 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 non-supervisory 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 Department-wide 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 steering committee under subsection (a), issue a Department-wide employee engagement action plan, reflecting input from the employee engagement steering committee established pursuant to subsection (a) 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.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item related to section 713, as added by this Act, the following new item:

"Sec. 714. Employee engagement.".

(c) SUBMISSIONS TO CONGRESS.—

(1) DEPARTMENT-WIDE EMPLOYEE ENGAGEMENT ACTION PLAN.—The Secretary of Homeland Security, acting through the Chief Human Capital Officer of the Department of Homeland Security, 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 the Department-wide employee engagement action plan required under subsection (b)(1) of section 714 of the Homeland Security Act of 2002 (as added by subsection (a) of this section) not later than 30 days after the issuance of such plan under such subsection (b)(1).

(2) COMPONENT-SPECIFIC EMPLOYEE ENGAGEMENT PLANS.—Each head of a component of the Department of Homeland Security 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 the component-specific employee engagement plan of each such component required under subsection (b)(2) of section 714 of the Homeland Security Act of 2002 (as added by subsection (a) of this section) not later than 30 days after the issuance of each such plan under such subsection (b)(2).

SEC. 123. ANNUAL EMPLOYEE AWARD PROGRAM.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.), as amended by section 122 of this Act, is further amended by adding at the end the following new section:

"SEC. 715. 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 emphasizes honoring employees who are at the non-supervisory 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 Sec-

retary 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 non-supervisory 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.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002, as amended this Act, is further amended by inserting after the item relating to section 714 the following new item:

"Sec. 715. Annual employee award program.".

SEC. 124. INDEPENDENT INVESTIGATION AND IMPLEMENTATION PLAN.

(a) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act or the issuance of a report by the Inspector General of the Department of Homeland Security on the extent to which the Department has an equitable and consistent disciplinary process, whichever is later, but in no case later than one year after such date of enactment, the Comptroller General of the United States shall utilize, if available, such report and investigate whether the application of discipline and adverse actions are administered in an equitable and consistent manner that results in the same or substantially similar disciplinary outcomes across the Department for misconduct by a non-supervisory or supervisor employee who engaged in the same or substantially similar misconduct.

(b) CONSULTATION.—In carrying out the investigation described in subsection (a), the Comptroller General of the United States shall consult with the employee engagement steering committee established pursuant to subsection (b)(1) of section 714 of the Homeland Security Act of 2002 (as added by section 122(a) of this Act).

(c) ACTION BY UNDER SECRETARY FOR MANAGEMENT.—Upon completion of the investigation described in subsection (a), the Under Secretary for Management of the Department of Homeland Security shall review the findings and recommendations of such investigation and implement a plan, in consultation with the employee engagement steering committee established pursuant to subsection (b)(1) of section 714 of the Homeland Security Act of 2002, to correct any relevant deficiencies identified by the Comptroller General of the United States. The Under Secretary for Management shall direct the employee engagement steering committee to review such plan to inform committee activities and action plans authorized under such section 714.

SEC. 125. CENTER FOR FAITH-BASED AND NEIGHBORHOOD PARTNERSHIPS.

(a) IN GENERAL.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.), is amended by adding at the end the following:

"SEC. 528. CENTER FOR FAITH-BASED AND NEIGHBORHOOD PARTNERSHIPS.

"(a) IN GENERAL.—There is established in the Department a Center for Faith-Based and Neighborhood Partnerships, headed by a Director.

"(b) MISSION.—The mission of the Center shall be to develop and coordinate Departmental outreach efforts with faith-based and community organizations and serve as a liaison between such organizations and components of the Department for activities related to securing facilities, emergency preparedness and response, and combating human trafficking.

"(c) RESPONSIBILITIES.—In support of the mission of the Center for Faith-Based and Neighborhood Partnerships, the Director shall—

"(1) develop, in collaboration with the Administrator of the Federal Emergency Management Agency, exercises that engage faith-based and community organizations to test capabilities for all hazards, including active shooter incidents;

"(2) coordinate the delivery of guidance and training to faith-based and community organizations related to securing their facilities against natural disasters, acts of terrorism, and other man-made disasters;

"(3) conduct outreach to faith-based and community organizations regarding guidance, training, and exercises and Departmental capabilities available to as-

sist faith-based and community organizations secure their facilities against natural disasters, acts of terrorism, and other man-made disasters;

"(4) facilitate engagement and coordination among the emergency management community and faith-based and community organizations;

"(5) deliver training and technical assistance to faith-based and community-based organizations and provide subject-matter expertise related to anti-human trafficking efforts to help communities successfully partner with other Blue Campaign components; and

"(6) perform any other duties as assigned by the Secretary.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by inserting after the item relating to section 527 the following:

"Sec. 528. Center For Faith-Based And Neighborhood Partnerships.".

SEC. 126. TIMELY GUIDANCE TO DHS PERSONNEL REGARDING EXECUTIVE ORDERS.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 is further amended by adding at the end the following new section:

"SEC. 716. TIMELY GUIDANCE TO PERSONNEL REGARDING EXECUTIVE ORDERS.

"To the maximum extent practicable, before any Executive Order affecting Department functions, programs, or operations takes effect, the Secretary, in coordination with the heads of relevant Department components and offices, shall make every effort to, as expeditiously as possible, provide to relevant Department personnel written guidance regarding how such Executive Order is to be implemented.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by inserting after the item relating to section 715, as added by this Act, the following new item:

"Sec. 716. Timely guidance to personnel regarding Executive Orders.".

SEC. 127. SECRETARY'S RESPONSIBILITIES REGARDING ELECTION INFRASTRUCTURE.

The Secretary of Homeland Security shall continue to prioritize the provision of assistance, on a voluntary basis, to State and local election officials in recognition of the importance of election infrastructure to the United States and that its incapacity or destruction would have a debilitating impact on national security, and that state and non-state adversaries should not compromise election infrastructure.

TITLE II—DEPARTMENT OF HOMELAND SECURITY ACQUISITION ACCOUNTABILITY AND EFFICIENCY

SEC. 201. DEFINITIONS.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 is amended by inserting before section 831 the following new section:

"SEC. 830. DEFINITIONS.

"In this subtitle:

"(1) The term 'acquisition' has the meaning given such term in section 131 of title 41, United States Code.

"(2) The term 'acquisition decision authority' means the authority, held by the Secretary acting through the Deputy Secretary or Under Secretary for Management to—

"(A) ensure compliance with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives;

"(B) review (including approving, pausing, modifying, or canceling) an acquisition program through the life cycle of such program;

"(C) ensure that acquisition program managers have the resources necessary to successfully execute an approved acquisition program;

"(D) ensure good acquisition program management of cost, schedule, risk, and system performance of the acquisition program at issue, including assessing acquisition program baseline breaches and directing any corrective action for such breaches; and

"(E) ensure that acquisition program managers, on an ongoing basis, monitor cost, schedule, and performance against established baselines and use tools to assess risks to an acquisition program at all phases of the life cycle of such program to avoid and mitigate acquisition program baseline breaches.

"(3) The term 'acquisition decision event' means, with respect to an acquisition program, a predetermined point within each of the acquisition phases at

which the acquisition decision authority determines whether such acquisition program shall proceed to the next acquisition phase.

"(4) The term 'acquisition decision memorandum' means, with respect to an acquisition, the official acquisition decision event record that includes a documented record of decisions, exit criteria, and assigned actions for such acquisition, as determined by the person exercising acquisition decision authority for such acquisition.

"(5) The term 'acquisition program' means the process by which the Department acquires, with any appropriated amounts, by contract for purchase or lease, property or services (including construction) that support the missions and goals of the Department.

"(6) The term 'acquisition program baseline', with respect to an acquisition program, means a summary of the cost, schedule, and performance parameters, expressed in standard, measurable, quantitative terms, which must be met in order to accomplish the goals of such program.

"(7) The term 'best practices', with respect to acquisition, means a knowledge-based approach to capability development that includes—

"(A) identifying and validating needs;

"(B) assessing alternatives to select the most appropriate solution;

"(C) clearly establishing well-defined requirements;

"(D) developing realistic cost assessments and schedules;

"(E) securing stable funding that matches resources to requirements;

"(F) demonstrating technology, design, and manufacturing maturity;

"(G) using milestones and exit criteria or specific accomplishments that demonstrate progress;

"(H) adopting and executing standardized processes with known success across programs;

"(I) establishing an adequate workforce that is qualified and sufficient to perform necessary functions; and

"(J) integrating the capabilities described in subparagraphs (A) through (I) into the Department's mission and business operations.

"(8) The term 'breach', with respect to a major acquisition program, means a failure to meet any cost, schedule, or performance threshold specified in the most recently approved acquisition program baseline.

"(9) The term 'congressional homeland security committees' means—

"(A) 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 Committee on Appropriations of the House of Representatives and of the Senate.

"(10) The term 'Component Acquisition Executive' means the senior acquisition official within a component who is designated in writing by the Under Secretary for Management, in consultation with the component head, with authority and responsibility for leading a process and staff to provide acquisition and program management oversight, policy, and guidance to ensure that statutory, regulatory, and higher level policy requirements are fulfilled, including compliance with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives established by the Under Secretary for Management.

"(11) The term 'life cycle cost' means the total ownership cost of an acquisition, including all relevant costs related to acquiring, owning, operating, maintaining, and disposing of the system, project, or product over a specified period of time.

"(12) The term 'major acquisition program' means a Department acquisition program that is estimated by the Secretary to require an eventual total expenditure of at least $300,000,000 (based on fiscal year 2017 constant dollars) over its life cycle cost.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by inserting before the item relating to section 831 the following new item:

"830. Definitions.".

Subtitle A—Acquisition Authorities

SEC. 211. ACQUISITION AUTHORITIES FOR UNDER SECRETARY FOR MANAGEMENT OF THE DEPARTMENT OF HOMELAND SECURITY.

Section 701 of the Homeland Security Act of 2002 (6 U.S.C. 341) is amended—

(1) in subsection (a)(2), by inserting "and acquisition management" after "procurement";

(2) by redesignating subsections (d) and (e) as subsections (e) and (f), respectively; and

(3) by inserting after subsection (c) the following new subsection:

"(d) ACQUISITION AND RELATED RESPONSIBILITIES.—

"(1) IN GENERAL.—Notwithstanding subsection (a) of section 1702 of title 41, United States Code, the Under Secretary for Management is the Chief Acquisition Officer of the Department. As Chief Acquisition Officer, the Under Secretary shall have the authorities and perform the functions specified in subsection (b) of such section and shall perform all other functions and responsibilities delegated by the Secretary or described in this subsection.

"(2) FUNCTIONS AND RESPONSIBILITIES.—In addition to the authorities and functions specified in section 1702(b) of title 41, United States Code, the functions and responsibilities of the Under Secretary for Management related to acquisition include the following:

"(A) Advising the Secretary regarding acquisition management activities, taking into account risks of failure to achieve cost, schedule, or performance parameters, to ensure that the Department achieves its mission through the adoption of widely accepted program management best practices and standards and, where appropriate, acquisition innovation best practices.

"(B) Leading the acquisition oversight body of the Department, the Acquisition Review Board, and exercising the acquisition decision authority to approve, pause, modify (including the rescission of approvals of program milestones), or cancel major acquisition programs, unless the Under Secretary delegates such authority to a Component Acquisition Executive pursuant to paragraph (3).

"(C) Establishing policies for acquisition that implement an approach that takes into account risks of failure to achieve cost, schedule, or performance parameters that all components of the Department shall comply with, including outlining relevant authorities for program managers to effectively manage acquisition programs.

"(D) Ensuring that each major acquisition program has a Department-approved acquisition program baseline, pursuant to the Department's acquisition management policy.

"(E) Ensuring that the heads of components and Component Acquisition Executives comply with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives.

"(F) Providing additional scrutiny and oversight for an acquisition that is not a major acquisition if—

"(i) the acquisition is for a program that is important to departmental strategic and performance plans;

"(ii) the acquisition is for a program with significant program or policy implications; and

"(iii) the Secretary determines that such scrutiny and oversight for the acquisition is proper and necessary.

"(G) Ensuring that grants and financial assistance are provided only to individuals and organizations that are not suspended or debarred.

"(H) Distributing guidance throughout the Department to ensure that contractors involved in acquisitions, particularly contractors that access the Department's information systems and technologies, adhere to relevant Department policies related to physical and information security as identified by the Under Secretary for Management.

"(I) Overseeing the Component Acquisition Executive organizational structure to ensure Component Acquisition Executives have sufficient capabilities and comply with Department acquisition policies.

"(J) Ensuring acquisition decision memoranda adequately document decisions made at acquisition decision events, including any affirmative determination of contractor responsibility at the down selection phase and any other significant procurement decisions related to the acquisition at issue.

"(3) DELEGATION OF ACQUISITION DECISION AUTHORITY.—

"(A) LEVEL 3 ACQUISITIONS.—The Under Secretary for Management may delegate acquisition decision authority in writing to the relevant Component Acquisition Executive for an acquisition program that has a life cycle cost estimate of less than $300,000,000.

"(B) LEVEL 2 ACQUISITIONS.—The Under Secretary for Management may delegate acquisition decision authority in writing to the relevant Component Acquisition Executive for a major acquisition program that has a life

cycle cost estimate of at least $300,000,000 but not more than $1,000,000,000 if all of the following requirements are met:

"(i) The component concerned possesses working policies, processes, and procedures that are consistent with Department-level acquisition policy.

"(ii) The Component Acquisition Executive concerned has adequate, experienced, and dedicated professional employees with program management training, as applicable, commensurate with the size of the acquisition programs and related activities delegated to such Component Acquisition Executive by the Under Secretary for Management.

"(iii) Each major acquisition program concerned has written documentation showing that it has a Department-approved acquisition program baseline and it is meeting agreed-upon cost, schedule, and performance thresholds.

"(4) RELATIONSHIP TO UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.—

"(A) IN GENERAL.—Nothing in this subsection shall diminish the authority granted to the Under Secretary for Science and Technology under this Act. The Under Secretary for Management and the Under Secretary for Science and Technology shall cooperate in matters related to the coordination of acquisitions across the Department so that investments of the Directorate of Science and Technology are able to support current and future requirements of the components of the Department.

"(B) OPERATIONAL TESTING AND EVALUATION.—The Under Secretary for Science and Technology shall—

"(i) ensure, in coordination with relevant component heads, that major acquisition programs—

"(I) complete operational testing and evaluation of technologies and systems;

"(II) use independent verification and validation of operational test and evaluation implementation and results; and

"(III) document whether such programs meet all performance requirements included in their acquisition program baselines;

"(ii) ensure that such operational testing and evaluation includes all system components and incorporates operators into the testing to ensure that systems perform as intended in the appropriate operational setting; and

"(iii) determine if testing conducted by other Federal agencies and private entities is relevant and sufficient in determining whether systems perform as intended in the operational setting.

"(5) DEFINITIONS.—In this subsection, the terms 'acquisition', 'best practices', 'acquisition decision authority', 'major acquisition program', 'acquisition program baseline', and 'Component Acquisition Executive' have the meanings given such terms in section 830.".

SEC. 212. ACQUISITION AUTHORITIES FOR CHIEF FINANCIAL OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.

Paragraph (2) of section 702(b) of the Homeland Security Act of 2002 (6 U.S.C. 342(b)) is amended by adding at the end the following new subparagraph:

"(J) Oversee the costs of acquisition programs and related activities to ensure that actual and planned costs are in accordance with budget estimates and are affordable, or can be adequately funded, over the life cycle of such programs and activities.".

SEC. 213. ACQUISITION AUTHORITIES FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.

Section 703 of the Homeland Security Act of 2002 (6 U.S.C. 343) is amended—

(1) by redesignating subsection (b) as subsection (c); and

(2) by inserting after subsection (a) the following new subsection:

"(b) ACQUISITION RESPONSIBILITIES.—Notwithstanding section 11315 of title 40, United States Code, the acquisition responsibilities of the Chief Information Officer, in consultation with the Under Secretary for Management, shall include the following:

"(1) Oversee the management of the Homeland Security Enterprise Architecture and ensure that, before each acquisition decision event (as such term is defined in section 830), approved information technology acquisitions comply with departmental information technology management processes, technical requirements, and the Homeland Security Enterprise Architecture, and in any case in which information technology acquisitions do not comply with the Department's management directives, make recommendations to the Acquisition Review Board regarding such noncompliance.

"(2) Be responsible for providing recommendations to the Acquisition Review Board regarding information technology programs, and be responsible for developing information technology acquisition strategic guidance.".

SEC. 214. ACQUISITION AUTHORITIES FOR PROGRAM ACCOUNTABILITY AND RISK MANAGEMENT.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.) is further amended by adding at the end the following:

"SEC. 717. ACQUISITION AUTHORITIES FOR PROGRAM ACCOUNTABILITY AND RISK MANAGEMENT.

"(a) ESTABLISHMENT OF OFFICE.—There is in the Management Directorate of the Department an office to be known as 'Program Accountability and Risk Management'. The purpose of the office is to—

"(1) provide consistent accountability, standardization, and transparency of major acquisition programs of the Department; and

"(2) serve as the central oversight function for all Department acquisition programs.

"(b) RESPONSIBILITIES OF EXECUTIVE DIRECTOR.—The Program Accountability and Risk Management shall be led by an Executive Director to oversee the requirement under subsection (a). The Executive Director shall report directly to the Under Secretary for Management, and shall carry out the following responsibilities:

"(1) Monitor regularly the performance of Department acquisition programs between acquisition decision events to identify problems with cost, performance, or schedule that components may need to address to prevent cost overruns, performance issues, or schedule delays.

"(2) Assist the Under Secretary for Management in managing the acquisition programs and related activities of the Department.

"(3) Conduct oversight of individual acquisition programs to implement Department acquisition program policy, procedures, and guidance with a priority on ensuring the data the office collects and maintains from Department components is accurate and reliable.

"(4) Serve as the focal point and coordinator for the acquisition life cycle review process and as the executive secretariat for the Acquisition Review Board.

"(5) Advise the persons having acquisition decision authority in making acquisition decisions consistent with all applicable laws and in establishing clear lines of authority, accountability, and responsibility for acquisition decision making within the Department.

"(6) Engage in the strategic planning and performance evaluation process required under section 306 of title 5, United States Code, and sections 1105(a)(28), 1115, 1116, and 9703 of title 31, United States Code, by supporting the Chief Procurement Officer in developing strategies and specific plans for hiring, training, and professional development in order to rectify any deficiency within the Department's acquisition workforce.

"(7) Develop standardized certification standards in consultation with the Component Acquisition Executives for all acquisition program managers.

"(8) In the event that a certification or action of an acquisition program manager needs review for purposes of promotion or removal, provide input, in consultation with the relevant Component Acquisition Executive, into the performance evaluation of the relevant acquisition program manager and report positive or negative experiences to the relevant certifying authority.

"(9) Provide technical support and assistance to Department acquisitions and acquisition personnel in conjunction with the Chief Procurement Officer.

"(10) Prepare the Comprehensive Acquisition Status Report for the Department, as required by title I of division D of the Consolidated Appropriations Act, 2016 (Public Law 114–113), and make such report available to the congressional homeland security committees.

"(c) RESPONSIBILITIES OF COMPONENTS.—Each head of a component shall comply with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives established by the Under Secretary for Management. For each major acquisition program, each head of a component shall—

"(1) define baseline requirements and document changes to such requirements, as appropriate;

"(2) establish a complete life cycle cost estimate with supporting documentation, including an acquisition program baseline;

"(3) verify each life cycle cost estimate against independent cost estimates, and reconcile any differences;

"(4) complete a cost-benefit analysis with supporting documentation;

"(5) develop and maintain a schedule that is consistent with scheduling best practices as identified by the Comptroller General of the United States, including, in appropriate cases, an integrated master schedule; and

"(6) ensure that all acquisition program information provided by the component is complete, accurate, timely, and valid.

"(d) CONGRESSIONAL HOMELAND SECURITY COMMITTEES DEFINED.—In this section, the term 'congressional homeland security committees' means—

"(1) the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate; and

"(2) the Committee on Appropriations of the House of Representatives and the Committee on Appropriations of the Senate.

"SEC. 718. ACQUISITION DOCUMENTATION.

"(a) IN GENERAL.—For each major acquisition program, the Executive Director responsible for the preparation of the Comprehensive Acquisition Status Report, pursuant to paragraph (11) of section 710(b), shall require certain acquisition documentation to be submitted by Department components or offices.

"(b) WAIVER.—The Secretary may waive the requirement for submission under subsection (a) for a program for a fiscal year if either—

"(1) the program has not—

"(A) entered the full rate production phase in the acquisition life cycle;

"(B) had a reasonable cost estimate established; and

"(C) had a system configuration defined fully; or

"(2) the program does not meet the definition of 'capital asset', as defined by the Director of the Office of Management and Budget.

"(c) CONGRESSIONAL OVERSIGHT.—At the same time the President's budget is submitted for a fiscal year under section 1105(a) of title 31, United States Code, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and Committee on Homeland Security and Governmental Affairs of the Senate information on the exercise of authority under subsection (b) in the prior fiscal year that includes the following specific information regarding each program for which a waiver is issued under subsection (b):

"(1) The grounds for granting a waiver for that program.

"(2) The projected cost of that program.

"(3) The proportion of a component's annual acquisition budget attributed to that program, as available.

"(4) Information on the significance of the program with respect to the component's operations and execution of its mission.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is further amended by inserting after the item relating to section 716, as added by this Act, the following new items:

"Sec. 717. Acquisition authorities for Program Accountability and Risk Management.
"Sec. 718. Acquisition documentation.".

SEC. 215. ACQUISITION INNOVATION.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.) as amended by this Act, is further amended by adding at the end the following new section:

"SEC. 719. ACQUISITION INNOVATION.

"The Under Secretary for Management may—

"(1) designate an individual within the Department to manage acquisition innovation efforts of the Department;

"(2) test emerging acquisition best practices to carrying out acquisitions, consistent with the Federal Acquisition Regulation and Department acquisition management directives, as appropriate;

"(3) develop and distribute best practices and lessons learned regarding acquisition innovation throughout the Department;

"(4) establish metrics to measure the effectiveness of acquisition innovation efforts with respect to cost, operational efficiency of the acquisition program (including timeframes for executing contracts), and collaboration with the private sector, including small businesses; and

"(5) determine impacts of acquisition innovation efforts on the private sector by—

"(A) engaging with the private sector, including small businesses, to provide information and obtain feedback on procurement practices and acquisition innovation efforts of the Department;

"(B) obtaining feedback from the private sector on the impact of acquisition innovation efforts of the Department; and

"(C) incorporating such feedback, as appropriate, into future acquisition innovation efforts of the Department.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 718, as added by this Act, the following new item:

"Sec. 719. Acquisition innovation.".

(c) INFORMATION.—Not later than 90 days after the date on which the Secretary of Homeland Security submits the annual budget justification for the Department of Homeland Security for each of fiscal years 2019 through 2023, the Secretary shall, if appropriate, provide information to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on the activities undertaken in the previous fiscal year in furtherance of section 719 of the Homeland Security Act of 2002, as added by subsection (a) of this Act, on the following:

(1) Emerging acquisition best practices that were tested within the Department during such fiscal year.

(2) Efforts to distribute best practices and lessons learned within the Department, including through web-based seminars, training, and forums, during such fiscal year.

(3) Utilization by components throughout the Department of best practices distributed by the Under Secretary of Management pursuant to paragraph (3) of such section 719.

(4) Performance as measured by the metrics established under paragraph (4) of such section 719.

(5) Outcomes of efforts to distribute best practices and lessons learned within the Department, including through web-based seminars, training, and forums.

(6) Any impacts of the utilization of innovative acquisition mechanisms by the Department on the private sector, including small businesses.

(7) The criteria used to identify specific acquisition programs or activities to be included in acquisition innovation efforts and the outcomes of such programs or activities.

(8) Recommendations, as necessary, to enhance acquisition innovation in the Department.

Subtitle B—Acquisition Program Management Discipline

SEC. 221. ACQUISITION REVIEW BOARD.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.) is amended by adding at the end the following new section:

"SEC. 836. ACQUISITION REVIEW BOARD.

"(a) IN GENERAL.—The Secretary shall establish an Acquisition Review Board (in this section referred to as the 'Board') to—

"(1) strengthen accountability and uniformity within the Department acquisition review process;

"(2) review major acquisition programs; and

"(3) review the use of best practices.

"(b) COMPOSITION.—The Under Secretary for Management shall serve as chair of the Board. The Secretary shall also ensure participation by other relevant Department officials, including at least two component heads or their designees, as permanent members of the Board.

"(c) MEETINGS.—The Board shall meet regularly for purposes of ensuring all acquisitions processes proceed in a timely fashion to achieve mission readiness. The Board shall convene at the discretion of the Secretary and at any time—

"(1) a major acquisition program—

"(A) requires authorization to proceed from one acquisition decision event to another throughout the acquisition life cycle;

"(B) is in breach of its approved requirements; or

"(C) requires additional review, as determined by the Under Secretary for Management; or

"(2) a non-major acquisition program requires review, as determined by the Under Secretary for Management.

"(d) RESPONSIBILITIES.—The responsibilities of the Board are as follows:

"(1) Determine whether a proposed acquisition has met the requirements of key phases of the acquisition life cycle framework and is able to proceed to the next phase and eventual full production and deployment.

"(2) Oversee whether a proposed acquisition's business strategy, resources, management, and accountability is executable and is aligned to strategic initiatives.

"(3) Support the person with acquisition decision authority for an acquisition in determining the appropriate direction for such acquisition at key acquisition decision events.

"(4) Conduct systematic reviews of acquisitions to ensure that such acquisitions are progressing in compliance with the approved documents for their current acquisition phases.

"(5) Review the acquisition documents of each major acquisition program, including the acquisition program baseline and documentation reflecting consideration of tradeoffs among cost, schedule, and performance objectives, to ensure the reliability of underlying data.

"(6) Ensure that practices are adopted and implemented to require consideration of trade-offs among cost, schedule, and performance objectives as part of the process for developing requirements for major acquisition programs prior to the initiation of the second acquisition decision event, including, at a minimum, the following practices:

"(A) Department officials responsible for acquisition, budget, and cost estimating functions are provided with the appropriate opportunity to develop estimates and raise cost and schedule matters before performance objectives are established for capabilities when feasible.

"(B) Full consideration is given to possible trade-offs among cost, schedule, and performance objectives for each alternative.

"(e) ACQUISITION PROGRAM BASELINE REPORT REQUIREMENT.—If the person exercising acquisition decision authority over a major acquisition program approves such program to proceed into the planning phase before such program has a Department-approved acquisition program baseline, the Under Secretary for Management shall create and approve an acquisition program baseline report regarding such approval, and the Secretary shall—

"(1) within seven days after an acquisition decision memorandum is signed, notify in writing the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate of such decision; and

"(2) within 60 days after the acquisition decision memorandum is signed, submit to such committees a report stating the rationale for such decision and a plan of action to require an acquisition program baseline for such program.

"(f) REPORT.—The Under Secretary for Management shall provide information to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on an annual basis through fiscal year 2022 on the activities of the Board for the prior fiscal year that includes information relating to the following:

"(1) For each meeting of the Board, any acquisition decision memoranda.

"(2) Results of the systematic reviews conducted pursuant to paragraph (4) of subsection (d).

"(3) Results of acquisition document reviews required pursuant to paragraph (5) of subsection (d).

"(4) Activities to ensure that practices are adopted and implemented throughout the Department pursuant to paragraph (6) of subsection (d).".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is further amended by adding after the item relating to section 835 the following new item:

"Sec. 836. Acquisition Review Board.".

SEC. 222. REQUIREMENTS TO REDUCE DUPLICATION IN ACQUISITION PROGRAMS.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.) is further amended by adding at the end the following new section:

"SEC. 837. REQUIREMENTS TO REDUCE DUPLICATION IN ACQUISITION PROGRAMS.

"(a) REQUIREMENT TO ESTABLISH POLICIES.—In an effort to reduce unnecessary duplication and inefficiency for all Department investments, including major acquisition programs, the Deputy Secretary, in consultation with the Under Secretary for Management, shall establish Department-wide policies to integrate all phases of the investment life cycle and help the Department identify, validate, and prioritize common component requirements for major acquisition programs in order to increase opportunities for effectiveness and efficiencies. The policies shall also include strategic alternatives for developing and facilitating a Department component-driven requirements process that includes oversight of a development test and evaluation capability; identification of priority gaps and overlaps in Department capability needs;

and provision of feasible technical alternatives, including innovative commercially available alternatives, to meet capability needs.

"(b) MECHANISMS TO CARRY OUT REQUIREMENT.—The Under Secretary for Management shall coordinate the actions necessary to carry out subsection (a), using such mechanisms as considered necessary by the Secretary to help the Department reduce unnecessary duplication and inefficiency for all Department investments, including major acquisition programs.

"(c) COORDINATION.—In coordinating the actions necessary to carry out subsection (a), the Deputy Secretary shall consult with the Under Secretary for Management, Component Acquisition Executives, and any other Department officials, including the Under Secretary for Science and Technology or his designee, with specific knowledge of Department or component acquisition capabilities to prevent unnecessary duplication of requirements.

"(d) ADVISORS.—The Deputy Secretary, in consultation with the Under Secretary for Management, shall seek and consider input within legal and ethical boundaries from members of Federal, State, local, and tribal governments, nonprofit organizations, and the private sector, as appropriate, on matters within their authority and expertise in carrying out the Department's mission.

"(e) MEETINGS.—The Deputy Secretary, in consultation with the Under Secretary for Management, shall meet at least quarterly and communicate with components often to ensure that components do not overlap or duplicate spending or activities on major investments and acquisition programs within their areas of responsibility.

"(f) RESPONSIBILITIES.—In carrying out this section, the responsibilities of the Deputy Secretary, in consultation with the Under Secretary for Management, are as follows:

"(1) To review and validate the requirements documents of major investments and acquisition programs prior to acquisition decision events of the investments or programs.

"(2) To ensure the requirements and scope of a major investment or acquisition program are stable, measurable, achievable, at an acceptable risk level, and match the resources planned to be available.

"(3) Before any entity of the Department issues a solicitation for a new contract, coordinate with other Department entities as appropriate to prevent unnecessary duplication and inefficiency and—

"(A) to implement portfolio reviews to identify common mission requirements and crosscutting opportunities among components to harmonize investments and requirements and prevent unnecessary overlap and duplication among components; and

"(B) to the extent practicable, to standardize equipment purchases, streamline the acquisition process, improve efficiencies, and conduct best practices for strategic sourcing.

"(4) To ensure program managers of major investments and acquisition programs conduct analyses, giving particular attention to factors such as cost, schedule, risk, performance, and operational efficiency in order to determine that programs work as intended within cost and budget expectations.

"(5) To propose schedules for delivery of the operational capability needed to meet each Department investment and major acquisition program.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is further amended by adding after the item relating to section 836, as added by this Act, the following new item:

"Sec. 837. Requirements to reduce duplication in acquisition programs.".

SEC. 223. DEPARTMENT LEADERSHIP COUNCIL.

(a) IN GENERAL.—Subtitle H of title VIII of the Homeland Security Act of 2002 is amended by adding at the end the following new section:

"SEC. 890B. DEPARTMENT LEADERSHIP COUNCIL.

"(a) DEPARTMENT LEADERSHIP COUNCIL.—

"(1) ESTABLISHMENT.—The Secretary may establish a Department leadership council as the Secretary determines necessary to ensure coordination and improve programs and activities of the Department.

"(2) FUNCTION.—A Department leadership council shall—

"(A) serve as coordinating forums;

"(B) advise the Secretary and Deputy Secretary on Department strategy, operations, and guidance; and

"(C) consider and report on such other matters as the Secretary or Deputy Secretary may direct.

"(3) RELATIONSHIP TO OTHER FORUMS.—The Secretary or Deputy Secretary may delegate the authority to direct the implementation of any decision or guid-

ance resulting from the action of a Department leadership council to any office, component, coordinator, or other senior official of the Department.

"(4) MISSION.—In addition to other matters assigned to it by the Secretary and Deputy Secretary, a leadership council shall—

"(A) identify, assess, and validate joint requirements (including existing systems and associated capability gaps) to meet mission needs of the Department;

"(B) ensure that appropriate efficiencies are made among life-cycle cost, schedule, and performance objectives, and procurement quantity objectives, in the establishment and approval of joint requirements; and

"(C) make prioritized capability recommendations for the joint requirements validated under subparagraph (A) to the Secretary, the Deputy Secretary, or the chairperson of a Department leadership council designated by the Secretary to review decisions of the leadership council.

"(5) CHAIRPERSON.—The Secretary shall appoint a chairperson of a leadership council, for a term of not more than 2 years, from among senior officials from components of the Department or other senior officials as designated by the Secretary.

"(6) COMPOSITION.—A leadership council shall be composed of senior officials representing components of the Department and other senior officials as designated by the Secretary.

"(7) RELATIONSHIP TO FUTURE YEARS HOMELAND SECURITY PROGRAM.—The Secretary shall ensure that the Future Years Homeland Security Program required under section 874 is consistent with any recommendations of a leadership council required under paragraph (2)(C), as affirmed by the Secretary, the Deputy Secretary, or the chairperson of a Department leadership council designated by the Secretary under that paragraph.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 890A the following new item:

"Sec. 890B. Department leadership council.".

SEC. 224. GOVERNMENT ACCOUNTABILITY OFFICE REVIEW OF BOARD AND OF REQUIREMENTS TO REDUCE DUPLICATION IN ACQUISITION PROGRAMS.

(a) REVIEW REQUIRED.—The Comptroller General of the United States shall conduct a review of the effectiveness of the Acquisition Review Board established under section 836 of the Homeland Security Act of 2002 (as added by section 221) and the requirements to reduce unnecessary duplication in acquisition programs established under section 837 of such Act (as added by section 222) in improving the Department's acquisition management process.

(b) SCOPE OF REPORT.—The review shall include the following:

(1) An assessment of the effectiveness of the Board in increasing program management oversight, best practices and standards, and discipline among the components of the Department, including in working together and in preventing overlap and unnecessary duplication.

(2) An assessment of the effectiveness of the Board in instilling program management discipline.

(3) A statement of how regularly each major acquisition program is reviewed by the Board, how often the Board stops major acquisition programs from moving forward in the phases of the acquisition life cycle process, and the number of major acquisition programs that have been halted because of problems with operational effectiveness, schedule delays, or cost overruns.

(4) An assessment of the effectiveness of the Board in impacting acquisition decisionmaking within the Department, including the degree to which the Board impacts decision making within other headquarters mechanisms and bodies involved in the administration of acquisition activities.

(c) REPORT REQUIRED.—Not later than one year after the date of the enactment of this Act, the Comptroller General shall submit to the congressional homeland security committees a report on the review required by this section. The report shall be submitted in unclassified form but may include a classified annex.

SEC. 225. EXCLUDED PARTY LIST SYSTEM WAIVERS.

Not later than five days after the issuance of a waiver by the Secretary of Homeland Security of Federal requirements that an agency not engage in business with a contractor in the Excluded Party List System (or successor system) as maintained by the General Services Administration, the Secretary shall submit to Congress notice of such waiver and an explanation for a finding by the Secretary that a compelling reason exists for issuing such waiver.

SEC. 226. INSPECTOR GENERAL OVERSIGHT OF SUSPENSION AND DEBARMENT.

The Inspector General of the Department of Homeland Security—

(1) may audit decisions about grant and procurement awards to identify instances where a contract or grant was improperly awarded to a suspended or debarred entity and whether corrective actions were taken to prevent recurrence; and

(2) shall review the suspension and debarment program throughout the Department of Homeland Security to assess whether suspension and debarment criteria are consistently applied throughout the Department and whether disparities exist in the application of such criteria, particularly with respect to business size and categories.

Subtitle C—Acquisition Program Management Accountability and Transparency

SEC. 231. CONGRESSIONAL NOTIFICATION FOR MAJOR ACQUISITION PROGRAMS.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.) is further amended by adding at the end the following new section:

"SEC. 838. CONGRESSIONAL NOTIFICATION AND OTHER REQUIREMENTS FOR MAJOR ACQUISITION PROGRAM BREACH.

"(a) REQUIREMENTS WITHIN DEPARTMENT IN EVENT OF BREACH.—

"(1) NOTIFICATIONS.—

"(A) NOTIFICATION OF BREACH.—If a breach occurs in a major acquisition program, the program manager for such program shall notify the Component Acquisition Executive for such program, the head of the component concerned, the Executive Director of the Program Accountability and Risk Management division, the Under Secretary for Management, and the Deputy Secretary not later than 30 calendar days after such breach is identified.

"(B) NOTIFICATION TO SECRETARY.—If a breach occurs in a major acquisition program and such breach results in a cost overrun greater than 15 percent, a schedule delay greater than 180 days, or a failure to meet any of the performance thresholds from the cost, schedule, or performance parameters specified in the most recently approved acquisition program baseline for such program, the Component Acquisition Executive for such program shall notify the Secretary and the Inspector General of the Department not later than five business days after the Component Acquisition Executive for such program, the head of the component concerned, the Executive Director of the Program Accountability and Risk Management Division, the Under Secretary for Management, and the Deputy Secretary are notified of the breach pursuant to subparagraph (A).

"(2) REMEDIATION PLAN AND ROOT CAUSE ANALYSIS.—

"(A) IN GENERAL.—If a breach occurs in a major acquisition program, the program manager for such program shall submit to the head of the component concerned, the Executive Director of the Program Accountability and Risk Management division, and the Under Secretary for Management in writing a remediation plan and root cause analysis relating to such breach and program. Such plan and analysis shall be submitted at a date established at the discretion of the Under Secretary for Management.

"(B) REMEDIATION PLAN.—The remediation plan required under this subparagraph (A) shall—

"(i) explain the circumstances of the breach at issue;

"(ii) provide prior cost estimating information;

"(iii) include a root cause analysis that determines the underlying cause or causes of shortcomings in cost, schedule, or performance of the major acquisition program with respect to which such breach has occurred, including the role, if any, of—

"(I) unrealistic performance expectations;

"(II) unrealistic baseline estimates for cost or schedule or changes in program requirements;

"(III) immature technologies or excessive manufacturing or integration risk;

"(IV) unanticipated design, engineering, manufacturing, or technology integration issues arising during program performance;

"(V) changes to the scope of such program;

"(VI) inadequate program funding or changes in planned out-year funding from one 5-year funding plan to the next 5-year funding

plan as outlined in the Future Years Homeland Security Program required under section 874;

"(VII) legislative, legal, or regulatory changes; or

"(VIII) inadequate program management personnel, including lack of sufficient number of staff, training, credentials, certifications, or use of best practices;

"(iv) propose corrective action to address cost growth, schedule delays, or performance issues;

"(v) explain the rationale for why a proposed corrective action is recommended; and

"(vi) in coordination with the Component Acquisition Executive for such program, discuss all options considered, including the estimated impact on cost, schedule, or performance of such program if no changes are made to current requirements, the estimated cost of such program if requirements are modified, and the extent to which funding from other programs will need to be reduced to cover the cost growth of such program.

"(3) REVIEW OF CORRECTIVE ACTIONS.—

"(A) IN GENERAL.—The Under Secretary for Management shall review the remediation plan required under paragraph (2). The Under Secretary may approve such plan or provide an alternative proposed corrective action within 30 days of the submission of such plan under such paragraph.

"(B) SUBMISSION TO CONGRESS.—Not later than 30 days after the review required under subparagraph (A) is completed, the Under Secretary for Management shall submit to the congressional homeland security committees the following:

"(i) A copy of the remediation plan and the root cause analysis required under paragraph (2).

"(ii) A statement describing the corrective action or actions that have occurred pursuant to paragraph (2)(b)(iv) for the major acquisition program at issue, with a justification for such action or actions.

"(b) REQUIREMENTS RELATING TO CONGRESSIONAL NOTIFICATION IF BREACH OCCURS.—

"(1) NOTIFICATION TO CONGRESS.—If a notification to the Secretary is made under subsection (a)(1)(B) relating to a breach in a major acquisition program, the Under Secretary for Management shall notify the congressional homeland security committees of such breach in the next quarterly Comprehensive Acquisition Status Report, as required by title I of division D of the Consolidated Appropriations Act, 2016, (Public Law 114–113) following receipt by the Under Secretary of notification under such subsection.

"(2) SIGNIFICANT VARIANCES IN COSTS OR SCHEDULE.—If a likely cost overrun is greater than 20 percent or a likely delay is greater than 12 months from the costs and schedule specified in the acquisition program baseline for a major acquisition program, the Under Secretary for Management shall include in the notification required in paragraph (1) a written certification, with supporting explanation, that—

"(A) such program is essential to the accomplishment of the Department's mission;

"(B) there are no alternatives to the capability or asset provided by such program that will provide equal or greater capability in both a more cost-effective and timely manner;

"(C) the new acquisition schedule and estimates for total acquisition cost are reasonable; and

"(D) the management structure for such program is adequate to manage and control cost, schedule, and performance.

"(c) CONGRESSIONAL HOMELAND SECURITY COMMITTEES DEFINED.—In this section, the term 'congressional homeland security committees' means—

"(1) the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate; and

"(2) the Committee on Appropriations of the House of Representatives and the Committee on Appropriations of the Senate.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 837, as added by this Act, the following new item:

"Sec. 838. Congressional notification and other requirements for major acquisition program breach.".

SEC. 232. MULTIYEAR ACQUISITION STRATEGY.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.) is further amended by adding at the end the following new section:

"SEC. 839. MULTIYEAR ACQUISITION STRATEGY.

"(a) MULTIYEAR ACQUISITION STRATEGY REQUIRED.—

"(1) IN GENERAL.—Not later than one year after the date of the enactment of this section, the Secretary shall submit to the appropriate congressional committees and the Comptroller General of the United States a multiyear acquisition strategy to guide the overall direction of the acquisitions of the Department while allowing flexibility to deal with ever-changing threats and risks, to keep pace with changes in technology that could impact deliverables, and to help industry better understand, plan, and align resources to meet the future acquisition needs of the Department. Such strategy shall be updated and included in each Future Years Homeland Security Program required under section 874.

"(2) FORM.—The strategy required under paragraph (1) shall be submitted in unclassified form but may include a classified annex for any sensitive or classified information if necessary. The Secretary shall publish such strategy in an unclassified format that is publicly available.

"(b) CONSULTATION.—In developing the strategy required under subsection (a), the Secretary shall, as the Secretary determines appropriate, consult with headquarters, components, employees in the field, and individuals from industry and the academic community.

"(c) CONTENTS OF STRATEGY.—The strategy shall include the following:

"(1) PRIORITIZED LIST.—A systematic and integrated prioritized list developed by the Under Secretary for Management in coordination with all of the Component Acquisition Executives of Department major acquisition programs that Department and component acquisition investments seek to address, including the expected security and economic benefit of the program or system that is the subject of acquisition and an analysis of how the security and economic benefit derived from such program or system will be measured.

"(2) INVENTORY.—A plan to develop a reliable Department-wide inventory of investments and real property assets to help the Department—

"(A) plan, budget, schedule, and acquire upgrades of its systems and equipment; and

"(B) plan for the acquisition and management of future systems and equipment.

"(3) FUNDING GAPS.—A plan to address funding gaps between funding requirements for major acquisition programs and known available resources, including, to the maximum extent practicable, ways of leveraging best practices to identify and eliminate overpayment for items to—

"(A) prevent wasteful purchasing;

"(B) achieve the greatest level of efficiency and cost savings by rationalizing purchases;

"(C) align pricing for similar items; and

"(D) utilize purchase timing and economies of scale.

"(4) IDENTIFICATION OF CAPABILITIES.—An identification of test, evaluation, modeling, and simulation capabilities that will be required to—

"(A) support the acquisition of technologies to meet the needs of such strategy;

"(B) leverage to the greatest extent possible emerging technological trends and research and development trends within the public and private sectors; and

"(C) identify ways to ensure that appropriate technology is acquired and integrated into the Department's operating doctrine to improve mission performance.

"(5) FOCUS ON FLEXIBLE SOLUTIONS.—An assessment of ways the Department can improve its ability to test and acquire innovative solutions to allow needed incentives and protections for appropriate risk-taking in order to meet its acquisition needs with resiliency, agility, and responsiveness to assure homeland security and facilitate trade.

"(6) FOCUS ON INCENTIVES TO SAVE TAXPAYER DOLLARS.—An assessment of ways the Department can develop incentives for program managers and senior Department acquisition officials to—

"(A) prevent cost overruns;

"(B) avoid schedule delays; and

"(C) achieve cost savings in major acquisition programs.

"(7) FOCUS ON ADDRESSING DELAYS AND BID PROTESTS.—An assessment of ways the Department can improve the acquisition process to minimize cost overruns in—

"(A) requirements development;
"(B) procurement announcements;
"(C) requests for proposals;
"(D) evaluation of proposals;
"(E) protests of decisions and awards; and
"(F) the use of best practices.

"(8) FOCUS ON IMPROVING OUTREACH.—An identification and assessment of ways to increase opportunities for communication and collaboration with industry, small and disadvantaged businesses, intra-government entities, university centers of excellence, accredited certification and standards development organizations, and national laboratories to ensure that the Department understands the market for technologies, products, and innovation that is available to meet its mission needs and to inform the Department's requirements-setting process before engaging in an acquisition, including—

"(A) methods designed especially to engage small and disadvantaged businesses, a cost-benefit analysis of the tradeoffs that small and disadvantaged businesses provide, information relating to barriers to entry for small and disadvantaged businesses, and information relating to unique requirements for small and disadvantaged businesses; and

"(B) within the Department Vendor Communication Plan and Market Research Guide, instructions for interaction by acquisition program managers with such entities to—

"(i) prevent misinterpretation of acquisition regulations; and

"(ii) permit, within legal and ethical boundaries, interacting with such entities with transparency.

"(9) COMPETITION.—A plan regarding competition under subsection (d).

"(10) ACQUISITION WORKFORCE.—A plan regarding the Department acquisition workforce under subsection (e).

"(d) COMPETITION PLAN.—The strategy required under subsection (a) shall also include a plan to address actions to ensure competition, or the option of competition, for major acquisition programs. Such plan may include assessments of the following measures in appropriate cases if such measures are cost effective:

"(1) Competitive prototyping.
"(2) Dual-sourcing.
"(3) Unbundling of contracts.
"(4) Funding of next-generation prototype systems or subsystems.
"(5) Use of modular, open architectures to enable competition for upgrades.
"(6) Acquisition of complete technical data packages.
"(7) Periodic competitions for subsystem upgrades.
"(8) Licensing of additional suppliers, including small businesses.
"(9) Periodic system or program reviews to address long-term competitive effects of program decisions.

"(e) ACQUISITION WORKFORCE PLAN.—

"(1) ACQUISITION WORKFORCE.—The strategy required under subsection (a) shall also include a plan to address Department acquisition workforce accountability and talent management that identifies the acquisition workforce needs of each component performing acquisition functions and develops options for filling such needs with qualified individuals, including a cost-benefit analysis of contracting for acquisition assistance.

"(2) ADDITIONAL MATTERS COVERED.—The acquisition workforce plan under this subsection shall address ways to—

"(A) improve the recruitment, hiring, training, and retention of Department acquisition workforce personnel, including contracting officer's representatives, in order to retain highly qualified individuals who have experience in the acquisition life cycle, complex procurements, and management of large programs;

"(B) empower program managers to have the authority to manage their programs in an accountable and transparent manner as such managers work with the acquisition workforce;

"(C) prevent duplication within Department acquisition workforce training and certification requirements through leveraging already-existing training within the Federal Government, academic community, or private industry;

"(D) achieve integration and consistency with Government-wide training and accreditation standards, acquisition training tools, and training facilities;

"(E) designate the acquisition positions that will be necessary to support the Department acquisition requirements, including in the fields of—

"(i) program management;

"(ii) systems engineering;

"(iii) procurement, including contracting;

"(iv) test and evaluation;

"(v) life cycle logistics;

"(vi) cost estimating and program financial management; and

"(vii) additional disciplines appropriate to Department mission needs;

"(F) strengthen the performance of contracting officers' representatives (as defined in subpart 1.602–2 and subpart 2.101 of the Federal Acquisition Regulation), including by—

"(i) assessing the extent to which such representatives are certified and receive training that is appropriate;

"(ii) assessing what training is most effective with respect to the type and complexity of assignment; and

"(iii) implementing actions to improve training based on such assessments; and

"(G) identify ways to increase training for relevant investigators and auditors of the Department to examine fraud in major acquisition programs, including identifying opportunities to leverage existing Government and private sector resources in coordination with the Inspector General of the Department.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 838, as added by this Act, the following new item:

"Sec. 839. Multiyear acquisition strategy.".

(c) GOVERNMENT ACCOUNTABILITY OFFICE REVIEW OF MULTI-YEAR ACQUISITION STRATEGY.—

(1) REVIEW.—After submission of the first multiyear acquisition strategy in accordance with section 839 of the Homeland Security Act of 2002, as added by subsection (a), after the date of the enactment of this Act, the Comptroller General of the United States shall conduct a review of such plan within 180 days to analyze the viability of such plan's effectiveness in the following:

(A) Complying with the requirements of such section 839.

(B) Establishing clear connections between Department of Homeland Security objectives and acquisition priorities.

(C) Demonstrating that Department acquisition policy reflects program management best practices and standards.

(D) Ensuring competition or the option of competition for major acquisition programs.

(E) Considering potential cost savings through using already-existing technologies when developing acquisition program requirements.

(F) Preventing duplication within Department acquisition workforce training requirements through leveraging already-existing training within the Federal Government, academic community, or private industry.

(G) Providing incentives for acquisition program managers to reduce acquisition and procurement costs through the use of best practices and disciplined program management.

(2) DEFINITIONS.—The terms "acquisition", "best practices", and "major acquisition programs" have the meaning given such terms in section 830 of the Homeland Security Act of 2002, as added by section 201.

(3) REPORT.—Not later than 180 days after the completion of the review required by subsection (a), the Comptroller General of the United States shall submit to 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 a report on the review. Such report shall be submitted in unclassified form but may include a classified annex.

SEC. 233. ACQUISITION REPORTS.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.) is further amended by adding at the end the following new section:

"SEC. 840. ACQUISITION REPORTS.

"(a) COMPREHENSIVE ACQUISITION STATUS REPORT.—

"(1) IN GENERAL.—At the same time as the President's budget is submitted for a fiscal year under section 1105(a) of title 31, United States Code, the Under

Secretary for Management shall submit to the congressional homeland security committees an annual comprehensive acquisition status report. The report shall include the following:

"(A) The information required under the heading 'Office of the Under Secretary for Management' under title I of division D of the Consolidated Appropriations Act, 2012 (Public Law 112–74) (as required under the Department of Homeland Security Appropriations Act, 2013 (Public Law 113–6)).

"(B) A listing of programs that have been cancelled, modified, paused, or referred to the Under Secretary for Management or Deputy Secretary for additional oversight or action by the Board, Department Office of Inspector General, or the Comptroller General.

"(C) A listing of established Executive Steering Committees, which provide governance of a program or related set of programs and lower-tiered oversight, and support between acquisition decision events and component reviews, including the mission and membership for each.

"(2) INFORMATION FOR MAJOR ACQUISITION PROGRAMS.—For each major acquisition program, the report shall include the following:

"(A) A narrative description, including current gaps and shortfalls, the capabilities to be fielded, and the number of planned increments or units.

"(B) Acquisition Review Board (or other board designated to review the acquisition) status of each acquisition, including the current acquisition phase, the date of the last review, and a listing of the required documents that have been reviewed with the dates reviewed or approved.

"(C) The most current, approved acquisition program baseline (including project schedules and events).

"(D) A comparison of the original acquisition program baseline, the current acquisition program baseline, and the current estimate.

"(E) Whether or not an independent verification and validation has been implemented, with an explanation for the decision and a summary of any findings.

"(F) A rating of cost risk, schedule risk, and technical risk associated with the program (including narrative descriptions and mitigation actions).

"(G) Contract status (including earned value management data as applicable).

"(H) A lifecycle cost of the acquisition, and time basis for the estimate.

"(3) UPDATES.—The Under Secretary shall submit quarterly updates to such report not later than 45 days after the completion of each quarter.

"(b) QUARTERLY PROGRAM ACCOUNTABILITY REPORT.—The Under Secretary for Management shall prepare a quarterly program accountability report to meet the mandate of the Department to perform program health assessments and improve program execution and governance. The report shall be submitted to the congressional homeland security committees.

"(c) CONGRESSIONAL HOMELAND SECURITY COMMITTEES DEFINED.—In this section, the term 'congressional homeland security committees' means—

"(1) the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate; and

"(2) the Committee on Appropriations of the House of Representatives and the Committee on Appropriations of the Senate.".

(b) LEVEL 3 ACQUISITION PROGRAMS OF COMPONENTS OF THE DEPARTMENT.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, component heads of the Department of Homeland Security shall identify to the Under Secretary for Management of the Department all level 3 acquisition programs of each respective component. Not later than 30 days after receipt of such information, the Under Secretary shall certify in writing to the congressional homeland security committees whether such component heads have properly identified such programs. To carry out this paragraph, the Under Secretary shall establish a process with a repeatable methodology to continually identify level 3 acquisition programs.

(2) POLICIES AND GUIDANCE.—Not later than 180 days after the date of the enactment of this Act, component heads of the Department of Homeland Security shall submit to the Under Secretary for Management of the Department their respective policies and relevant guidance for level 3 acquisition programs of each respective component. Not later than 90 days after receipt of such policies and guidance, the Under Secretary for Management shall certify to the congressional homeland security committees that each component's respective policies and guidance adhere to Department-wide acquisition policies.

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by inserting after the item relating to section 839 the following new item:

"840. Acquisition reports.".

TITLE III—INTELLIGENCE AND INFORMATION SHARING

Subtitle A—Department of Homeland Security Intelligence Enterprise

SEC. 301. HOMELAND INTELLIGENCE DOCTRINE.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following new section:

"SEC. 210G. HOMELAND INTELLIGENCE DOCTRINE.

"(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Secretary, acting through the Chief Intelligence Officer of the Department, in coordination with intelligence components of the Department, the Office of the General Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties, shall develop and disseminate written Department-wide guidance for the processing, analysis, production, and dissemination of homeland security information (as such term is defined in section 892) and terrorism information (as such term is defined in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485)).

"(b) CONTENTS.—The guidance required under subsection (a) shall, at a minimum, include the following:

"(1) A description of guiding principles and purposes of the Department's intelligence enterprise.

"(2) A summary of the roles and responsibilities of each intelligence component of the Department and programs of the intelligence components of the Department in the processing, analysis, production, or dissemination of homeland security information and terrorism information, including relevant authorities and restrictions applicable to each intelligence component of the Department and programs of each such intelligence components.

"(3) Guidance for the processing, analysis, and production of such information.

"(4) Guidance for the dissemination of such information, including within the Department, among and between Federal departments and agencies, among and between State, local, tribal, and territorial governments, including law enforcement, and with foreign partners and the private sector.

"(5) An assessment and description of how the dissemination to the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))) and Federal law enforcement of homeland security information and terrorism information assists such entities in carrying out their respective missions.

"(c) FORM.—The guidance required under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

"(d) ANNUAL REVIEW.—For each of the five fiscal years beginning with the fiscal year that begins after the date of the enactment of this section, the Secretary shall conduct a review of the guidance required under subsection (a) and, as appropriate, revise such guidance.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 210F the following new item:

"Sec. 210G. Homeland intelligence doctrine.".

SEC. 302. ANALYSTS FOR THE CHIEF INTELLIGENCE OFFICER.

Paragraph (1) of section 201(e) of the Homeland Security Act of 2002 (6 U.S.C. 121(e)) is amended by adding at the end the following new sentence: "The Secretary shall also provide the Chief Intelligence Officer with a staff having appropriate expertise and experience to assist the Chief Intelligence Officer.".

SEC. 303. ANNUAL HOMELAND TERRORIST THREAT ASSESSMENTS.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.), as amended by section 301 of this Act, is further amended by adding at the end the following new section:

"SEC. 210H. HOMELAND TERRORIST THREAT ASSESSMENTS.

"(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this section and for each of the next five fiscal years (beginning in the fiscal year that begins after the date of the enactment of this section) the Secretary, acting through the Under Secretary for Intelligence and Analysis, and using departmental information, including component information, and information provided through State and major urban area fusion centers, shall conduct an assessment of the terrorist threat to the homeland.

"(b) CONTENTS.—Each assessment under subsection (a) shall include the following:

"(1) Empirical data assessing terrorist activities and incidents over time in the United States, including terrorist activities and incidents planned or supported by persons outside of the United States targeting the homeland.

"(2) An evaluation of current terrorist tactics, as well as ongoing and possible future changes in terrorist tactics.

"(3) An assessment of criminal activity encountered or observed by officers or employees of components in the field which is suspected of financing terrorist activity.

"(4) Detailed information on all individuals denied entry to or removed from the United States as a result of material support provided to a foreign terrorist organization (as such term is used in section 219 of the Immigration and Nationality Act (8 U.S.C. 1189)).

"(5) The efficacy and spread of foreign terrorist organization propaganda, messaging, or recruitment.

"(6) An assessment of threats, including cyber threats, to the homeland, including to critical infrastructure and Federal civilian networks.

"(7) An assessment of current and potential terrorism and criminal threats posed by individuals and organized groups seeking to unlawfully enter the United States.

"(8) An assessment of threats to the transportation sector, including surface and aviation transportation systems.

"(c) ADDITIONAL INFORMATION.—The assessments required under subsection (a)—

"(1) shall, to the extent practicable, utilize existing component data collected from the field; and

"(2) may incorporate relevant information and analysis from other agencies of the Federal Government, agencies of State and local governments (including law enforcement agencies), as well as the private sector, disseminated in accordance with standard information sharing procedures and policies.

"(d) FORM.—The assessments required under subsection (a) shall be shared with the appropriate congressional committees and submitted in classified form, but—

"(1) shall include unclassified summaries; and

"(2) may include unclassified annexes, if appropriate.".

(b) CONFORMING AMENDMENT.—Subsection (d) of section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121) is amended by adding at the end the following new paragraph:

"(27) To carry out section 210H (relating to homeland terrorist threat assessments).".

(c) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 210G, as added by this Act, the following new item:

"Sec. 210H. Homeland terrorist threat assessments.".

SEC. 304. DEPARTMENT OF HOMELAND SECURITY DATA FRAMEWORK.

(a) IN GENERAL.—The Secretary of Homeland Security shall develop a data framework to integrate existing Department of Homeland Security datasets and systems, as appropriate, for access by authorized personnel in a manner consistent with relevant legal authorities and privacy, civil rights, and civil liberties policies and protections. In developing such framework, the Secretary shall ensure, in accordance with all applicable statutory and regulatory requirements, the following information is included:

(1) All information acquired, held, or obtained by an office or component of the Department that falls within the scope of the information sharing environment, including homeland security information, terrorism information, weapons of mass destruction information, and national intelligence.

(2) Any information or intelligence relevant to priority mission needs and capability requirements of the homeland security enterprise, as determined appropriate by the Secretary.

(b) DATA FRAMEWORK ACCESS.—

(1) IN GENERAL.—The Secretary of Homeland Security shall ensure that the data framework required under this section is accessible to employees of the Department of Homeland Security who the Secretary determines—

(A) have an appropriate security clearance;

(B) are assigned to perform a function that requires access to information in such framework; and

(C) are trained in applicable standards for safeguarding and using such information.

(2) GUIDANCE.—The Secretary of Homeland Security shall—

(A) issue guidance for Department of Homeland Security employees authorized to access and contribute to the data framework pursuant to paragraph (1); and

(B) ensure that such guidance enforces a duty to share between offices and components of the Department when accessing or contributing to such framework for mission needs.

(3) EFFICIENCY.—The Secretary of Homeland Security shall promulgate data standards and instruct components of the Department of Homeland Security to make available information through the data framework under this section in a machine-readable standard format, to the greatest extent practicable.

(c) EXCLUSION OF INFORMATION.—The Secretary of Homeland Security may exclude from the data framework information that the Secretary determines access to or the confirmation of the existence of could—

(1) jeopardize the protection of sources, methods, or activities;

(2) compromise a criminal or national security investigation;

(3) be inconsistent with the other Federal laws or regulations; or

(4) be duplicative or not serve an operational purpose if included in such framework.

(d) SAFEGUARDS.—The Secretary of Homeland Security shall incorporate into the date framework systems capabilities for auditing and ensuring the security of information included in such framework. Such capabilities shall include the following:

(1) Mechanisms for identifying insider threats.

(2) Mechanisms for identifying security risks.

(3) Safeguards for privacy, civil rights, and civil liberties.

(e) DEADLINE FOR IMPLEMENTATION.—Not later than two years after the date of the enactment of this Act, the Secretary of Homeland Security shall ensure the data framework required under this section has the ability to include appropriate information in existence within the Department of Homeland Security to meet its critical mission operations.

(f) NOTICE TO CONGRESS.—

(1) OPERATIONAL NOTIFICATION.—Not later than 60 days after the date on which the data framework required under this section is fully operational, the Secretary of Homeland Security shall provide notice to the appropriate congressional committees of such.

(2) REGULAR STATUS.—The Secretary shall submit to the appropriate congressional committees regular updates on the status of the data framework required under this section, including, when applicable, the use of such data framework to support classified operations.

(g) DEFINITIONS.—In this section:

(1) NATIONAL INTELLIGENCE.—The term "national intelligence" has the meaning given such term in section 3(5) of the National Security Act of 1947 (50 U.S.C. 3003(5)).

(2) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term "appropriate congressional committee" has the meaning given such term in section 2(2) of the Homeland Security Act of 2002 (6 U.S.C. 101(11)).

SEC. 305. ESTABLISHMENT OF INSIDER THREAT PROGRAM.

(a) IN GENERAL.—Title I of the Homeland Security Act of 2002 (6 U.S.C. 111 et seq.) is amended by adding at the end the following new section:

"SEC. 104. INSIDER THREAT PROGRAM.

"(a) ESTABLISHMENT.—The Secretary shall establish an Insider Threat Program within the Department. Such Program shall—

"(1) provide training and education for Department personnel to identify, prevent, mitigate, and respond to insider threat risks to the Department's critical assets;

"(2) provide investigative support regarding potential insider threats that may pose a risk to the Department's critical assets; and

"(3) conduct risk mitigation activities for insider threats.

"(b) STEERING COMMITTEE.—

"(1) IN GENERAL.—The Secretary shall establish a Steering Committee within the Department. The Under Secretary for Intelligence and Analysis shall serve as the Chair of the Steering Committee. The Chief Security Officer shall serve as the Vice Chair. The Steering Committee shall be comprised of representatives of the Office of Intelligence and Analysis, the Office of the Chief Information Officer, the Office of the General Counsel, the Office for Civil Rights and Civil Liberties, the Privacy Office, the Office of the Chief Human Capital Officer, the Office of the Chief Financial Officer, the Federal Protective Service, the Office of the Chief Procurement Officer, the Science and Technology Directorate, and other components or offices of the Department as appropriate. Such representatives shall meet on a regular basis to discuss cases and issues related to insider threats to the Department's critical assets, in accordance with subsection (a).

"(2) RESPONSIBILITIES.—Not later than one year after the date of the enactment of this section, the Under Secretary for Intelligence and Analysis and the Chief Security Officer, in coordination with the Steering Committee established pursuant to paragraph (1), shall—

"(A) develop a holistic strategy for Department-wide efforts to identify, prevent, mitigate, and respond to insider threats to the Department's critical assets;

"(B) develop a plan to implement the insider threat measures identified in the strategy developed under subparagraph (A) across the components and offices of the Department;

"(C) document insider threat policies and controls;

"(D) conduct a baseline risk assessment of insider threats posed to the Department's critical assets;

"(E) examine existing programmatic and technology best practices adopted by the Federal Government, industry, and research institutions to implement solutions that are validated and cost-effective;

"(F) develop a timeline for deploying workplace monitoring technologies, employee awareness campaigns, and education and training programs related to identifying, preventing, mitigating, and responding to potential insider threats to the Department's critical assets;

"(G) require the Chair and Vice Chair of the Steering Committee to consult with the Under Secretary for Science and Technology and other appropriate stakeholders to ensure the Insider Threat Program is informed, on an ongoing basis, by current information regarding threats, beset practices, and available technology; and

"(H) develop, collect, and report metrics on the effectiveness of the Department's insider threat mitigation efforts.

"(c) DEFINITIONS.—In this section:

"(1) CRITICAL ASSETS.—The term 'critical assets' means the people, facilities, information, and technology required for the Department to fulfill its mission.

"(2) INSIDER.—The term 'insider' means—

"(A) any person who has access to classified national security information and is employed by, detailed to, or assigned to the Department, including members of the Armed Forces, experts or consultants to the Department, industrial or commercial contractors, licensees, certificate holders, or grantees of the Department, including all subcontractors, personal services contractors, or any other category of person who acts for or on behalf of the Department, as determined by the Secretary; or

"(B) State, local, tribal, territorial, and private sector personnel who possess security clearances granted by the Department.

"(3) INSIDER THREAT.—The term 'insider threat' means the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States, including damage to the United States through espionage, terrorism, the unauthorized disclosure of classified national security information, or through the loss or degradation of departmental resources or capabilities.".

(b) REPORTING.—

(1) IN GENERAL.—Not later than two years after the date of the enactment of section 104 of the Homeland Security Act of 2002 (as added by subsection (a) of this section) and the biennially thereafter for the next four years, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate a report on how the Department of Homeland Security and its components and offices have implemented the strategy developed pursuant to subsection (b)(2)(A) of such sec-

tion 104, the status of the Department's risk assessment of critical assets, the types of insider threat training conducted, the number of Department employees who have received such training, and information on the effectiveness of the Insider Threat Program (established pursuant to subsection (a) of such section 104), based on metrics developed, collected, and reported pursuant to subsection (b)(2)(H) of such section 104.

(2) DEFINITIONS.—In this subsection, the terms "critical assets", "insider", and "insider threat" have the meanings given such terms in section 104 of the Homeland Security Act of 2002 (as added by subsection (a) of this section).

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 103 the following new item:

"Sec. 104. Insider Threat Program.".

SEC. 306. THREAT ASSESSMENT ON TERRORIST USE OF VIRTUAL CURRENCY.

(a) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Under Secretary of Homeland Security for Intelligence and Analysis, as authorized by section 201(b)(1) of the Homeland Security Act of 2002 (6 U.S.C. 121), shall, in coordination with appropriate Federal partners, develop and disseminate a threat assessment regarding the actual and potential threat posed by individuals using virtual currency to carry out activities in furtherance of an act of terrorism, including the provision of material support or resources to a foreign terrorist organization. Consistent with the protection of classified and confidential unclassified information, the Under Secretary shall share the threat assessment developed under this section with State, local, and tribal law enforcement officials, including officials that operate within State, local, and regional fusion centers through the Department of Homeland Security State, Local, and Regional Fusion Center Initiative established in section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h).

(b) DEFINITIONS.—In this section:

(1) FOREIGN TERRORIST ORGANIZATION.—The term "foreign terrorist organization" means an organization designated as a foreign terrorist organization under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189).

(2) VIRTUAL CURRENCY.—The term "virtual currency" means a digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

SEC. 307. DEPARTMENT OF HOMELAND SECURITY COUNTERTERRORISM ADVISORY BOARD.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.), as amended by sections 301 and 303 of this Act, is further amended by adding at the end the following new section:

"SEC. 210I. DEPARTMENTAL COORDINATION ON COUNTERTERRORISM.

"(a) ESTABLISHMENT.—There is in the Department a board to be composed of senior representatives of departmental operational components and headquarters elements. The purpose of the board shall be to coordinate and integrate departmental intelligence, activities, and policy related to the counterterrorism mission and functions of the Department.

"(b) CHARTER.—There shall be a charter to govern the structure and mission of the board. Such charter shall direct the board to focus on the current threat environment and the importance of aligning departmental counterterrorism activities under the Secretary's guidance. The charter shall be reviewed and updated every four years, as appropriate.

"(c) MEMBERS.—

"(1) CHAIR.—The Secretary shall appoint a Coordinator for Counterterrorism within the Department who will serve as the chair of the board.

"(2) ADDITIONAL MEMBERS.—The Secretary shall appoint additional members of the board from among the following:

"(A) The Transportation Security Administration.
"(B) U.S. Customs and Border Protection.
"(C) U.S. Immigration and Customs Enforcement.
"(D) The Federal Emergency Management Agency.
"(E) The Coast Guard.
"(F) United States Citizenship and Immigration Services.
"(G) The United States Secret Service.
"(H) The National Protection and Programs Directorate.
"(I) The Office of Operations Coordination.
"(J) The Office of the General Counsel.
"(K) The Office of Intelligence and Analysis.
"(L) The Office of Policy.
"(M) The Science and Technology Directorate.

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

"(d) MEETINGS.—The board shall 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 shall make recommendations to the Secretary.

"(e) TERRORISM ALERTS.—The board shall advise the Secretary on the issuance of terrorism alerts pursuant to section 203 of this Act.

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

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 210H, as added by this Act, the following new item:

"Sec. 210I. Departmental coordination on counterterrorism.".

(c) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Coordinator for Counterterrorism, shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the status and activities of the board established under section 210I of the Homeland Security Act of 2002, as added by subsection (a) of this section.

SEC. 308. BORDER AND GANG THREAT ASSESSMENT.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall conduct a threat assessment on whether human smuggling organizations and transnational gangs are exploiting vulnerabilities in border security screening programs to gain access to the United States and threaten the United States or border security.

(b) RECOMMENDATIONS.—Upon completion of the threat assessment required under subsection (a), the Secretary of Homeland Security shall make a determination if any changes are required to address security vulnerabilities identified in such assessment.

SEC. 309. SECURITY CLEARANCE MANAGEMENT AND ADMINISTRATION.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 is amended—

(1) by inserting before section 701 (6 U.S.C. 341) the following:

"Subtitle A—Headquarters Activities";

and

(2) by adding at the end the following new subtitle:

"Subtitle B—Security Clearances

"SEC. 731. DESIGNATION OF NATIONAL SECURITY SENSITIVE AND PUBLIC TRUST POSITIONS.

"(a) IN GENERAL.—The Secretary shall require the designation of the sensitivity level of national security positions (pursuant to part 1400 of title 5, Code of Federal Regulations, or similar successor regulation) be conducted in a consistent manner with respect to all components and offices of the Department, and consistent with Federal guidelines.

"(b) IMPLEMENTATION.—In carrying out subsection (a), the Secretary shall require the utilization of uniform designation tools throughout the Department and provide training to appropriate staff of the Department on such utilization. Such training shall include guidance on factors for determining eligibility for access to classified information and eligibility to hold a national security position.

"SEC. 732. REVIEW OF POSITION DESIGNATIONS.

"(a) IN GENERAL.—Not later than one year after the date of the enactment of this subtitle, and every five years thereafter, the Secretary shall review all sensitivity level designations of national security positions (pursuant to part 1400 of title 5, Code of Federal Regulations, or similar successor regulation) at the Department.

"(b) DETERMINATION.—If during the course of a review required under subsection (a), the Secretary determines that a change in the sensitivity level of a position that affects the need for an individual to obtain access to classified information is warranted, such access shall be administratively adjusted and an appropriate level periodic reinvestigation completed, as necessary.

"(c) CONGRESSIONAL REPORTING.—Upon completion of each review required under subsection (a), the Secretary shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on the findings of each such review, including the number of positions by classification level and by component and office of the Department in which the Secretary made a determination in accordance with subsection (b) to—

"(1) require access to classified information;

"(2) no longer require access to classified information; or

"(3) otherwise require a different level of access to classified information.

"SEC. 733. AUDITS.

"Beginning not later than 180 days after the date of the enactment of this section, the Inspector General of the Department shall conduct regular audits of compliance of the Department with part 1400 of title 5, Code of Federal Regulations, or similar successor regulation.

"SEC. 734. REPORTING.

"(a) IN GENERAL.—The Secretary shall annually through fiscal year 2022 submit to the Committee on Homeland Security and the Committee on Oversight and Government Reform of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the following:

"(1) The number of denials, suspensions, revocations, and appeals of the eligibility for access to classified information of an individual throughout the Department.

"(2) The date and status or disposition of each reported action under paragraph (1).

"(3) The identification of the sponsoring entity, whether by a component, office, or headquarters of the Department, of each action under paragraph (1), and description of the grounds for each such action.

"(4) Demographic data, including data relating to race, sex, national origin, and disability, of each individual for whom eligibility for access to classified information was denied, suspended, revoked, or appealed, and the number of years that each such individual was eligible for access to such information.

"(5) In the case of a suspension in excess of 180 days, an explanation for such duration.

"(b) FORM.—The report required under subsection (a) shall be submitted in unclassified form and be made publicly available, but may include a classified annex for any sensitive or classified information if necessary.

"SEC. 735. UNIFORM ADJUDICATION, SUSPENSION, DENIAL, AND REVOCATION.

"Not later than one year after the date of the enactment of this section, the Secretary, in consultation with the Homeland Security Advisory Committee, shall develop a plan to achieve greater uniformity within the Department with respect to the adjudication of eligibility of an individual for access to classified information that are consistent with the Adjudicative Guidelines for Determining Access to Classified Information published on December 29, 2005, or similar successor regulation. 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 the plan. The plan shall consider the following:

"(1) Mechanisms to foster greater compliance with the uniform Department adjudication, suspension, denial, and revocation standards by the head of each component and office of the Department with the authority to adjudicate access to classified information.

"(2) The establishment of an internal appeals panel responsible for final national security clearance denial and revocation determinations that is comprised of designees who are career, supervisory employees from components and offices of the Department with the authority to adjudicate access to classified information and headquarters, as appropriate.

"SEC. 736. DATA PROTECTION.

"The Secretary shall ensure that all information received for the adjudication of eligibility of an individual for access to classified information is consistent with the Adjudicative Guidelines for Determining Access to Classified Information published on December 29, 2005, or similar successor regulation, and is protected against misappropriation.

"SEC. 737. REFERENCE.

"Except as otherwise provided, for purposes of this subtitle, any reference to the 'Department' includes all components and offices of the Department.".

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended—

(1) by inserting before the item relating to section 701 the following new item:

"Subtitle A—Headquarters Activities";

and

(2) by inserting after the final item relating to title VII the following new items:

"Subtitle B—Security Clearances

"Sec. 731. Designation of national security sensitive and public trust positions.
"Sec. 732. Review of position designations.
"Sec. 733. Audits.
"Sec. 734. Reporting.
"Sec. 735. Uniform adjudication, suspension, denial, and revocation.
"Sec. 736. Data protection.
"Sec. 737. Reference.".

Subtitle B—Stakeholder Information Sharing

SEC. 311. DEPARTMENT OF HOMELAND SECURITY FUSION CENTER PARTNERSHIP INITIATIVE.

(a) IN GENERAL.—Section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h) is amended—

(1) by amending the section heading to read as follows:

"SEC. 210A. DEPARTMENT OF HOMELAND SECURITY FUSION CENTER PARTNERSHIP INITIATIVE.";

(2) in subsection (a), by adding at the end the following new sentence: "Beginning on the date of the enactment of the Department of Homeland Security Authorization Act of 2017, such Initiative shall be known as the 'Department of Homeland Security Fusion Center Partnership Initiative'.";

(3) by amending subsection (b) to read as follows:

"(b) INTERAGENCY SUPPORT AND COORDINATION.—Through the Department of Homeland Security Fusion Center Partnership Initiative, in coordination with principal officials of fusion centers in the National Network of Fusion Centers and the officers designated as the Homeland Security Advisors of the States, the Secretary shall—

"(1) coordinate with the heads of other Federal departments and agencies to provide operational and intelligence advice and assistance to the National Network of Fusion Centers;

"(2)(A) support the integration of fusion centers into the information sharing environment;

"(B) conduct outreach to such fusion centers to identify any gaps in information sharing; and

"(C) consult with other Federal agencies to develop methods to address any such gaps, as appropriate;

"(3)(A) identify Federal databases and datasets, including databases and datasets used, operated, or managed by Department components, the Federal Bureau of Investigation, and the Department of the Treasury, that are appropriate, in accordance with Federal laws and policies, to address any gaps identified pursuant to paragraph (2), for inclusion in the information sharing environment; and

"(B) coordinate with the appropriate Federal agency to deploy or access such databases and datasets;

"(4) support the maturation and sustainment of the National Network of Fusion Centers;

"(5) reduce inefficiencies and maximize the effectiveness of Federal resource support to the National Network of Fusion Centers;

"(6) provide analytic and reporting advice and assistance to the National Network of Fusion Centers;

"(7) 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 the National Network of Fusion Centers and incorporate such information, as appropriate, into the Department's own such information;

"(8) provide for the effective dissemination of information within the scope of the information sharing environment to the National Network of Fusion Centers;

"(9) facilitate close communication and coordination between the National Network of Fusion Centers and the Department and other Federal departments and agencies;

"(10) provide the National Network of Fusion Centers with expertise on Department resources and operations;

"(11) coordinate the provision of training and technical assistance to the National Network of Fusion Centers and encourage participating fusion centers to take part in terrorism threat-related exercises conducted by the Department;

"(12) ensure, to the greatest extent practicable, that support for the National Network of Fusion Centers is included as a national priority in applicable homeland security grant guidance;

"(13) ensure that each fusion center in the National Network of Fusion Centers has a privacy policy approved by the Chief Privacy Officer of the Department and a civil rights and civil liberties policy approved by the Officer for Civil Rights and Civil Liberties of the Department;

"(14) coordinate the nationwide suspicious activity report initiative to ensure information gathered by the National Network of Fusion Centers is incorporated as appropriate;

"(15) promote and facilitate, to the greatest extent practicable, nationwide suspicious activity report training of fire, emergency medical services, emergency management, and public heath personnel;

"(16) lead Department efforts to ensure fusion centers in the National Network of Fusion Centers are the primary focal points for the sharing of homeland security information, terrorism information, and weapons of mass destruction information with State, local, tribal, and territorial entities to the greatest extent practicable;

"(17) develop and disseminate best practices on the appropriate levels for staffing at fusion centers in the National Network of Fusion Centers of qualified representatives from State, local, tribal, and territorial law enforcement, fire, emergency medical, and emergency management services, and public health disciplines, as well as the private sector; and

"(18) carry out such other duties as the Secretary determines appropriate.";

(4) in subsection (c)—

(A) by striking so much as precedes paragraph (3)(B) and inserting the following:

"(c) RESOURCE ALLOCATION.—

"(1) INFORMATION SHARING AND PERSONNEL ASSIGNMENT.—

"(A) INFORMATION SHARING.—The Under Secretary for Intelligence and Analysis shall ensure that, as appropriate—

"(i) fusion centers in the National Network of Fusion Centers have access to homeland security information sharing systems; and

"(ii) Department personnel are deployed to support fusion centers in the National Network of Fusion Centers in a manner consistent with the Department's mission and existing statutory limits.

"(B) PERSONNEL ASSIGNMENT.—Department personnel referred to in subparagraph (A)(ii) may include the following:

"(i) Intelligence officers.

"(ii) Intelligence analysts.

"(iii) Other liaisons from components and offices of the Department, as appropriate.

"(C) MEMORANDA OF UNDERSTANDING.—The Under Secretary for Intelligence and Analysis shall negotiate memoranda of understanding between the Department and a State or local government, in coordination with the appropriate representatives from fusion centers in the National Network of Fusion Centers, regarding the exchange of information between the Department and such fusion centers. Such memoranda shall include the following:

"(i) The categories of information to be provided by each entity to the other entity that are parties to any such memoranda.

"(ii) The contemplated uses of the exchanged information that is the subject of any such memoranda.

"(iii) The procedures for developing joint products.

"(iv) The information sharing dispute resolution processes.

"(v) Any protections necessary to ensure the exchange of information accords with applicable law and policies.

"(2) SOURCES OF SUPPORT.—

"(A) IN GENERAL.—Information shared and personnel assigned pursuant to paragraph (1) may be shared or provided, as the case may be, by the following Department components and offices, in coordination with the respec-

tive component or office head and in consultation with the principal officials of fusion centers in the National Network of Fusion Centers:

"(i) The Office of Intelligence and Analysis.

"(ii) The Office of Infrastructure Protection.

"(iii) The Transportation Security Administration.

"(iv) U.S. Customs and Border Protection.

"(v) U.S. Immigration and Customs Enforcement.

"(vi) The Coast Guard.

"(vii) The national cybersecurity and communications integration center under section 227.

"(viii) Other components or offices of the Department, as determined by the Secretary.

"(B) COORDINATION WITH OTHER FEDERAL AGENCIES.—The Under Secretary for Intelligence and Analysis shall coordinate with appropriate officials throughout the Federal Government to ensure the deployment to fusion centers in the National Network of Fusion Centers of representatives with relevant expertise of other Federal departments and agencies.

"(3) RESOURCE ALLOCATION CRITERIA.—

"(A) IN GENERAL.—The Secretary shall make available criteria for sharing information and deploying personnel to support a fusion center in the National Network of Fusion Centers in a manner consistent with the Department's mission and existing statutory limits."; and

(B) in paragraph (4)(B), in the matter preceding clause (i), by inserting "in which such fusion center is located" after "region";

(5) in subsection (d)—

(A) in paragraph (3), by striking "and" at the end;

(B) in paragraph (4)—

(i) by striking "government" and inserting "governments"; and

(ii) by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following new paragraph:

"(5) utilize Department information, including information held by components and offices, to develop analysis focused on the mission of the Department under section 101(b).";

(6) in subsection (e)—

(A) by amending paragraph (1) to read as follows:

"(1) IN GENERAL.—To the greatest extent practicable, the Secretary shall make it a priority to allocate resources, including deployed personnel, under this section from U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Coast Guard to support fusion centers in the National Network of 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, tribal, and territorial law enforcement authorities to identify, investigate, and otherwise interdict persons, weapons, and related contraband that pose a threat to homeland security."; and

(B) in paragraph (2), in the matter preceding subparagraph (A), by striking "participating State, local, and regional fusion centers" and inserting "fusion centers in the National Network of Fusion Centers";

(7) in subsection (j)—

(A) in paragraph (4), by striking "and" at the end;

(B) by redesignating paragraph (5) as paragraph (6); and

(C) by inserting after paragraph (4) the following new paragraph:

"(5) the term 'National Network of Fusion Centers' means a decentralized arrangement of fusion centers intended to enhance individual State and urban area fusion centers' ability to leverage the capabilities and expertise of all fusion centers for the purpose of enhancing analysis and homeland security information sharing nationally; and"; and

(8) by striking subsection (k).

(b) ACCOUNTABILITY REPORT.—Not later than one year after the date of the enactment of this Act and annually thereafter through 2024, the Under Secretary for Intelligence and Analysis of the Department of Homeland Security shall report 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 on the efforts of the Office of Intelligence and Analysis of the Department and other relevant components and offices of the Department to enhance support provided to fusion centers in the National Network of Fusion Centers, including meeting the requirements specified in section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h), as amended by subsection (a) of this section.

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the item relating to section 210A and inserting the following new item:

"Sec. 210A. Department of Homeland Security Fusion Center Partnership Initiative.".

(d) REFERENCE.—Any reference in any law, rule, or regulation to the "Department of Homeland Security State, Local, and Regional Fusion Center Initiative" shall be deemed to be a reference to the "Department of Homeland Security Fusion Center Partnership Initiative".

SEC. 312. FUSION CENTER PERSONNEL NEEDS ASSESSMENT.

(a) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Comptroller General of the United States shall conduct an assessment of Department of Homeland Security personnel assigned to fusion centers pursuant to subsection (c) of section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h), as amended by section 311 of this Act, including an assessment of whether deploying additional Department personnel to such fusion centers would enhance the Department's mission under section 101(b) of such Act and the National Network of Fusion Centers. The assessment required under this subsection shall include the following:

(1) Information on the current deployment of the Department's personnel to each fusion center.

(2) Information on the roles and responsibilities of the Department's Office of Intelligence and Analysis intelligence officers, intelligence analysts, senior reports officers, reports officers, and regional directors deployed to fusion centers.

(3) Information on Federal resources, in addition to personnel, provided to each fusion center.

(4) An analysis of the optimal number of personnel the Office of Intelligence and Analysis should deploy to fusion centers, including a cost-benefit analysis comparing deployed personnel with technological solutions to support information sharing.

(5) An assessment of fusion centers located in jurisdictions along land and maritime borders of the United States, and the degree to which deploying personnel, as appropriate, from U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Coast Guard to such fusion centers would enhance the integrity and security at such borders by helping Federal, State, local, tribal, and territorial law enforcement authorities to identify, investigate, and interdict persons, weapons, and related contraband that pose a threat to homeland security.

(6) An assessment of fusion centers located in jurisdictions with large and medium hub airports, and the degree to which deploying, as appropriate, personnel from the Transportation Security Administration to such fusion centers would enhance the integrity and security of aviation security.

(b) DEFINITIONS.—In this section:

(1) FUSION CENTER.—The term "fusion center" has the meaning given such term in subsection (j) of section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h).

(2) NATIONAL NETWORK OF FUSION CENTERS.—The term "National Network of Fusion Centers" has the meaning given such term in subsection (j) of section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h), as amended by section 311 of this Act.

SEC. 313. PROGRAM FOR STATE AND LOCAL ANALYST CLEARANCES.

(a) SENSE OF CONGRESS.—It is the sense of Congress that any program established by the Under Secretary for Intelligence and Analysis of the Department of Homeland Security to provide eligibility for access to information classified as Top Secret for State, local, tribal, and territorial analysts located in fusion centers shall be consistent with the need to know requirements pursuant to Executive Order No. 13526 (50 U.S.C. 3161 note).

(b) REPORT.—Not later than two years after the date of the enactment of this Act, the Under Secretary of Intelligence and Analysis of the Department of Homeland Security, in consultation with the Director of National Intelligence, shall submit to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate a report on the following:

(1) The process by which the Under Secretary of Intelligence and Analysis determines a need to know pursuant to Executive Order No. 13526 to sponsor Top Secret clearances for appropriate State, local, tribal, and territorial analysts located in fusion centers.

(2) The effects of such Top Secret clearances on enhancing information sharing with State, local, tribal, and territorial partners.

(3) The cost for providing such Top Secret clearances for State, local, tribal, and territorial analysts located in fusion centers, including training and background investigations.

(4) The operational security protocols, training, management, and risks associated with providing such Top Secret clearances for State, local, tribal, and territorial analysts located in fusion centers.

(c) DEFINITION.—In this section, the term "fusion center" has the meaning given such term in subsection (j) of section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h).

SEC. 314. INFORMATION TECHNOLOGY ASSESSMENT.

(a) IN GENERAL.—The Under Secretary of Intelligence and Analysis of the Department of Homeland Security, in collaboration with the Chief Information Officer of the Department and representatives from the National Network of Fusion Centers, shall conduct an assessment of information systems (as such term is defined in section 3502 of title 44, United States Code) used to share homeland security information between the Department and fusion centers in the National Network of Fusion Centers and make upgrades to such systems, as appropriate. Such assessment shall include the following:

(1) An evaluation of the accessibility and ease of use of such systems by fusion centers in the National Network of Fusion Centers.

(2) A review to determine how to establish improved interoperability of departmental information systems with existing information systems used by fusion centers in the National Network of Fusion Centers.

(3) An evaluation of participation levels of departmental components and offices of information systems used to share homeland security information with fusion centers in the National Network of Fusion Centers.

(b) DEFINITIONS.—In this section:

(1) FUSION CENTER.—The term "fusion center" has the meaning given such term in subsection (j) of section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h).

(2) NATIONAL NETWORK OF FUSION CENTERS.—The term "National Network of Fusion Centers" has the meaning given such term in subsection (j) of section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h), as amended by section 311 of this Act.

SEC. 315. DEPARTMENT OF HOMELAND SECURITY CLASSIFIED FACILITY INVENTORY AND DISSEMINATION.

(a) IN GENERAL.—The Secretary of Homeland Security shall, to the extent practicable—

(1) maintain an inventory of those Department of Homeland Security facilities that the Department certifies to house classified infrastructure or systems at the secret level and above;

(2) update such inventory on a regular basis; and

(3) share part or all of such inventory with—

(A) Department personnel who have been granted the appropriate security clearance;

(B) non-Federal governmental personnel who have been granted a Top Secret security clearance; and

(C) other personnel as determined appropriate by the Secretary.

(b) INVENTORY.—The inventory of facilities described in subsection (a) may include—

(1) the location of such facilities;

(2) the attributes of such facilities (including the square footage of, the total capacity of, the number of workstations in, and the number of conference rooms in, such facilities);

(3) the entities that operate such facilities; and

(4) the date of establishment of such facilities.

SEC. 316. TERROR INMATE INFORMATION SHARING.

(a) IN GENERAL.—The Secretary of Homeland Security, in coordination with the Attorney General and in consultation with other appropriate Federal officials, shall, as appropriate, share with State, local, and regional fusion centers through the Department of Homeland Security Fusion Center Partnership Initiative under section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h), as amended by section 311 of this Act, as well as other relevant law enforcement entities, release information from a Federal correctional facility, including the name, charging date, and ex-

pected place and date of release, of certain individuals who may pose a terrorist threat.

(b) SCOPE.—The information shared pursuant to subsection (a) shall be—

(1) for homeland security purposes; and

(2) regarding individuals convicted of a Federal crime of terrorism (as such term is defined in section 2332b of title 18, United States Code).

(c) PERIODIC THREAT ASSESSMENTS.—Consistent with the protection of classified information and controlled unclassified information, the Secretary of Homeland Security shall coordinate with appropriate Federal officials to provide State, local, and regional fusion centers described in subsection (a) with periodic assessments regarding the overall threat from known or suspected terrorists currently incarcerated in a Federal correctional facility, including the assessed risks of such populations engaging in terrorist activity upon release.

(d) PRIVACY PROTECTIONS.—Prior to affecting the information sharing described in subsection (a), the Secretary shall receive input and advice from the Officer for Civil Rights and Civil Liberties, the Officer for Privacy and the Chief Intelligence Officer of the Department.

(e) RULE OF CONSTRUCTION.—Nothing in this section may be construed as requiring the establishment of a list or registry of individuals convicted of terrorism.

SEC. 317. ANNUAL REPORT ON OFFICE FOR STATE AND LOCAL LAW ENFORCEMENT.

Subsection (b) of section 2006 of the Homeland Security Act of 2002 (6 U.S.C. 607) is amended—

(1) by redesignating paragraph (5) as paragraph (6); and

(2) by inserting after paragraph (4) the following new paragraph:

"(5) ANNUAL REPORT.—For each of fiscal years 2018 through 2022, the Assistant Secretary for State and Local Law Enforcement 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 activities of the Office for State and Local Law Enforcement. Each such report shall include, for the fiscal year covered by the report, a description of each of the following:

"(A) Efforts to coordinate and share information regarding Department and component agency programs with State, local, and tribal law enforcement agencies.

"(B) Efforts to improve information sharing through the Homeland Security Information Network by appropriate component agencies of the Department and by State, local, and tribal law enforcement agencies.

"(C) The status of performance metrics within the Office of State and Local Law Enforcement to evaluate the effectiveness of efforts to carry out responsibilities set forth within the subsection.

"(D) Any feedback from State, local, and tribal law enforcement agencies about the Office, including the mechanisms utilized to collect such feedback.

"(E) Efforts to carry out all other responsibilities of the Office of State and Local Law Enforcement.".

SEC. 318. ANNUAL CATALOG ON DEPARTMENT OF HOMELAND SECURITY TRAINING, PUBLICATIONS, PROGRAMS, AND SERVICES FOR STATE, LOCAL, AND TRIBAL LAW ENFORCEMENT AGENCIES.

Paragraph (4) of section 2006(b) of the Homeland Security Act of 2002 (6 U.S.C. 607(b)) is amended—

(1) in subparagraph (E), by striking "and" at the end;

(2) in subparagraph (F), by striking the period and inserting a semicolon; and

(3) by adding at the end the following new subparagraphs:

"(G) produce an annual catalog that summarizes opportunities for training, publications, programs, and services available to State, local, and tribal law enforcement agencies from the Department and from each component and office within the Department and, not later than 30 days after the date of such production, disseminate the catalog, including by—

"(i) making such catalog available to State, local, and tribal law enforcement agencies, including by posting the catalog on the website of the Department and cooperating with national organizations that represent such agencies;

"(ii) making such catalog available through the Homeland Security Information Network; and

"(iii) submitting such catalog to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate; and

"(H) in coordination with appropriate components and offices of the Department and other Federal agencies, develop, maintain, and make avail-

able information on Federal resources intended to support fusion center access to Federal information and resources.".

TITLE IV—MARITIME SECURITY

SEC. 401. STRATEGIC PLAN TO ENHANCE THE SECURITY OF THE INTERNATIONAL SUPPLY CHAIN.

Paragraph (2) of section 201(g) of the Security and Accountability for Every Port Act of 2006 (6 U.S.C. 941(g)) is amended to read as follows:

"(2) UPDATES.—Not later than 270 days after the date of the enactment of this paragraph and every three years thereafter, the Secretary shall submit to the appropriate congressional committees a report that contains an update of the strategic plan required by subsection (a).".

SEC. 402. CONTAINER SECURITY INITIATIVE.

Subsection (l) of section 205 of the Security and Accountability for Every Port Act of 2006 (6 U.S.C. 945) is amended—

(1) by striking "(1) IN GENERAL.—Not later than September 30, 2007," and inserting "Not later than 270 days after the date of the enactment of the Border and Maritime Security Coordination Improvement Act,";

(2) by redesignating subparagraphs (A) through (H) as paragraphs (1) through (8), respectively, and by moving the margins of such paragraphs (as so redesignated) two ems to the left; and

(3) by striking paragraph (2).

SEC. 403. CYBER AT PORTS.

(a) CYBERSECURITY ENHANCEMENTS TO MARITIME SECURITY ACTIVITIES.—Subparagraph (B) of section 70112(a)(2) of title 46, United States Code, is amended—

(1) by redesignating clauses (i) through (iii) as clauses (ii) and (iv), respectively; and

(2) by inserting before clause (ii) the following new clause:

"(i) shall facilitate the sharing of information relating to cybersecurity risks and incidents (as such terms are defined in section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)) to address port-specific cybersecurity risks and incidents, which may include the establishment of a working group of members of such committees to address such port-specific cybersecurity risks and incidents;".

(b) VULNERABILITY ASSESSMENTS AND SECURITY PLANS.—Title 46, United States Code, is amended—

(1) in subparagraph (C) of section 70102(b)(1), by inserting "cybersecurity," after "physical security,"; and

(2) in subparagraph (C) of section 70103(c)(3)—

(A) in clause (i), by inserting "cybersecurity," after "physical security,";

(B) in clause (iv), by striking "and" after the semicolon at the end;

(C) by redesignating clause (v) as clause (vi); and

(D) by inserting after clause (iv) the following new clause:

"(v) prevention, management, and response to cybersecurity risks and incidents (as such terms are defined in section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)); and".

SEC. 404. FACILITY INSPECTION INTERVALS.

Subparagraph (D) of section 70103(c)(4) of title 46, United States Code, is amended to read as follows:

"(D) subject to the availability of appropriations, verify the effectiveness of each such facility security plan periodically, but not less than one time per year without notice, and more frequently as determined necessary, in a risk based manner, with or without notice to the facility.".

SEC. 405. UPDATES OF MARITIME OPERATIONS COORDINATION PLAN.

(a) IN GENERAL.—Subtitle C of title IV of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.) is amended by adding at the end the following new section:

"SEC. 434. UPDATES OF MARITIME OPERATIONS COORDINATION PLAN.

"Not later than 180 days after the date of the enactment of this section and biennially thereafter, the Secretary 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 of the Senate a maritime operations coordination plan for the coordination and cooperation of maritime operations undertaken by components and offices of the Department with responsibility for maritime security missions. Such plan shall update

the maritime operations coordination plan released by the Department in July 2011, and shall address the following:

"(1) Coordination of 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 homeland 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) Cooperation and coordination with other departments and agencies of the Federal Government, and State and local agencies, in the maritime environment, in support of maritime homeland security missions.

"(4) Work conducted within the context of other national and Department maritime security strategic guidance.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by adding after the item relating to section 433 the following new item:

"Sec. 434. Updates of maritime operations coordination plan.".

SEC. 406. EVALUATION OF COAST GUARD DEPLOYABLE SPECIALIZED FORCES.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, 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 a report that describes and assesses the state of the Coast Guard's Deployable Specialized Forces (in this section referred to as the "DSF"). Such report shall include, at a minimum, the following elements:

(1) For each of the past three fiscal years, and for each type of DSF, the following:

(A) A cost analysis, including training, operating, and travel costs.

(B) The number of personnel assigned.

(C) The total number of units.

(D) The total number of operations conducted.

(E) The number of operations requested by each of the following:

(i) The Coast Guard.

(ii) Other components or offices of the Department of Homeland Security.

(iii) Other Federal departments or agencies.

(iv) State agencies.

(v) Local agencies.

(F) The number of operations fulfilled by the entities specified in subparagraph (E).

(2) An examination of alternative distributions of DSFs, including the feasibility, cost (including cost savings), and impact on mission capability of such distributions, including at a minimum the following:

(A) Combining DSFs, primarily focused on counterdrug operations, under one centralized command.

(B) Distributing counter-terrorism and anti-terrorism capabilities to DSFs in each major United States port.

(b) DEPLOYABLE SPECIALIZED FORCE DEFINED.—In this section, the term "Deployable Specialized Force" means a unit of the Coast Guard that serves as a quick reaction force designed to be deployed to handle counter-drug, counter-terrorism, and anti-terrorism operations or other maritime threats to the United States.

SEC. 407. COST BENEFIT ANALYSIS OF CO-LOCATING DHS ASSETS.

(a) IN GENERAL.—For any location in which U.S. Customs and Border Protection's Office of Air and Marine Operations is based within 45 miles of locations where any other Department of Homeland Security agency also operates air and marine assets, the Secretary of Homeland Security shall conduct a cost-benefit analysis to consider the potential cost of and savings derived from co-locating aviation and maritime operational assets of the Office of Air and Marine Operations at facilities where other agencies of the Department operate such assets. In analyzing such potential cost savings achieved by sharing aviation and maritime facilities, such analysis shall consider, at a minimum, the following factors:

(1) Potential enhanced cooperation derived from Department personnel being co-located.

(2) Potential costs of, and savings derived through, shared maintenance and logistics facilities and activities.

(3) Joint use of base and facility infrastructure, such as runways, hangars, control towers, operations centers, piers and docks, boathouses, and fuel depots.

(4) Potential operational costs of co-locating aviation and maritime assets and personnel.

(5) Short term moving costs required in order to co-locate facilities.

(6) Acquisition and infrastructure costs for enlarging current facilities, as needed.

(b) REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security 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 of the Senate a report summarizing the results of the cost-benefit analysis required under subsection (a) and any planned actions based upon such results.

SEC. 408. REPEAL OF INTERAGENCY OPERATIONAL CENTERS FOR PORT SECURITY AND SECURE SYSTEMS OF TRANSPORTATION.

Sections 70107A and 70116 of title 46, United States Code, are repealed.

SEC. 409. MARITIME SECURITY CAPABILITIES ASSESSMENTS.

(a) IN GENERAL.—Subtitle C of title IV of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.), as amended by section 405 of this Act, is further amended by adding at the end the following new section:

"SEC. 435. MARITIME SECURITY CAPABILITIES ASSESSMENTS.

"Not later than 180 days after the date of the enactment of this section 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 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; Public Law 114–328).".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002, as amended by section 405 of this Act, is further amended by inserting after the item relating to section 434 the following new item:

"Sec. 435. Maritime security capabilities assessments.".

SEC. 410. CONFORMING AND CLERICAL AMENDMENTS.

(a) SECTIONS.—The following provisions of the Security and Accountability for Every Port Act of 2006 (Public Law 109–347) are amended as follows:

(1) By striking section 105.

(2) By redesignating sections 106 and 107 as sections 105 and 106, respectively.

(3) By striking section 108.

(4) By redesignating sections 109 and 110 as sections 107 and 108, respectively.

(5) In section 121 (6 U.S.C. 921)—

(A) by striking subsections (c), (d), and (e); and

(B) redesignating subsections (f), (g), (h), and (i) as subsections (c), (d), (e), and (f), respectively.

(6) By striking sections 122 and 127 (6 U.S.C. 922 and).

(7) By redesignating sections 123, 124, 125, 126, and 128 as sections 122, 123, 124, 125, and 126, respectively.

(8) In section 233 (6 U.S.C. 983), by striking subsection (c).

(9) By striking section 235 (6 U.S.C. 984).

(10) By redesignating section 236 as section 235.

(11) By striking sections 701 and 708 (and the item relating to such section in the table of contents of such Act).

(12) By redesignating sections 702, 703, 704, 705, 706, 707, and 709 as sections 701, 702, 703, 704, 705, 706, and 707, respectively.

(b) TABLE OF CONTENTS.—

(1) SECURITY AND ACCOUNTABILITY FOR EVERY PORT ACT OF 2006.—The table of contents of the Security and Accountability for Every Port Act of 2006 (Public Law 109–347) is amended as follows:

(A) In the list of items relating to subtitle A of title I, by striking the items relating to sections 105 through 110 and inserting the following new items:

"Sec. 105. Prohibition of issuance of transportation security cards to persons convicted of certain felonies.
"Sec. 106. Long-range vessel tracking.
"Sec. 107. Notice of arrival for foreign vessels on the Outer Continental Shelf.
"Sec. 108. Enhanced crewmember identification.".

(B) In the list of items relating to subtitle C of title I, by striking the items relating to sections 122 through 128 and inserting the following new items:

"Sec. 122. Random searches of containers.
"Sec. 123. Work stoppages and employee-employer disputes.
"Sec. 124. Threat assessment screening of port truck drivers.
"Sec. 125. Border Patrol unit for United States Virgin Islands.
"Sec. 126. Center of Excellence for Maritime Domain Awareness.".

(C) In the list of items relating to subtitle C of title II, by striking the items relating to sections 235 and 236 and inserting the following new item:

"Sec. 235. Information sharing relating to supply chain security cooperation.".

(D) In the list of items relating to title VII, by striking the items relating to sections 701 through 709 and inserting the following new items:

"Sec. 701. Disclosures regarding homeland security grants.
"Sec. 702. Trucking security.
"Sec. 703. Air and Marine Operations of the Northern Border Air Wing.
"Sec. 704. Phaseout of vessels supporting oil and gas development.
"Sec. 705. Coast Guard property in Portland, Maine.
"Sec. 706. Methamphetamine and methamphetamine precursor chemicals.
"Sec. 707. Protection of health and safety during disasters.".

(2) TITLE 46.—In the list of items relating to the analysis for chapter 701 of title 46, United States Code, by striking the items relating to sections 70107A and 70116.

TITLE V—TRANSPORTATION SECURITY ADMINISTRATION

Subtitle A—Administration

SEC. 501. AMENDMENTS TO THE HOMELAND SECURITY ACT OF 2002 AND TITLE 5, UNITED STATES CODE.

(a) HOMELAND SECURITY ACT OF 2002.—Paragraph (1) of section 103(a) of the Homeland Security Act of 2002, as amended by this Act, is further amended by adding at the end the following new subparagraph:

"(K) An Administrator of the Transportation Security Administration, in accordance with section 114 of title 49, United States Code.".

(b) INCLUSION IN EXECUTIVE SCHEDULE.—Section 5315 of title 5, United States Code, is amended by adding at the end the following:

"Administrator of the Transportation Security Administration, Department of Homeland Security.".

SEC. 502. AMENDMENTS TO TITLE 49, UNITED STATES CODE.

(a) AMENDMENTS.—Section 114 of title 49, United States Code, is amended—

(1) in subsection (a), by striking "Department of Transportation" and inserting "Department of Homeland Security";

(2) in subsection (b)(1), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration";

(3) by striking "Under Secretary" each place it appears and inserting "Administrator";

(4) in subsection (b), in the heading, by striking "UNDER SECRETARY" and inserting "ADMINISTRATOR";

(5) in subsection (e)(4), by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security";

(6) in subsection (f)—

(A) in paragraph (6), by striking "Managers" and inserting "Directors"; and

(B) in paragraph (14), by inserting "air carriers or" before "foreign air carriers";

(7) in subsection (g)—

(A) by striking "the Secretary" each place it appears and inserting "the Secretary of Homeland Security"; and

(B) in paragraph (3), by striking "The Secretary" and inserting "The Secretary of Homeland Security";

(8) in subsection (j)(1)(D), by striking "the Secretary" and inserting "the Secretary of Homeland Security";

(9) in subsection (l)—

(A) in paragraph (2)(A), by striking "the Secretary" and inserting "the Secretary of Homeland Security"; and

(B) in paragraph (4)(B), by striking "the Administrator under subparagraph (A)" and inserting "the Administrator of the Federal Aviation Administration under subparagraph (A)";

(10) in subsection (m)—

(A) in the heading, by striking "UNDER SECRETARY" and inserting "ADMINISTRATOR"; and

(B) in paragraph (1), in the heading, by striking "UNDER SECRETARY" and inserting "ADMINISTRATOR";

(11) in subsection (n), by striking "Department of Transportation" and inserting "Department of Homeland Security";

(12) in subsection (o), by striking "Department of Transportation" and inserting "Department of Homeland Security";

(13) in subsection (p)(4), by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security";

(14) by redesignating subsections (u), (v), and (w) as subsections (t), (cc), and (dd), respectively; and

(15) by inserting after subsection (t), as so redesignated, the following new subsections:

"(u) DEPUTY ADMINISTRATOR.—There is established in the Transportation Security Administration a Deputy Administrator, who shall assist the Administrator in the management of the Transportation Security Administration.

"(v) OFFICE OF PUBLIC AFFAIRS.—

"(1) ESTABLISHMENT.—There is established in the Transportation Security Administration an Office of Public Affairs (in this subsection referred to as the 'Office').

"(2) ASSISTANT ADMINISTRATOR.—The head of the Office shall be the Assistant Administrator for Public Affairs, who shall report to the Administrator of the Transportation Security Administration or the Administrator's designee.

"(3) FUNCTIONS.—The Office shall be responsible for facilitating understanding of the Transportation Security Administration's mission by communicating with internal and external audiences in a timely, accurate, and transparent manner.

"(w) OFFICE OF CIVIL RIGHTS AND LIBERTIES, OMBUDSMAN, AND TRAVELER ENGAGEMENT.—

"(1) ESTABLISHMENT.—There is established in the Transportation Security Administration an Office of Civil Rights and Liberties, Ombudsman, and Traveler Engagement (in this subsection referred to as the 'Office').

"(2) ASSISTANT ADMINISTRATOR.—The head of the Office shall be the Assistant Administrator for Civil Rights and Liberties, Ombudsman, and Traveler Engagement, who shall report to the Administrator of the Transportation Security Administration or the Administrator's designee.

"(3) FUNCTIONS.—The Office shall be responsible for managing allegations of violations of civil rights and civil liberties from the public, carrying out the Administration's equal employment opportunity and diversity policies and programs, including complaint management and adjudication, and helping to ensure that employees and the traveling public are treated in a fair and lawful manner.

"(x) OFFICE OF LEGISLATIVE AFFAIRS.—

"(1) ESTABLISHMENT.—There is established in the Transportation Security Administration an Office of Legislative Affairs (in this subsection referred to as the 'Office').

"(2) ASSISTANT ADMINISTRATOR.—The head of the Office shall be the Assistant Administrator for Legislative Affairs, who shall report to the Administrator of the Transportation Security Administration or the Administrator's designee.

"(3) FUNCTIONS.—The Office shall be responsible for developing and implementing strategies within the Transportation Security Administration to achieve congressional approval or authorization of the Administration's programs and policies.

"(y) OFFICE OF FINANCE AND ADMINISTRATION.—

"(1) ESTABLISHMENT.—There is established in the Transportation Security Administration an Office of Finance and Administration (in this subsection referred to as the 'Office').

"(2) CHIEF FINANCIAL OFFICER.—The head of the Office shall be the Chief Financial Officer, who shall report to the Administrator of the Transportation Security Administration or the Administrator's designee.

"(3) FUNCTIONS.—The Office shall be responsible for financial, budgetary, and administrative activities that support the mission of the Transportation Security Administration.

"(z) OFFICE OF THE CHIEF OF OPERATIONS.—

"(1) ESTABLISHMENT.—There is established in the Transportation Security Administration an Office of the Chief of Operations (in this subsection referred to as the 'Office').

"(2) CHIEF OF OPERATIONS.—The head of the Office shall be the Chief of Operations, who shall report to the Administrator of the Transportation Security Administration or the Administrator's designee.

"(3) FUNCTIONS.—The Office shall be responsible for the following:

"(A) Conducting protection, response, detection, assessment, and investigation activities in airports and other transportation facilities and deploying Federal Air Marshals on United States aircraft traveling domestically and internationally.

"(B) Identifying, analyzing, and mitigating risk by assessing vulnerabilities at international locations to determine risk, evaluating risk impacts to determine mitigation activities, and executing mitigation activities to reduce risk to the United States.

"(C) Providing security and intelligence professionals with timely information in order to prevent a terrorist attack against the transportation systems of the United States.

"(D) Developing security policies and plans that reduce the risk of catastrophic terrorist attacks.

"(E) Providing risk-based, adaptive security that includes airport checkpoint and baggage screening operations, regulatory compliance, cargo inspections, and other specialized programs designed to secure transportation.

"(F) Safeguarding the transportation systems of the United States through the qualification and delivery of innovative security capabilities.

"(aa) OFFICE OF THE CHIEF OF MISSION SUPPORT.—

"(1) ESTABLISHMENT.—There is established in the Transportation Security Administration an Office of the Chief of Mission Support (in this subsection referred to as the 'Office').

"(2) CHIEF OF MISSION SUPPORT.—The head of the Office shall be the Chief of Mission Support, who shall report to the Administrator of the Transportation Security Administration or the Administrator's designee.

"(3) FUNCTIONS.—The Office shall be responsible for the following:

"(A) Negotiating and awarding contracts and other procurement vehicles that improve the Transportation Security Administration's capabilities.

"(B) Providing strategic, sustainable, and comprehensive programs and services that attract, build, and inspire a talented workforce.

"(C) Overseeing the development, delivery, and evaluation of training programs for Transportation Security Administration employees.

"(D) Providing information technologies and services that enable global transportation security.

"(E) Ensuring the integrity, efficiency, and effectiveness of the Transportation Security Administration's workforce, operations, and programs through objective audits, covert testing, inspections, and criminal investigations.

"(F) Ensuring consistency in misconduct penalty determinations and an expeditious and fair adjudication process.

"(G) Building the Transportation Security Administration's capabilities by managing the acquisition, testing, deployment, and sustainment of security technology and other acquisition programs.

"(bb) OFFICE OF THE CHIEF COUNSEL.—

"(1) ESTABLISHMENT.—There is established in the Transportation Security Administration an Office of the Chief Counsel (in this subsection referred to as the 'Office').

"(2) CHIEF COUNSEL.—The head of the Office shall be the Chief Counsel for the Transportation Security Administration, who shall report to the General Counsel of the Department of Homeland Security.

"(3) FUNCTIONS.—The Office shall be responsible for providing legal advice and services across the Transportation Security Administration.".

(b) SECTION 115.—Subsection (c) of section 115 of title 49, United States Code, is amended—

(1) in paragraph (1), by striking "Under Secretary of Transportation for security" and inserting "Administrator of the Transportation Security Administration"; and

(2) in paragraph (6), by striking "Under Secretary" and inserting "Administrator of the Transportation Security Administration".

(c) SECTION 40119.—Section 40119 of title 49, United States Code, is amended—

(1) in subsection (a), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration";

(2) in subsection (b)(4)—

(A) by inserting "of the Federal Aviation Administration" after "Administrator"; and

(B) by inserting "Federal Aviation" before "Administration"; and

(3) in subsection (c), by striking "Under Secretary" and inserting "Administrator of the Transportation Security Administration".

(d) SECTION 44901.—Section 44901 of title 49, United States Code, is amended—

(1) by striking "Under Secretary of Transportation for Security" each place it appears and inserting "Administrator of the Transportation Security Administration";

(2) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration";

(3) by striking "Assistant Secretary (Transportation Security Administration)" each place it appears and inserting "Administrator of the Transportation Security Administration";

(4) by striking "Assistant Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration"; and

(5) in subsection (d), by striking "Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Transportation" each place it appears and inserting "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".

(e) SECTION 44902.—Section 44902 of title 49, United States Code, is amended—

(1) in subsection (a), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(2) in subsection (b), by striking "Under Secretary" and inserting "Administrator of the Transportation Security Administration".

(f) SECTION 44903.—Section 44903 of title 49, United States Code, is amended—

(1) in subsection (b)(1), by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security";

(2) in subsection (c)(2)(C), by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security";

(3) in subsection (d), in the matter preceding paragraph (1), by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security";

(4) in subsection (g)—

(A) in paragraph (1)(A), in the heading, by striking "UNDER SECRETARY" and inserting "ADMINISTRATOR"; and

(B) in paragraph (2), by striking "Under Secretary's" each place it appears and inserting "Transportation Security Administration Administrator's";

(5) in subsection (h)—

(A) in paragraph (3), by inserting "of Homeland Security" after "Secretary";

(B) in paragraph (6)(C), in the matter preceding clause (i), by inserting "of Homeland Security" after "Secretary";

(6) in subsection (i)(l), by striking ", after receiving the recommendations of the National Institute of Justice,";

(7) in subsection (j)—

(A) in paragraph (1)—

(i) in the matter preceding subparagraph (A), by striking "Under Secretary for Transportation Security" and inserting "Administrator of the Transportation Security Administration"; and

(ii) in the matter following subparagraph (E), by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security"; and

(B) in paragraph (2), by striking "Secretary of Transportation" each place it appears and inserting "Secretary of Homeland Security";

(8) in subsection (l)(1), by striking "Under Secretary for Border and Transportation Security of the Department of Homeland Security" and inserting "Administrator of the Transportation Security Administration";

(9) by striking "Under Secretary of Transportation for Security" each place it appears and inserting "Administrator of the Transportation Security Administration";

(10) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration";

(11) by striking "Assistant Secretary of Homeland Security (Transportation Security Administration)" each place it appears and inserting "Administrator of the Transportation Security Administration"; and

(12) by striking "Assistant Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(g) SECTION 44904.—Section 44904 of title 49, United States Code, is amended—

(1) in subsection (a), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration";

(2) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration"; and

(3) in subsection (d) by striking "Assistant Secretary of Homeland Security (Transportation Security Administration)" and inserting "Administrator of the Transportation Security Administration".

(h) SECTION 44905.—Section 44905 of title 49, United States Code, is amended—

(1) in subsection (a), by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security";

(2) in subsection (b), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(3) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(i) SECTION 44906.—Section 44906 of title 49, United States Code, is amended—

(1) by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(2) by striking "Under Secretary" each place it appears and inserting "Administrator".

(j) SECTION 44908.—Section 44908 of title 49, United States Code, is amended by striking "Secretary of Transportation" each place it appears and inserting "Secretary of Homeland Security".

(k) SECTION 44909.—Section 44909 of title 49, United States Code, is amended—

(1) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration"; and

(2) by striking "the Customs Service" each place it appears and inserting "U.S. Customs and Border Protection".

(l) SECTION 44911.—Section 44911 of title 49, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraphs (1) through (10), by striking "the" each place it appears and inserting "The"; and

(B) by inserting the following at the end the following new paragraphs:

"(11) The Coast Guard.

"(12) The Department of Homeland Security.

"(13) The National Geospatial-Intelligence Agency.

"(14) The National Reconnaissance Office.";

(2) in subsection (b)—

(A) by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security"; and

(B) by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration";

(3) in subsection (d), by striking "the Secretary" and inserting "the Secretary of Homeland Security"; and

(4) in subsection (e)—

(A) by striking "the Secretary" and inserting "the Secretary of Homeland Security"; and

(B) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(m) SECTION 44912.—Section 44912 of title 49, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(B) in paragraph (3), by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security";

(2) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(n) SECTION 44913.—Section 44913 of title 49, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(B) in paragraph (2), by striking "the Committee on Transportation and Infrastructure" and inserting "the Committee on Homeland Security";

(2) in subsection (b), by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security"; and

(3) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(o) SECTION 44914.—Section 44914 of title 49, United States Code, is amended—

(1) by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(2) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(p) SECTION 44915.—Section 44915 of title 49, United States Code, is amended by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration".

(q) SECTION 44916.—Section 44916 of title 49, United States Code, is amended—

(1) in subsection (a), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(2) in subsection (b), by striking "Under Secretary" and inserting "Administrator of the Transportation Security Administration".

(r) SECTION 44917.—Section 44917 of title 49, United States Code, is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(B) in paragraph (2), by inserting "of Homeland Security, utilizing a risk-based security methodology," after "Secretary";

(2) by striking subsections (b) and (c);

(3) redesignating subsection (d) as subsection (b); and

(4) in subsection (b), as so redesignated—

(A) in paragraph (1), by striking "Assistant Secretary for Immigration and Customs Enforcement" and inserting "Administrator of the Transportation Security Administration"; and

(B) in paragraph (3), by striking "Assistant Secretary" each place it appears and inserting "Administrator".

(s) SECTION 44918.—Section 44918 of title 49, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (2)(E), by striking "the Under Secretary for Border and Transportation Security of the Department of Homeland Security" and inserting "the Administrator of the Transportation Security Administration"; and

(B) in paragraphs (5), (6), and (7), by striking "the Administrator" each place it appears and inserting "the Administrator of the Federal Aviation Administration"; and

(2) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(t) SECTION 44919.—Section 44919 of title 49, United States Code, is amended by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(u) SECTION 44920.—Section 44920 of title 49, United States Code, is amended by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(v) SECTION 44921.—Section 44921 of title 49, United States Code, is amended—

(1) in subsection (a), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(2) in subsection (b)(6)—

(A) by inserting "the Committee on Homeland Security and" before "the Committee on Transportation and Infrastructure"; and

(B) by inserting "the Committee on Homeland Security and Governmental Affairs" before "the Committee on Commerce, Science, and Transportation";

(3) in subsection (d)(4), by striking "may," and inserting "may";
(4) in subsection (i)(2), by striking "the Under Secretary" before "may";
(5) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration"; and
(6) by striking "Under Secretary's" each place it appears and inserting "Transportation Security Administration Administrator's".

(w) SECTION 44922.—Section 44922 of title 49, United States Code, is amended—
(1) in subsection (a), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and
(2) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(x) SECTION 44923.—Section 44923 of title 49, United States Code, is amended—
(1) in subsection (a), in the matter preceding paragraph (1), by striking "the Under Secretary for Border and Transportation Security of the Department of Homeland Security" and inserting "the Administrator of the Transportation Security Administration";
(2) in subsection (c), by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security"; and
(3) in subsection (d)—
(A) in paragraph (3), in the heading, by striking "UNDER SECRETARY" and inserting "ADMINISTRATOR"; and
(B) in paragraph (4), by inserting ", Homeland Security," before "and Transportation and Infrastructure"; and
(4) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(y) SECTION 44924.—Section 44924 of title 49, United States Code, is amended—
(1) in subsection (a)—
(A) by striking "Under Secretary for Border and Transportation for Security of the Department of Homeland Security" and inserting "Administrator of the Transportation Security Administration"; and
(B) by striking "Administrator under" and inserting "Administrator of the Federal Aviation Administration under";
(2) in each of subsections (b) through (f), by inserting "of the Federal Aviation Administration" after "Administrator" each place it appears;
(3) in subsection (g), by inserting "the Committee on Homeland Security and" before "the Committee on Transportation and Infrastructure"; and
(4) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(z) SECTION 44925.—Section 44925 of title 49, United States Code, is amended—
(1) in subsection (b)—
(A) in paragraph (1), by striking "Assistant Security of Homeland Security (Transportation Security Administration)" and inserting "Administrator of the Transportation Security Administration"; and
(B) in paragraph (3), by inserting "of Homeland Security" after "Secretary"; and
(2) in subsection (d), by striking "Assistant Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(aa) SECTION 44926.—Section 44926 of title 49, United States Code, is amended—
(1) in subsection (a), by striking "United States" and inserting "U.S."; and
(2) in subsection (b)(3)—
(A) in the matter preceding subparagraph (A), by striking "an" and inserting "a"; and
(B) in subparagraph (B), by striking "United States" and inserting "U.S.".

(bb) SECTION 44927.—Section 44927 of title 49, United States Code, is amended—
(1) in subsection (a), in the first sentence, by striking "Veteran" and inserting "Veterans"; and
(2) by striking "Assistant Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(cc) SECTION 44933.—Section 44933 of title 49, United States Code, is amended—
(1) in the heading, by striking "**MANAGERS**" and inserting "**DIRECTORS**";
(2) in subsection (a)—
(A) in the first sentence—
(i) by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and
(ii) by striking "Manager" and inserting "Director";
(B) in the second sentence—

(i) by striking "Under Secretary" and inserting "Administrator of the Transportation Security Administration"; and

(ii) by striking the term "Managers" each place it appears and inserting "Directors"; and

(3) in subsection (b)—

(A) in the matter preceding paragraph (1), by striking "Manager" and inserting "Director"; and

(B) in paragraph (2), by striking "Under Secretary" and inserting "the Administrator of the Transportation Security Administration".

(dd) SECTION 44934.—Section 44934 of title 49, United States Code, is amended—

(1) in subsection (a), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(2) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(ee) SECTION 44935.—Section 44935 of title 49, United States Code, is amended—

(1) by striking "Under Secretary of Transportation for Security" each place it appears and inserting "Administrator of the Transportation Security Administration";

(2) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration";

(3) in subsection (e)(2)(A)(ii), by striking "section 1101(a)(22) of the Immigration and Nationality Act" and inserting "section 101(a)(22) of the Immigration and Nationality Act"; and

(4) by redesignating the second subsection (i) (relating to accessibility of computer-based training facilities) as subsection (k).

(ff) SECTION 44936.—Section 44936 of title 49, United States Code, is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A)—

(i) by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(ii) by striking "Under Secretary of Transportation for Transportation Security,," and inserting "Administrator of the Transportation Security Administration,"; and

(B) in subparagraphs (B) and (C), by striking "Under Secretary of Transportation for Transportation Security" each place it appears and inserting "Administrator of the Transportation Security Administration";

(2) in subsection (c)(1), by striking "Under Secretary's" and inserting "Transportation Security Administration Administrator's"; and

(3) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(gg) SECTION 44937.—Section 44937 of title 49, United States Code, is amended by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration".

(hh) SECTION 44938.—Section 44938 of title 49, United States Code, is amended—

(1) in subsection (a), in the matter preceding paragraph (1)—

(A) by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security";

(B) by striking "the Secretary considers" and inserting "the Secretary of Homeland Security considers";

(C) by striking "The Secretary" and inserting "The Secretary of Homeland Security"; and

(D) by striking "Under Secretary of Transportation Security" and inserting "Administrator of the Transportation Security Administration"; and

(2) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(ii) SECTION 44940.—Section 44940 of title 49, United States Code, is amended—

(1) in subsection (a)(1)—

(A) in the matter preceding paragraph (1), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(B) in subparagraph (F) by striking " Managers" and inserting "Directors";

(2) in subsection (e)(1), in the heading, by striking "UNDER SECRETARY" and inserting "ADMINISTRATOR"; and

(3) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(jj) SECTION 44941.—Section 44941 of title 49, United States Code, is amended by inserting "the Department of Homeland Security," before "the Department of Transportation".

(kk) SECTION 44942.—Section 44942 of title 49, United States Code, is amended—

(1) in subsection (b)—

(A) in paragraph (1)—

(i) by redesignating paragraph (1) as subsection (c) and moving such subsection, as so redesignated, two ems to the left; and

(ii) by redesignating subparagraphs (A) and (B) as subsections (d) and (e), respectively, and moving such subsections, as so redesignated, four ems to the left;

(2) by striking subsections (a) and (b);

(3) by striking subsection (c), as so redesignated;

(4) by redesignating subsections (d) and (e), as so redesignated, as subsections (a) and (b), respectively;

(5) by striking the term "the Secretary" each place it appears and inserting "the Secretary of Homeland Security";

(6) by striking "Under Secretary for Transportation Security" each place it appears and inserting "Administrator of the Transportation Security Administration"; and

(7) by striking "Congress" and inserting "the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate".

(ll) SECTION 44943.—Section 44943 of title 49, United States Code, is amended—

(1) in subsection (a), by striking "The Under Secretary for Transportation Security" and inserting "The Administrator of the Transportation Security Administration";

(2) in subsection (b)—

(A) in paragraph (1)—

(i) by striking "the Secretary" and inserting "the Secretary of Homeland Security"; and

(ii) by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(B) by striking "the Under Secretary" each place it appears and inserting "the Administrator of the Transportation Security Administration"; and

(3) in subsection (c), by striking "the Under Secretary for Transportation Security" and inserting "the Administrator of the Transportation Security Administration".

(mm) SECTION 44944.—Section 44944 of title 49, United States Code, is amended—

(1) in subsection (a)(1), by striking "Under Secretary of Transportation for Transportation Security" and inserting "Administrator of the Transportation Security Administration"; and

(2) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(nn) SECTION 44945.—Section 44945 of title 49, United States Code, is amended by striking "Assistant Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(oo) SECTION 44946.—Section 44946 of title 49, United States Code, is amended—

(1) in subsection (c)(2)(A), by striking ", but a member may continue to serve until a successor is appointed" and inserting "but may continue until such time as a successor member begins serving on the Advisory Committee";

(2) in subsection (g)—

(A) by striking paragraph (2); and

(B) redesignating paragraph (3) as paragraph (2); and

(3) by striking "Assistant Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration".

(pp) SECTION 45107.—Section 45107 of title 49, United States Code, is amended—

(1) in subsection (a), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(2) in subsection (b), by striking the second sentence.

(qq) CLERICAL AMENDMENTS.—The analysis for chapter 449 of title 49, United States Code, is amended by striking the item relating to section 44933 and inserting the following new item:

"44933. Federal Security Directors.".

SEC. 503. AMENDMENTS TO THE AVIATION AND TRANSPORTATION SECURITY ACT.

(a) SECTION 101.—Section 101 of the Aviation and Transportation Security Act (Public Law 107–71) is amended—

(1) in subsection (c) (5 U.S.C. 5313 note)—

(A) by striking paragraph (1);

(B) by redesignating paragraphs (2) and (3) as paragraph (1) and (2), respectively; and

(C) in paragraph (1), as so redesignated—

(i) by striking "Under Secretary" and inserting "Administrator of the Transportation Security Administration";

(ii) by striking "30 percent" and inserting "15 percent";

(iii) by striking "the Secretary's" and inserting "the Secretary of Homeland Security's"; and

(iv) by striking "Under Secretary's" and inserting "Transportation Security Administration Administrator's"; and

(2) by striking subsection (g) (49 U.S.C. 44901 note).

(b) SECTION 106.—Section 106 of the Aviation and Transportation Security Act (49 U.S.C. 44903 note) is amended—

(1) in subsection (b)—

(A) in paragraph (1), in the matter preceding subparagraph (A), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration";

(B) in paragraph (2)(A), by striking "Under Secretary" each place it appears and inserting "Administrator"; and

(C) in paragraph (2)(B), in the matter preceding clause (i), by striking "Secretary" and inserting "Secretary of Homeland Security"; and

(2) in subsection (e), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration".

(c) SECTION 109.—Section 109 of the Aviation and Transportation Security Act (49 U.S.C. 114 note) is amended—

(1) in subsection (a)—

(A) by striking "(a) IN GENERAL.—The Under Secretary of Transportation for Security" and inserting "The Administrator of the Transportation Security Administration";

(B) in paragraph (4), by—

(i) striking "medical product" and inserting "liquid or gel medical product or nourishment and nutrition for infants and toddlers, including formula, breast milk, and juice,"; and

(ii) by striking "the product" and inserting "such product or nourishment or nutrition"; and

(C) in paragraph (7), by striking "voice stress analysis, biometric," and inserting "biometric"; and

(2) by striking subsection (b).

(d) SECTION 110.—Section 110 of the Aviation and Transportation Security Act is amended by striking subsections (c) and (d).

(e) SECTION 111.—Section 111 of the Aviation and Transportation Security Act (49 U.S.C. 44935 note) is amended—

(1) in subsection (c)—

(A) by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(B) by striking "Under Secretary" each place it appears and inserting "Administrator of the Transportation Security Administration";

(2) in subsection (d)—

(A) in paragraph (1)—

(i) by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and

(ii) by striking "Under Secretary" each place it appears and inserting "Administrator"; and

(B) in paragraph (2), by striking "Under Secretary" and inserting "Administrator of the Transportation Security Administration".

(f) SECTION 117.—Section 117 of the Aviation and Transportation Security Act (49 U.S.C. 44903 note) is amended by striking "Secretary of Transportation" and inserting "Secretary of Homeland Security".

(g) SECTION 132.—Section 132 of the Aviation and Transportation Security Act is repealed.

(h) SECTION 135.—Section 135 of the Aviation and Transportation Security Act is repealed.

(i) SECTION 137.—Section 137 of the Aviation and Transportation Security Act (49 U.S.C. 44912 note) is repealed.

(j) REDESIGNATIONS.—Sections 133, 134, 136, 138, 139, 140, 141, 142, 143, 144, 145, 146, and 147 of the Aviation and Transportation Security Act are amended by redesignating such sections as sections 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, and 144, respectively.

SEC. 504. INFORMATION REQUIRED TO BE SUBMITTED TO CONGRESS UNDER THE STRATEGIC 5-YEAR TECHNOLOGY INVESTMENT PLAN OF THE TRANSPORTATION SECURITY ADMINISTRATION.

(a) ADDITIONAL INFORMATION REQUIRED.—Section 1611 of the Homeland Security Act of 2002 (6 U.S.C. 563) is amended—

(1) in subsection (g)—

(A) in the matter preceding paragraph (1), by striking "biennially" and inserting "annually";

(B) in paragraph (1), by striking "and";

(C) in paragraph (2), by striking the period and inserting "; and";

(D) by adding at the end the following new paragraph:

"(3) information about acquisitions completed during the fiscal year preceding the fiscal year during which the report is submitted."; and

(2) by adding at the end the following new subsections:

"(h) 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 House of Representatives notice of any covered change to the Plan by not later than 90 days after the date on which the change is made.

"(2) DEFINITION OF CHANGE.—In this subsection, the term 'covered change' means an increase or decrease in the dollar amount allocated to the procurement of a technology or an increase or decrease in the number of a technology.".

(b) REPORT ON EQUIPMENT IN OPERATION POST-LIFE-CYCLE.—Not later than 90 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives a report describing any equipment of the Transportation Security Administration that is in operation after—

(1) the end of the life-cycle of the equipment specified by the manufacturer of the equipment; or

(2) the end of the useful life projection for the equipment under the strategic 5-year technology investment plan of the Transportation Security Administration, as required by section 1611 of the Homeland Security Act of 2002 (6 U.S.C. 563).

(c) NOTICE TO AIRPORTS AND AIRLINES.—Upon the enactment of this Act, the Administrator of the Transportation Security Administration shall notify airports and airlines of any changes to the 5-year technology investment plan of the Transportation Security Administration.

SEC. 505. MAINTENANCE OF SECURITY-RELATED TECHNOLOGY.

(a) IN GENERAL.—Title XVI of the Homeland Security Act of 2002 (6 U.S.C. 561 et seq.) is amended by adding at the end the following new subtitle:

"Subtitle C—Maintenance of Security-Related Technology

"SEC. 1621. MAINTENANCE VALIDATION AND OVERSIGHT.

"(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this subtitle, 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 contracts 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.".

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 1616 the following:

"Subtitle C—Maintenance of Security-Related Technology

"Sec. 1621. Maintenance validation and oversight.".

SEC. 506. TRANSPORTATION SECURITY ADMINISTRATION EFFICIENCY.

(a) EFFICIENCY REVIEW.—Not later than 270 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall conduct and complete a comprehensive, agency-wide efficiency review of the Administration to identify and effectuate spending reductions and administrative savings through the streamlining or restructuring of Administration divisions to make the Administration more efficient. In carrying out the review under this section, the Administrator shall consider each of the following:

(1) The elimination of any unnecessarily duplicative or overlapping programs and initiatives that can be streamlined.

(2) The elimination of any unnecessary or obsolete rules, regulations, directives, or procedures.

(3) The reduction in overall operating expenses of the Administration, including costs associated with the number of personnel, as a direct result of efficiencies gained through the implementation of risk-based screening or through any other means as determined by the Administrator.

(4) Any other matters the Administrator determines are appropriate.

(b) REPORT TO CONGRESS.—Not later than 30 days after the completion of the efficiency review required under subsection (a), the Administrator of the Transportation Security Administration shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on the results and cost savings expected to be achieved through such efficiency review.

SEC. 507. TRANSPORTATION SENIOR EXECUTIVE SERVICE ACCOUNTABILITY.

(a) REDUCTION PLAN.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Administrator of the Transportation Security Administration, shall develop a strategic plan, including a timeline, to reduce by 20 percent by June 30, 2019, the number of positions at the Senior Executive Service level at the Administration.

(b) CONGRESSIONAL REVIEW.—Not later than 30 days after the completion of the Senior Executive Service reduction plan required under subsection (a), the Administrator of the Transportation Security Administration shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a copy of such plan.

Subtitle B—Passenger Security and Screening

SEC. 511. DEPARTMENT OF HOMELAND SECURITY TRUSTED TRAVELER PROGRAM COLLABORATION.

The Secretary of Homeland Security shall continue the review of all trusted traveler vetting programs carried out by the Department of Homeland Security using representatives from such programs to make recommendations on possible efficiencies that could be gained by integrating requirements and operations and increasing information and data sharing across programs.

SEC. 512. PRECHECK BIOMETRIC PILOT PROJECT.

Not later than one year after the date of the enactment of this Act, the Administrator of the Transportation Security Administration (TSA) shall conduct a pilot project to test a secure, automated, and biometric-based system at airports to verify the identity of individuals who are members of TSA PreCheck or another Depart-

ment of Homeland Security trusted traveler program that affords TSA expedited screening. Such system shall be designed to—

(1) improve security while also reducing the need for security screening personnel to perform identity and travel document verification for such individuals;

(2) reduce the average wait time of such individuals;

(3) reduce overall operating expenses of the Administration;

(4) be integrated with the Department's watch list and trusted traveler matching programs; and

(5) be integrated with other technologies to further facilitate risk-based passenger screening at checkpoints, to the extent practicable and consistent with security standards.

SEC. 513. IDENTITY AND TRAVEL DOCUMENT VERIFICATION.

Section 44901 of title 49, United States Code, is amended by adding at the end the following new subsection:

"(m) ESTABLISHMENT OF SCREENING SYSTEM FOR CERTAIN PERSONS.—Not later than December 31, 2018, the Administrator of the Transportation Security Administration shall, subject to the availability of appropriations, implement an identity and travel document verification system designed to establish a secure, automated system at all airports for verifying identity and travel documents of persons seeking entry into the sterile area of an airport. Such system shall—

"(1) assess the need for security screening personnel to perform identity and travel document verification for such passengers, thereby assessing the overall number of such screening personnel;

"(2) reduce the average wait time of such passengers;

"(3) reduce overall operating expenses of the Administration;

"(4) be integrated with the Administration's watch list matching program; and

"(5) be integrated with other technologies to further facilitate risk-based passenger screening at checkpoints, to the extent practicable and consistent with security standards.".

SEC. 514. COMPUTED TOMOGRAPHY PILOT PROJECT.

Not later than 90 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall conduct a pilot project to test the use of screening equipment using computed tomography technology to screen baggage at passenger checkpoints.

SEC. 515. EXPLOSIVES DETECTION CANINE TEAMS FOR AVIATION.

(a) PASSENGER SCREENING TEAMS.—The Administrator of the Transportation Security Administration shall ensure that by December 31, 2018, at least 300 explosives detection canine teams are dedicated to passenger screening purposes at airports in the United States at which the Administration performs, or oversees the implementation and performance of, security measures, including screening responsibilities.

(b) USE OF CANINES TO DETECT SCREENING ANOMALIES.—At airports in the United States at which—

(1) canine teams trained to screen passengers are available, and

(2) the Transportation Security Administration has passenger screening responsibilities,

the Administrator of the Transportation Security Administration may use such teams to detect screening anomalies.

SEC. 516. STANDARD OPERATING PROCEDURES AT AIRPORT CHECKPOINTS.

(a) STANDARDIZATION.—The Administrator of the Transportation Security Administration shall require, to the extent practicable, that standard operating procedures at airport checkpoints for passengers and carry-on baggage are carried out in a uniform manner among similarly situated airports.

(b) REPORT TO CONGRESS.—Not later than 270 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on how standard operating procedures were made uniform in accordance with subsection (a).

(c) AUDITS.—Beginning one year after the date of the enactment of this Act, the Inspector General of the Department of Homeland Security shall conduct periodic audits of adherence to the standard operating procedures, as established by the Administrator of the Transportation Security Administration, under this section of screening personnel at large, medium, and small airports in diverse geographical areas.

SEC. 517. TRAVELER REDRESS IMPROVEMENT.

(a) REDRESS PROCESS.—

(1) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall, using existing resources, systems, and processes, ensure the availability of the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) redress process to adjudicate inquiries for individuals who—

(A) are citizens of the United States or aliens lawfully admitted for permanent residence;

(B) have filed an inquiry with DHS TRIP after receiving enhanced screening at an airport passenger security checkpoint more than three times in any 60-day period; and

(C) believe they have been wrongly identified as being a threat to aviation security.

(2) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the implementation of the redress process required under paragraph (1).

(b) PRIVACY IMPACT REVIEW AND UPDATE.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall review and update the Privacy Impact Assessment for the Secure Flight programs to ensure such Assessment accurately reflects the operation of such programs.

(2) PUBLIC DISSEMINATION; FORM.—The Secure Flight Privacy Impact Assessment review and update required under paragraph (1) shall be published on a publically-accessible internet webpage of the Transportation Security Administration and submitted to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

(c) TRANSPORTATION SECURITY ADMINISTRATION RULE REVIEW AND NOTIFICATION PROCESS.—

(1) RULE REVIEW.—Not later than 60 days after the date of the enactment of this Act and every 120 days thereafter, the Assistant Administrator of the Office of Intelligence and Analysis of the Transportation Security Administration, in coordination with the entities specified in paragraph (2), shall conduct a comprehensive review of the Transportation Security Administration's intelligence-based screening rules.

(2) NOTIFICATION PROCESS.—Not later than 48 hours after changing, updating, implementing, or suspending a Transportation Security Administration intelligence-based screening rule, the Assistant Administrator of the Office of Intelligence and Analysis of the Transportation Security Administration shall notify the following entities of any such change, update, implementation, or suspension, as the case may be:

(A) The Office of Civil Rights and Liberties, Ombudsman, and Traveler Engagement of the Transportation Security Administration.

(B) The Office of Civil Rights and Liberties of the Department of Homeland Security.

(C) The Office of Chief Counsel of the Administration.

(D) The Office of General Counsel of the Department.

(E) The Privacy Office of the Administration.

(F) The Privacy Office of the Department.

(G) The Federal Air Marshal Service.

(H) The Traveler Redress Inquiry Program of the Department.

(d) FEDERAL AIR MARSHAL SERVICE COORDINATION.—

(1) IN GENERAL.—The Administrator of the Transportation Security Administration shall ensure that the Transportation Security Administration's intelligence-based screening rules are taken into account for Federal Air Marshal mission scheduling.

(2) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on how the Transportation Security Administration's intelligence-based screening rules are incorporated in the risk analysis conducted during the Federal Air Marshal mission scheduling process.

(e) GAO REPORT.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a study on the Transportation Security Administration's intelligence-based screening rules and the effectiveness of such rules in identifying and mitigating potential threats to aviation security. Such study shall also examine coordination between the Transportation Security Administration, the Department of Homeland Security, and other relevant partners relating to changing, updating, implementing, or suspending such rules as necessary.

SEC. 518. SCREENING IN AREAS OTHER THAN PASSENGER TERMINALS.

The Administrator of the Transportation Security Administration is authorized to provide screening services to a commercial charter air carrier in areas other than primary passenger terminals upon the request of such carrier. A commercial charter air carrier shall direct any such request to the Federal Security Director for the airport where such services are requested. A Federal Security Director may elect to provide screening services if such services are available. The Administrator shall enter into an agreement with a commercial charter air carrier for compensation from such carrier requesting the use of screening services for all reasonable costs in addition to overtime costs that are incurred in the provision of screening services under this section.

SEC. 519. FEDERAL AIR MARSHAL SERVICE AGREEMENTS.

(a) STANDARDIZATION.—Not later than 60 days after the date of the enactment of the Act, the Administrator of the Transportation Security Administration shall develop a standard working document that shall be the basis of all negotiations and agreements that begin after the date of the enactment of this Act between the United States and foreign governments or partners regarding Federal Air Marshal coverage of flights to and from the United States.

(b) WRITTEN AGREEMENTS.—All agreements between the United States and foreign governments or partners regarding the presence of Federal Air Marshals on flights to and from the United States must be written and signed by the Secretary of Homeland Security or the Secretary's designee.

(c) CONGRESSIONAL NOTIFICATION.—The Secretary of Homeland Security shall transmit to the relevant Congressional committees any agreements described in subsection (b) within 30 days of such agreement being signed.

SEC. 520. FEDERAL AIR MARSHAL MISSION SCHEDULING AUTOMATION.

The Administrator of the Transportation Security Administration shall seek to acquire an automated software capability for the scheduling of Federal Air Marshal Service missions based on current risk modeling.

SEC. 521. CANINE DETECTION RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—The Secretary of Homeland Security shall conduct an audit of all canine training programs of the Department of Homeland Security and convene a working group of representatives from all such programs to make recommendations on possible efficiencies that could be gained by integrating training standards and facilities.

(b) CANINE STAFFING ALLOCATION MODEL.—The Administrator of the Transportation Security Administration shall develop a staffing allocation model for canines to determine the optimal number of passenger screening canines at airports in the United States.

(c) REPORT TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the recommendations required by subsection (a).

(d) BRIEFING TO CONGRESS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall brief the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate on the state of explosives detection canine production and training in the United States.

(2) CONTENTS.—The briefing required under paragraph (1) shall include the following:

(A) An analysis of the steps the Transportation Security Administration may take to foster additional production of explosives detection canines in the United States by the private sector.

(B) Perspectives from current explosives detection canine industry stakeholders regarding the impact of the Administration's procurement model on business considerations.

(C) An analysis regarding whether the Administration effectively communicates canine training guidelines and testing methodology to the private sector.

(D) The extent to which physical capacity limitations at current Administration-operated sites hinder the operations of either the Administration or industry.

SEC. 522. INTERNATIONAL CIVIL AVIATION ORGANIZATION.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the United States Ambassador or the Chargé d'Affaires to the United States Mission to the International Civil Aviation Organization shall pursue improvements to airport security, including if practicable, introducing a resolution to raise minimum standards for airport security.

(b) REPORT TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act, the United States Ambassador or the Chargé d'Affaires to the United States Mission to the International Civil Aviation Organization shall report to the Committee on Homeland Security and the Committee on Foreign Affairs of the House of Representatives and the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, and the Committee on Commerce, Science, and Transportation of the Senate on the implementation of subsection (a).

SEC. 523. PASSENGER SECURITY FEE.

The Secretary of Homeland Security is prohibited from incorporating an increase in the passenger security fee under section 44940 of title 49, United States Code, beyond what is authorized at the time the annual budget proposal for the Department of Homeland Security is transmitted to Congress.

SEC. 524. LAST POINT OF DEPARTURE AIRPORT CERTIFICATION.

Subparagraph (B) of section 44907(a)(2) of title 49, United States Code, is amended by inserting ", including the screening and vetting of airport workers" before the semicolon at the end.

SEC. 525. SECURITY STANDARDS AT FOREIGN AIRPORTS.

Section 44907 of title 49, United States Code, is amended—

(1) in subsections (a) through (d), by striking "Secretary of Transportation" each place it appears and inserting "Secretary of Homeland Security"; and

(2) in subsection (e), in the matter preceding paragraph (1)—

(A) by striking "and 40106(b) of this title, the Secretary of Transportation, with the approval of the Secretary of State and without notice or a hearing, shall" and inserting "40106(b), and 41307 of this title, at the request of the Secretary of Homeland Security and with the approval of the Secretary of State and without notice or a hearing, the Secretary of Transportation shall"; and

(B) by striking "when the Secretary of Transportation decides" and inserting "when the Secretary of Homeland Security decides".

SEC. 526. SECURITY INCIDENT RESPONSE AT AIRPORTS AND SURFACE TRANSPORTATION HUBS.

The Gerardo Hernandez Airport Security Act of 2015 (Public Law 114–50; 49 U.S.C. 44903 note) is amended—

(1) in section 3—

(A) in subsection (b), in the matter preceding paragraph (1), by striking "may" each place it appears and inserting "shall";

(B) by redesignating subsection (c) as subsection (d); and

(C) by inserting after subsection (b) the following new subsection:

"(c) REVIEW.—The Administrator of the Transportation Security Administration shall review the active shooter response guidelines specified for Department of Homeland Security personnel under this section and make a recommendation to the Secretary of Homeland Security to modify such guidelines for personnel who are certified Federal law enforcement officials and for personnel who are uniformed but unarmed security officials."; and

(2) in section 7—

(A) in subsection (b), in the matter preceding paragraph (1), by striking "may" each place it appears and inserting "shall";

(B) by redesignating subsections (c) and (d) as subsections (d) and (e), respectively; and

(C) by inserting after subsection (b) the following new subsection:

"(c) REVIEW.—The Administrator of the Transportation Security Administration shall review the active shooter response guidelines specified for Department of Homeland Security personnel under this section and make a recommendation to the Secretary of Homeland Security to modify such guidelines for personnel who are certified Federal law enforcement officials and for personnel who are uniformed but unarmed security officials.".

SEC. 527. AIRPORT SECURITY SCREENING OPT-OUT PROGRAM.

Section 44920 of title 49, United States Code, is amended—

(1) in subsection (b)—

(A) in paragraph (1), by striking "120" and inserting "90";

(B) by redesignating paragraph (3) as paragraph (4);

(C) by inserting after paragraph (2) the following new paragraph:

"(3) ENTRANCE INTO CONTRACT.—The Administrator of the Transportation Security Administration shall make best efforts to enter into a contract with a private screening company to provide screening services at an airport not later than 180 days after the date of approval of an application submitted by the operator of such airport under subsection (a).''; and

(D) in subparagraph (A) of paragraph (4), as so redesignated, in the matter preceding clause (i), by striking "not later than 60 days following the date of the denial" and inserting "immediately upon issuing the denial"; and

(2) by striking subsection (h) and inserting the following new subsections:

"(h) EVALUATION OF SCREENING COMPANY PROPOSALS FOR AWARD.—Notwithstanding any other provision of law, including title 48 of the Code of Federal Regulations and the Federal Advisory Committee Act (5 U.S.C. App.), an airport operator that has applied and been approved to have security screening services carried out by a qualified private screening company under contract with the Administrator of the Transportation Security Administration may nominate to the head of the contracting activity an individual to participate in the evaluation of proposals for the award of such contract. Any such participation on a proposal evaluation committee shall be conducted in accordance with the provisions and restrictions of chapter 21 of title 41, United States Code.

"(i) INNOVATIVE SCREENING APPROACHES AND TECHNOLOGIES.—The operator of an airport at which screening services are provided under this section is encouraged to recommend to the Administrator of the Transportation Security Administration innovative screening approaches and technologies. Upon receipt of any such recommendations, the Administrator, shall review and, if appropriate, test, conduct a pilot project, and, if appropriate, deploy such approaches and technologies.".

SEC. 528. PERSONNEL MANAGEMENT SYSTEM REVIEW.

(a) IN GENERAL.—Notwithstanding subsection (d) of section 111 of the Aviation and Transportation Security Act (49 U.S.C. 44935 note), not later than 30 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall convene a working group consisting of representatives of the Administration and representatives of the labor organization representing security screening personnel to negotiate reforms to the Administration's personnel management system, including appeals to the Merit Systems Protection Board and grievance procedures.

(b) REPORT.—Not later than one year after the date of the enactment of this Act, the working group convened under subsection (a) shall submit to the Administrator of the Transportation Security Administration and the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report containing agreed-upon reforms to the Administration's personnel management system. The Administrator may implement associated recommendations mutually agreed to by the parties to such working group before the end of such one year period.

SEC. 529. INNOVATION TASK FORCE.

(a) IN GENERAL.—The Administrator of the Transportation Security Administration may establish a task force to collaborate with air carriers, airport operators, and other aviation security stakeholders to foster the pursuit of innovations in aviation security prior to the acquisition process.

(b) ACTIVITIES.—The task force authorized under subsection (a) may conduct activities designed to identify and develop an innovative technology or capability with the potential of enhancing aviation security, including—

(1) conducting a field demonstration of such a technology or capability in the airport environment;

(2) gathering performance data from such a demonstration to inform the acquisition process; and

(3) providing funding and promoting efforts to enable participation in a demonstration by a small business that has an innovative technology but does not have adequate resources to participate.

(c) COMPOSITION.—The task force authorized under subsection (a) shall be—

(1) chaired by the Administrator of the Transportation Security Administration's designee; and

(2) comprised of representatives appointed by the Administrator, in consultation with the Chairperson of the Aviation Security Advisory Committee (established pursuant to section 44936 of title 49, United States Code), from appropriate stakeholders from—

(A) within the Administration;

(B) air carriers;

(C) airport operators;

(D) other aviation security stakeholders; and

(E) as appropriate, the Science and Technology Directorate of the Department of Homeland Security and any other appropriate component of the Department.

(d) RULE OF CONSTRUCTION.—Nothing in this section shall require the Administrator of the Transportation Security Administration to acquire an innovative technology or emerging security capability.

(e) NON-APPLICABILITY OF FACA.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the task force authorized under subsection (a).

SEC. 530. AIRPORT LAW ENFORCEMENT REIMBURSEMENT.

Not later than 120 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the Transportation Security Administration's law enforcement officer reimbursement program, which shall include information relating to the following:

(1) The current structure of the program, including how funding disbursement decisions are made.

(2) An assessment of threats requiring law enforcement officer response at airports.

(3) The scope of current law enforcement activities covered under the program, and an assessment of whether such covered activities should be expanded to reflect emerging threats.

(4) The annual costs to airport authorities for providing law enforcement for such covered activities at security checkpoints.

(5) Proposed methodology for funding allocations.

Subtitle C—Transportation Security Screening Personnel Training and Accountability

SEC. 531. TRANSPORTATION SECURITY TRAINING PROGRAMS.

(a) IN GENERAL.—Section 44935 of title 49, United States Code, as amended by this Act, is further amended by adding at the end the following new subsection:

"(l) INITIAL AND RECURRING TRAINING.—

"(1) IN GENERAL.—The Administrator of the Transportation Security Administration shall establish a training program for new security screening personnel located at the Federal Law Enforcement Training Center in Glynco, Georgia.

"(2) RECURRING TRAINING.—Not later than 180 days after the date of the enactment of this subsection, the Administrator of the Transportation Security Administration shall establish recurring training of security screening personnel regarding updates to screening procedures and technologies, including methods to identify the verification of false or fraudulent travel documents, as well as training on emerging threats, in response to weaknesses identified in covert tests at airports. The training shall include—

"(A) internal controls for monitoring and documenting compliance of transportation security officers with such training requirements; and

"(B) such other matters as identified by the Administrator with regard to such training.".

(b) GAO STUDY.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall report to Congress on the effectiveness of the new security screening personnel training at Glynco, Georgia, required under subsection (l) of section 44935 of title 49, United States Code, as amended by this section.

SEC. 532. ALTERNATE NEW SECURITY SCREENING PERSONNEL TRAINING PROGRAM COST AND FEASIBILITY STUDY.

Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall conduct a cost and feasibility study of developing a training program for security screening personnel that will provide such personnel with an equal level of training as is provided in the training program for new security screening personnel located at the Federal Law Enforcement Training Center in Glynco, Georgia, that could be conducted at or within 50 miles of such security screening personnel's duty station. Such study should examine the use of online seminar and training platforms for portions of the training curriculum that are conducive to such an outcome.

SEC. 533. PROHIBITION OF ADVANCE NOTICE OF COVERT TESTING TO SECURITY SCREENERS.

Section 44935 of title 49, United States Code, as amended by this Act, is further amended by adding at the end the following new subsection:

"(m) PROHIBITION OF ADVANCE NOTICE TO SECURITY SCREENERS OF COVERT TESTING AND EVALUATION.—

"(1) IN GENERAL.—The Administrator of the Transportation Security Administration shall ensure, to the greatest extent practicable, that information concerning a covert test of a transportation security system to be conducted by a covert testing office, the Inspector General of the Department of Homeland Security, or the Government Accountability Office is not provided to any individual involved in such test prior to the completion of such test.

"(2) EXCEPTIONS.—Notwithstanding paragraph (1)—

"(A) an authorized individual involved in a covert test of a transportation security system may provide information concerning such covert test to—

"(i) employees, officers, and contractors of the Federal Government (including military personnel);

"(ii) employees and officers of State and local governments; and

"(iii) law enforcement officials who are authorized to receive or directed to be provided such information by the Administrator of the Transportation Security Administration, the Inspector General of the Department of Homeland Security, or the Comptroller General of the United States, as the case may be; and

"(B) for the purpose of ensuring the security of any individual in the vicinity of a site at which a covert test of a transportation security system is being conducted, an individual conducting such test may disclose his or her status as an individual conducting such test to any appropriate individual if a security screener or other individual who is not a covered employee identifies the individual conducting such test as a potential threat.

"(3) SPECIAL RULES FOR TSA.—

"(A) MONITORING AND SECURITY OF TESTING PERSONNEL.—The head of each covert testing office shall ensure that a person or group of persons conducting a covert test of a transportation security system for a covert testing office is accompanied at the site of such test by a cover team composed of one or more employees of such covert testing office for the purpose of monitoring such test and confirming the identity of personnel involved in such test under subparagraph (B).

"(B) RESPONSIBILITY OF COVER TEAM.—Under this paragraph, a cover team for a covert test of a transportation security system shall—

"(i) monitor such test; and

"(ii) for the purpose of ensuring the security of any individual in the vicinity of a site at which such test is being conducted, confirm, notwithstanding paragraph (1), the identity of any individual conducting such test to any appropriate individual if a security screener or other individual who is not a covered employee identifies the individual conducting such test as a potential threat.

"(C) AVIATION SCREENING.—Notwithstanding subparagraph (A), the Transportation Security Administration is not required to have a cover team present during a test of the screening of persons, carry-on items, or checked baggage at an aviation security checkpoint at or serving an airport if such test—

"(i) is approved, in coordination with the designated security official for the airport operator by the Federal Security Director for such airport; and

"(ii) is carried out under an aviation screening assessment program of the Department of Homeland Security.

"(D) USE OF OTHER PERSONNEL.—The Transportation Security Administration may use employees, officers, and contractors of the Federal Government (including military personnel) and employees and officers of State and

local governments or any personnel authorized by the Federal Security Director to conduct covert tests.

"(4) DEFINITIONS.—In this subsection, the following definitions apply:

"(A) APPROPRIATE INDIVIDUAL.—The term 'appropriate individual', as used with respect to—

"(i) a covert test under paragraph (2)(B) of a transportation security system, means any individual who the individual conducting such test determines needs to know his or her status as an individual conducting such test; or

"(ii) a covert test under paragraph (3)(B)(i), means any individual who the cover team monitoring such test determines needs to know the identity of such cover team.

"(B) COVERED EMPLOYEE.—The term 'covered employee' means any individual who receives notice of a covert test before the completion of a test under paragraph (2)(B).

"(C) COVERT TEST.—

"(i) IN GENERAL.—The term 'covert test' means an exercise or activity conducted by a covert testing office, the Inspector General of the Department of Homeland Security, or the Government Accountability Office to intentionally test, compromise, or circumvent transportation security systems to identify vulnerabilities in such systems.

"(ii) LIMITATION.—Notwithstanding clause (i), the term 'covert test' does not mean an exercise or activity by an employee or contractor of the Transportation Security Administration to test or assess compliance with relevant regulations.

"(D) COVERT TESTING OFFICE.—The term 'covert testing office' means any office of the Transportation Security Administration designated by the Administrator of the Transportation Security Administration to conduct covert tests of transportation security systems.

"(E) EMPLOYEE OF A COVERT TESTING OFFICE.—The term 'employee of a covert testing office' means an individual who is an employee of a covert testing office or a contractor or an employee of a contractor of a covert testing office.".

Subtitle D—Airport Access Controls and Perimeter Security

SEC. 541. REFORMATION OF CERTAIN PROGRAMS OF THE TRANSPORTATION SECURITY ADMINISTRATION.

(a) DEFINITIONS.—In this subtitle:

(1) AIR CARRIER.—The term "air carrier" has the meaning given such term in section 40102 of title 49, United States Code.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate.

(3) FOREIGN AIR CARRIER.—The term "foreign air carrier" has the meaning given such term in section 40102 of title 49, United States Code.

(4) 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)).

(5) SECURED AREA.—The term "secured area" has the meaning given such term in section 1540.5 of title 49, Code of Federal Regulations.

(6) SECURITY IDENTIFICATION DISPLAY AREA.—The term "Security Identification Display Area" has the meaning given such term in section 1540.5 of title 49, Code of Federal Regulations.

(7) STERILE AREA.—The term "sterile area" has the meaning given such term in section 1540.5 of title 49, Code of Federal Regulations.

(b) COST AND FEASIBILITY STUDY.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration, in consultation with the Aviation Security Advisory Committee (established under section 44946 of title 49, United States Code), shall submit to the appropriate congressional committees and the Comptroller General of the United States a cost and feasibility study of a statistically significant number of Category I, II, III, IV, and X airports assessing the impact if all employee access points from

non-secured areas to secured areas of such airports are comprised of the following:

(A) A secure door utilizing card and pin entry or biometric technology.

(B) Surveillance video recording, capable of storing video data for at least 30 days.

(C) Advanced screening technologies, including at least one of the following:

(i) Magnetometer (walk-through or hand-held).

(ii) Explosives detection canines.

(iii) Explosives trace detection.

(iv) Advanced imaging technology.

(v) X-ray bag screening technology.

(2) CONTENTS.—The study required under paragraph (1) shall include information related to the employee screening costs of those category I, II, III, IV, and X airports which have already implemented practices of screening 100 percent of employees accessing secured areas of airports, including the following:

(A) Costs associated with establishing an operational minimum number of employee entry and exit points.

(B) A comparison of estimated costs and effectiveness associated with implementing the security features specified in paragraph (1) to—

(i) the Federal Government; and

(ii) airports and the aviation community.

(3) COMPTROLLER GENERAL ASSESSMENT.—

(A) IN GENERAL.—Upon completion of the study required under paragraph (1), the Comptroller General of the United States shall review such study to assess the quality and reliability of such study.

(B) ASSESSMENT.—Not later than 90 days after the receipt of the study required under paragraph (1), the Comptroller General of the United States shall report to the appropriate congressional committees on the results of the review required under subparagraph (A).

(c) AIRPORT WORKER EDUCATION AND SECURITY AWARENESS.—

(1) COOPERATIVE EFFORTS TO ENHANCE AIRPORT SECURITY AWARENESS.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall work with air carriers, foreign air carriers, airport operators, labor unions representing credentialed employees, and the Aviation Security Advisory Committee to enhance security awareness of credentialed airport populations regarding insider threats to aviation security and recognized practices related to airport access controls.

(2) CREDENTIALING STANDARDS.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall, in consultation with air carriers, foreign air carriers, airport operators, labor unions representing credentialed employees, and the Aviation Security Advisory Committee, assess credentialing standards, policies, and practices to ensure that insider threats to aviation security are adequately addressed.

(B) REPORT.—Not later than 30 days after completion of the assessment required under subparagraph (A), the Administrator of the Transportation Security Administration shall report to the appropriate congressional committees on the results of such assessment.

(3) SIDA, STERILE AREA, AND AOA APPLICATIONS.—

(A) SOCIAL SECURITY NUMBERS REQUIRED.—Not later than 60 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall require the submission of a social security number for each individual applying for a Security Identification Display Area, Sterile Area, or Air Operations Area airport credential to strengthen security vetting effectiveness. An applicant who does not provide such applicant's social security number may be denied such a credential.

(B) SCREENING NOTICE.—The Administrator of the Transportation Security Administration shall issue requirements for airport operators to include in applications for access to a Security Identification Display Area, Sterile Area, or Air Operations Area a notice informing applicants that an employee holding a credential granting access to such an area may be screened at any time while gaining access to, working in, or leaving such an area.

(d) SECURING AIRPORT WORKER ACCESS.—

(1) IN GENERAL.—The Administrator of the Transportation Security Administration shall work with airport operators and the Aviation Security Advisory Committee to identify advanced technologies, including biometric identification

technologies, for securing employee access to the secured areas and sterile areas of airports.

(2) RAP BACK VETTING.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall ensure that all credentialed aviation worker populations currently requiring a fingerprint-based criminal record history check are continuously vetted through the Federal Bureau of Investigation's Rap Back Service, in order to more rapidly detect and mitigate insider threats to aviation security.

(3) INSIDER THREAT EDUCATION AND MITIGATION.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall identify means of enhancing the Transportation Security Administration's ability to leverage the resources of the Department of Homeland Security and the intelligence community to educate Administration personnel on insider threats to aviation security and how the Administration can better mitigate such insider threats.

(4) PLAYBOOK OPERATIONS.—The Administrator of the Transportation Security Administration shall ensure that Transportation Security Administration-led employee physical inspection efforts of aviation workers, known as Playbook operations, are targeted, strategic, and focused on providing the greatest level of security effectiveness.

(5) COVERT TESTING.—

(A) IN GENERAL.—The Administrator shall conduct covert testing of Transportation Security Administration-led employee inspection operations at airports and measure existing levels of security effectiveness. The Administrator of the Transportation Security Administration shall provide—

(i) the results of such testing to the airport operator for the airport that is the subject of any such testing, and, as appropriate, to air carriers and foreign air carriers that operate at the airport that is the subject of such testing; and

(ii) recommendations and technical assistance for air carriers, foreign air carriers, and airport operators to conduct their own employee inspections, as needed.

(B) ANNUAL REPORTING.—The Administrator of the Transportation Security Administration shall annually, for each of fiscal years 2018 through 2022, submit to the appropriate congressional committees report on the frequency, methodology, strategy, and effectiveness of employee inspection operations at airports.

(6) CENTRALIZED DATABASE.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration, in consultation with the Aviation Security Advisory Committee, shall—

(A) establish a national database of individuals who have had either their airport or airport operator-issued badge revoked for failure to comply with aviation security requirements;

(B) determine the appropriate reporting mechanisms for air carriers, foreign air carriers, and airport operators to—

(i) submit to the Administrator data regarding individuals described in subparagraph (A); and

(ii) access the database established pursuant to such subparagraph; and

(C) establish a process to allow individuals whose names were mistakenly entered into such database to correct the record and have their names removed from such database.

(e) INSIDER THREAT COORDINATION EFFORTS.—The Department of Homeland Security is the lead interagency coordinator pertaining to insider threat investigations and mitigation efforts at airports. The Department shall make every practicable effort to coordinate with other relevant Government entities, as well as the security representatives of air carriers, foreign air carriers, and airport operators, as appropriate, when undertaking such investigations and efforts.

(f) AIRPORT TASK FORCES.—The Secretary of Homeland Security is authorized, through the Director of U.S. Immigration and Customs Enforcement, to form airport task forces using Homeland Security Investigations personnel and any other Department of Homeland Security personnel the Secretary determines necessary. Such airport task forces shall investigate and mitigate insider threats to aviation security, in coordination with Federal, State, local, tribal, and territorial law enforcement partners, as appropriate.

(g) INFORMATION TECHNOLOGY SECURITY.—Not later than 90 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall submit to the appropriate congressional committees a plan to con-

duct recurring reviews of the operational, technical, and management security controls for Administration information technology systems at airports.

SEC. 542. AIRPORT PERIMETER AND ACCESS CONTROL SECURITY.

(a) RISK ASSESSMENTS OF AIRPORT SECURITY.—

(1) IN GENERAL.—The Administrator of the Transportation Security Administration shall—

(A) not later than 120 days after the date of the enactment of this Act, update the Transportation Sector Security Risk Assessment (TSSRA) for the aviation sector; and

(B) not later than 180 days after such date—

(i) update with the latest and most currently available intelligence information the Comprehensive Risk Assessment of Perimeter and Access Control Security (in this section referred to as the "Risk Assessment of Airport Security") and determine a regular timeframe and schedule for further updates to such Risk Assessment of Airport Security; and

(ii) conduct a system-wide assessment of airport access control points and airport perimeter security, including cargo facilities.

(2) CONTENTS.—The security risk assessments required under paragraph (1)(B) shall

(A) include updates reflected in the TSSRA and Joint Vulnerability Assessment (JVA) findings;

(B) reflect changes to the risk environment relating to airport access control points and airport perimeters;

(C) use security breach data for specific analysis of system-wide trends related to airport access control points and airport perimeter security to better inform risk management decisions; and

(D) take into consideration the unique geography of and current recognized practices used by airports to mitigate potential vulnerabilities.

(3) REPORT.—The Administrator of the Transportation Security Administration shall report to the appropriate congressional committees, relevant Federal departments and agencies, and airport operators on the results of the security risk assessments required under paragraph (1).

(b) AIRPORT SECURITY STRATEGY DEVELOPMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall update the 2012 National Strategy for Airport Perimeter and Access Control Security (in this section referred to as the "National Strategy").

(2) CONTENTS.—The update to the National Strategy required under paragraph (1) shall include

(A) information from the Risk Assessment of Airport Security; and

(B) information on—

(i) airport security-related activities;

(ii) the status of efforts by the Transportation Security Administration to address the goals and objectives referred to in subsection (a);

(iii) finalized outcome-based performance measures and performance levels for each relevant activity and goal and objective under subparagraphs (A) and (B); and

(iv) input from airport operators.

(3) UPDATES.—Not later than 90 days after the update is completed under paragraph (1), the Administrator of the Transportation Security Administration shall implement a process for determining when additional updates to the strategy referred to in such subsection are needed.

SEC. 543. EXIT LANE SECURITY.

There is authorized $77,000,000 for each of fiscal years 2018 and 2019 to carry out subsection (n)(1) of section 44903 of title 49, United States Code.

SEC. 544. REIMBURSEMENT FOR DEPLOYMENT OF ARMED LAW ENFORCEMENT PERSONNEL AT AIRPORTS.

There is authorized $45,000,000 for each of fiscal years 2018 and 2019 to carry out subsection (h) of section 44901 of title 49, United States Code.

Subtitle E—Air Cargo Security

SEC. 551. AIR CARGO ADVANCE SCREENING PROGRAM.

(a) IN GENERAL.—Subtitle B of title IV of the Homeland Security Act of 2002 (6 U.S.C. 211 et seq.) is amended by adding at the end the following new section:

"SEC. 420. AIR CARGO ADVANCE SCREENING PROGRAM.

"(a) IN GENERAL.—The Secretary, consistent with the requirements of the Trade Act of 2002 (Public Law 107–210) shall—

"(1) establish an air cargo advance screening program (in this section referred to as the 'ACAS Program') for the collection by U.S. Customs and Border Protection of advance electronic information from air carriers and other persons and governments within the supply chain regarding cargo being transported to the United States by air;

"(2) under such program, require that such information be transmitted by such air carriers and other persons and governments at the earliest point practicable prior to loading of such cargo onto an aircraft destined to or transiting through the United States;

"(3) establish appropriate communications systems with freight forwarders, shippers, and air carriers;

"(4) establish a system that will allow freight forwarders, shippers, and air carriers to provide shipment level data for air cargo, departing from any location that is inbound to the United States; and

"(5) coordinate with the Administrator of the Transportation Security Administration to identify opportunities in which the information furnished in compliance with the ACAS Program could be used by the Administrator.

"(b) INSPECTION OF HIGH-RISK CARGO.—Under the ACAS Program, the Secretary shall ensure that all cargo that has been identified as high-risk is inspected prior to loading of such cargo onto aircraft at the last point of departure before departing for the United States.

"(c) CONSULTATION.—In carrying out the ACAS Program, the Secretary shall consult with relevant stakeholders, as appropriate, to ensure that an operationally feasible and practical approach to the collection of advance information with respect to cargo on aircraft departing for the United States recognizes the significant differences among air cargo business models and modes of transportation.

"(d) ANALYSIS.—The Secretary may analyze the information referred to in subsection (a) in the Department's automated targeting system and integrate such information with other intelligence to enhance the accuracy of the risk assessment process under the ACAS Program.

"(e) NO DUPLICATION.—The Secretary shall carry out this section in a manner that, after the ACAS Program is fully in effect, does not duplicate other programs or requirements relating to the submission of air cargo data.

"(f) CONSIDERATION OF INDUSTRY.—In carrying out the ACAS Program, the Secretary shall—

"(1) take into consideration that the content and timeliness of the available data may vary among entities in the air cargo industry and among countries, and shall explore procedures to accommodate such variations while maximizing the contribution of such data to the risk assessment process under the ACAS Program;

"(2) test the business processes, technologies, and operational procedures required to provide advance information with respect to cargo on aircraft departing for the United States, while ensuring delays and other negative impacts on vital supply chains are minimized; and

"(3) consider the cost, benefit, and feasibility before establishing any set time period for submission of certain elements of the data for air cargo under this section in line with the regulatory guidelines specified in Executive Order 13563, and any successor Executive Order or regulation.

"(g) GUIDANCE.—The Secretary shall provide guidance for participants in the ACAS Program regarding the requirements for participation, including requirements for transmitting shipment level data.

"(h) USE OF DATA.—The Secretary shall use the data provided under the ACAS Program for targeting shipments for screening and law enforcement purposes only.".

(b) FINAL RULE.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall issue a final regulation to implement the ACAS Program under section 420 of the Homeland Security Act of 2002 (as added by subsection (a) of this section) to include the electronic transmission to the Department of Homeland Security of data elements for targeting cargo, including appropriate security elements of shipment level data, as determined by the Secretary.

(c) REPORT.—Not later than 180 days after the date of the commencement of the ACAS Program under section 420 of the Homeland Security Act of 2002 (as added by subsection (a) of this section), the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a report detailing the oper-

ational implementation of providing advance information under the ACAS Program and the value of such information in targeting cargo.

(d) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 419 the following new item:

"Sec. 420. Air cargo advance screening program.".

SEC. 552. EXPLOSIVES DETECTION CANINE TEAMS FOR AIR CARGO SECURITY.

Section 1307 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1116) is amended by adding at the end the following new subsection:

"(h) EXPLOSIVES DETECTION CANINE TEAMS FOR AIR CARGO SECURITY.—

"(1) IN GENERAL.—In order to enhance the screening of air cargo and ensure that third-party explosives detection canine assets are leveraged for such purpose, the Administrator shall, not later than 180 days after the date of the enactment of this subsection—

"(A) develop and issue standards for the use of such third-party explosives detection canine assets for the primary screening of air cargo;

"(B) develop a process to identify qualified non-Federal entities that will certify canine assets that meet the standards established by the Administrator pursuant to subparagraph (A);

"(C) ensure that entities qualified to certify canine assets shall be independent from entities that will train and provide canines to end users of such canine assets;

"(D) establish a system of Transportation Security Administration audits of the process developed pursuant to subparagraph (B); and

"(E) provide that canines certified for the primary screening of air cargo can be used by air carriers, foreign air carriers, freight forwarders, and shippers.

"(2) IMPLEMENTATION.—Upon completion of the development of the process under subsection (a), the Administrator shall—

"(A) facilitate the deployment of such assets that meet the certification standards of the Administration, as determined by the Administrator;

"(B) make such standards available to vendors seeking to train and deploy third-party explosives detection canine assets; and

"(C) ensure that all costs for the training and certification of canines, and for the use of supplied canines, are borne by private industry and not the Federal Government.

"(3) DEFINITIONS.—In this subsection:

"(A) AIR CARRIER.—The term 'air carrier' has the meaning given such term in section 40102 of title 49, United States Code.

"(B) FOREIGN AIR CARRIER.—The term 'foreign air carrier' has the meaning given such term in section 40102 of title 49, United States Code.

"(C) THIRD-PARTY EXPLOSIVES DETECTION CANINE ASSETS.—The term 'third-party explosives detection canine assets' means any explosives detection canine or handler not owned or employed, respectively, by the Administration.".

Subtitle F—Information Sharing and Cybersecurity

SEC. 561. INFORMATION SHARING AND CYBERSECURITY.

(a) FEDERAL SECURITY DIRECTORS.—Section 44933 of title 49, United States Code, is amended by adding at the end the following new subsection:

"(c) INFORMATION SHARING.—Not later than one year after the date of the enactment of this subsection, the Administrator shall—

"(1) require each Federal Security Director of an airport to meet at least quarterly with the airport director, airport security coordinator, and law enforcement agencies serving each such airport to discuss incident management protocols, including the resolution of screening anomalies at passenger screening checkpoints; and

"(2) require each Federal Security Director at an airport to inform, consult, and coordinate, as appropriate, with the respective airport security coordinator in a timely manner on security matters impacting airport operations and to establish and maintain operational protocols with such airport operators to ensure coordinated responses to security matters.".

(b) PLAN TO IMPROVE INFORMATION SHARING.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Administrator of the Transportation Security Administration, shall develop a plan to improve intelligence information sharing with State and local transportation entities that includes best practices to ensure that the information shared is actionable, useful, and not redundant.

(2) CONTENTS.—The plan required under subsection (a) shall include the following:

(A) The incorporation of best practices for information sharing.

(B) The identification of areas of overlap and redundancy.

(C) An evaluation and incorporation of stakeholder input in the development of such plan.

(D) The integration of recommendations of the Comptroller General of the United States on information sharing.

(3) SOLICITATION.—The Administrator shall solicit on an annual basis input from appropriate stakeholders, including State and local transportation entities, on the quality and quantity of intelligence received by such stakeholders relating to information sharing.

(c) BEST PRACTICES SHARING.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Administrator of the Transportation Security Administration, shall establish a mechanism to share with State and local transportation entities best practices from across the law enforcement spectrum, including Federal, State, local, and tribal entities, that relate to employee training, employee professional development, technology development and deployment, hardening tactics, and passenger and employee awareness programs.

(2) CONSULTATION.—The Administrator of the Transportation Security Administration shall solicit and incorporate stakeholder input—

(A) in developing the mechanism for sharing best practices as required under paragraph (1); and

(B) not less frequently than once each year on the quality and quantity of information such stakeholders receive through the mechanism established under such subsection.

(d) CYBERSECURITY.—

(1) IN GENERAL.—The Secretary of Homeland Security shall—

(A) not later than 120 days after the date of the enactment of this Act, develop and implement a cybersecurity risk assessment model for aviation security, consistent with the National Institute of Standards and Technology Framework for Improvement Critical Infrastructure Cybersecurity and any update to such Framework pursuant to section 2 of the National Institute of Standards and Technology Act (15 U.S.C. 272), to evaluate current and future cybersecurity risks;

(B) evaluate, on a periodic basis, but not less often than once every two years, the effectiveness of the cybersecurity risk assessment model under subparagraph (A);

(C) seek to ensure participation of at least one information sharing and analysis organization (as such term is defined in section 212 of the Homeland Security Act of 2002 (6 U.S.C. 131)) representing the aviation community in the national cybersecurity and communications integration center, pursuant to subsection (d)(1)(B) of section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148);

(D) establish guidelines for voluntary reporting of aviation-related cybersecurity risks and incidents to the national cybersecurity and communications integration center under section 227 of the Homeland Security Act of 2002, and other appropriate Federal agencies; and

(E) request the Aviation Security Advisory Committee established pursuant to section 44946 of title 49, United States Code, to report and make recommendations to the Secretary on enhancing the sharing of information related to aviation-related cybersecurity risks and incidents between relevant Federal, state, local, tribal, and territorial entities and the aviation stakeholder community.

(2) CYBERSECURITY ENHANCEMENTS TO AVIATION SECURITY ACTIVITIES.—The Secretary of Homeland Security, in consultation with the Secretary of Transportation, shall—

(A) direct the sharing of information concerning cybersecurity risks and incidents to address aviation-specific risks; and

(B) upon request, conduct cybersecurity vulnerability assessments for airports and air carriers.

(3) TSA DATABASE CYBER ASSESSMENT.—

(A) ASSESSMENT REQUIRED.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security shall evaluate the cybersecurity of the Transportation Security Administration databases for trusted traveler and credentialing programs that contain personal information of specific individuals or information that identifies specific individuals, including the Transportation Worker Identification Credential and Pre-Check trusted traveler programs, and the means for transmission of data to and from such databases and develop information on any identified cybersecurity vulnerabilities and remediation plans to address such vulnerabilities;

(B) SUBMISSION TO CONGRESS.—Not later than 30 days after the completion of the evaluation required under subparagraph (A), the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate information relating to such evaluation. Such submission shall be provided in a classified form.

(C) SUBMISSION OF SUPPLEMENTARY INFORMATION.—Not later than 90 days after the completion of such evaluation, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate supplementary information relating to such evaluation, including information relating to any identified cybersecurity vulnerabilities and remediation plans to address such vulnerabilities. Such submission shall be provided in a classified form.

(4) DEFINITIONS.—In this subsection, the terms "cybersecurity risk" and "incident" have the meanings given such terms in section 227 of the Homeland Security Act of 2002.

Subtitle G—Surface Transportation Security

SEC. 571. DEFINITIONS.

In this subtitle:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

(2) EXPLOSIVES DETECTION CANINE TEAM.—The term "explosives detection canine team" means a canine and a canine handler trained to detect explosives and other threats as determined by the Secretary.

(3) RISK.—The term "risk" means the potential for an unwanted outcome resulting from an accident, event, or occurrence, as determined by its likelihood and the associated consequences.

(4) THREAT.—The term "threat" means an individual, entity, action, or natural or manmade occurrence that has or indicates the potential to harm life, information, operations, the environment, or property.

(5) VULNERABILITY.—The term "vulnerability" means a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

SEC. 572. SURFACE TRANSPORTATION SECURITY ASSESSMENT AND IMPLEMENTATION OF RISK-BASED STRATEGY.

(a) SECURITY ASSESSMENT.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall complete an assessment of the vulnerabilities of and risks to surface transportation systems, including findings from similar vulnerability analyses completed within three years of the date of the enactment of this Act.

(2) CONSIDERATIONS.—In conducting the security assessment under paragraph (1), the Secretary of Homeland Security shall, at a minimum—

(A) consider appropriate intelligence;

(B) consider security breaches and attacks at domestic and international transportation facilities;

(C) consider the vulnerabilities and risks associated with specific modes of surface transportation systems;

(D) evaluate the vetting and security training of—

(i) employees in surface transportation systems; and

(ii) other individuals with access to sensitive or secure areas of transportation systems; and

(E) consider input from—

(i) representatives of different modes of surface transportation systems;

(ii) subject to paragraph (3)—

(I) critical infrastructure entities; and

(II) the Transportation Systems Sector Coordinating Council; and

(iii) the heads of other relevant Federal departments or agencies.

(b) RISK-BASED SECURITY STRATEGY.—

(1) IN GENERAL.—Not later than 180 days after the date the security assessment under subsection (a) is complete, the Secretary of Homeland Security shall use the results of such assessment—

(A) to develop and implement a cross-cutting, risk-based security strategy that includes—

(i) all surface transportation systems;

(ii) a mitigating strategy that aligns with each vulnerability and risk identified in subsection (a);

(iii) a planning process to inform resource allocation;

(iv) priorities, milestones, and performance metrics to measure the effectiveness of such risk-based security strategy; and

(v) processes for sharing relevant and timely intelligence threat information with appropriate stakeholders;

(B) to develop a management oversight strategy that—

(i) identifies the parties responsible for the implementation, management, and oversight of the risk-based security strategy under subparagraph (A); and

(ii) includes a plan for implementing such risk-based security strategy; and

(C) to modify the risk-based budget and resource allocations, in accordance with section 573(c), for the Transportation Security Administration.

(2) COORDINATED APPROACH.—In developing and implementing the risk-based security strategy under paragraph (1)(A), the Secretary of Homeland Security shall coordinate with the heads of other relevant Federal departments or agencies, and stakeholders, as appropriate—

(A) to evaluate existing surface transportation security programs, policies, and initiatives, including the explosives detection canine teams, for consistency with the risk-based security strategy and, to the extent practicable, avoid any unnecessary duplication of effort;

(B) to determine the extent to which stakeholder security programs, policies, and initiatives address the vulnerabilities and risks to surface transportation systems identified in subsection (a); and

(C) subject to subparagraph (B), to mitigate each such vulnerability and risk.

(c) REPORT.—

(1) IN GENERAL.—Not later than one year after the date the security assessment under subsection (a) is complete, the Secretary of Homeland Security shall submit to the appropriate congressional committees and the Inspector General of the Department of Homeland Security a report that—

(A) describes the process used to complete such security assessment;

(B) describes the process used to develop the risk-based security strategy under subsection (b)(1)(A);

(C) describes such risk-based security strategy;

(D) includes the management oversight strategy under subsection (b)(1)(B);

(E) includes—

(i) the findings of such security assessment;

(ii) a description of the actions recommended or taken by the Department or another Federal department or agency to mitigate the vulnerabilities and risks identified in subsection (a);

(iii) any recommendations for improving the coordinated approach to mitigating vulnerabilities and risks to surface transportation systems; and

(iv) any recommended changes to the National Infrastructure Protection Plan developed pursuant to Homeland Security Presidential Directive–7, the modal annexes to such plan, or relevant surface transportation security programs, policies, or initiatives; and

(F) may contain a classified annex.

(2) PROTECTIONS.—In preparing the report required under paragraph (1), the Secretary of Homeland Security shall take appropriate actions to safeguard information described by section 552(b) of title 5, United States Code, or protected from disclosure by any other law of the United States.

(d) UPDATES.—Not less frequently than semiannually, the Secretary of Homeland Security shall report to or brief the appropriate congressional committees on the vulnerabilities of and risks to surface transportation systems and how such vulnerabilities and risks affect the risk-based security strategy under subsection (b)(1)(A).

SEC. 573. RISK-BASED BUDGETING AND RESOURCE ALLOCATION.

(a) REPORT.—In conjunction with the submission of the Department's annual budget request to the Office of Management and Budget, the Administrator of the Transportation Security Administration shall submit to the appropriate congressional committees a report that describes a risk-based budget and resource allocation plan for surface transportation sectors, within and across modes, that—

(1) reflects the risk-based security strategy under section 572(b)(1)(A); and

(2) is organized by appropriations account, program, project, and initiative.

(b) BUDGET TRANSPARENCY.—Subsection (a) of section 1105 of title 31, United States Code, is amended by adding at the end the following new paragraph:

"(40) a separate statement clearly distinguishing the resources requested for surface transportation security from the resources requested for aviation security.".

(c) RESOURCE REALLOCATION.—

(1) IN GENERAL.—Not later than 15 days after the date on which the Transportation Security Administration allocates any resources or personnel, including personnel sharing, detailing, or assignment, or the use of facilities, technology systems, or vetting resources, for a non-transportation security purpose or National Special Security Event (as defined in section 2001 of Homeland Security Act of 2002 (6 U.S.C. 601)), the Secretary of Homeland Security shall provide to the appropriate congressional committees the notification described in paragraph (2).

(2) NOTIFICATION.—A notification described in this paragraph shall include—

(A) the reason for and a justification of the resource or personnel allocation at issue;

(B) the expected end date of such resource or personnel allocation; and

(C) the projected cost to the Transportation Security Administration of such personnel or resource allocation.

SEC. 574. SURFACE TRANSPORTATION SECURITY MANAGEMENT AND INTERAGENCY COORDINATION REVIEW.

(a) REVIEW.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall—

(1) review the staffing, budget, resource, and personnel allocation, and management oversight strategy of the Transportation Security Administration's surface transportation security programs;

(2) review the coordination between relevant entities of leadership, planning, policy, inspections, and implementation of security programs relating to surface transportation to reduce redundancy and regulatory burden; and

(3) submit to the appropriate congressional committees a report on the findings of the reviews under paragraphs (1) and (2), including any recommendations for improving coordination between relevant entities and reducing redundancy and regulatory burden.

(b) RELEVANT ENTITIES DEFINED.—In this section, the term "relevant entities" means—

(1) the Transportation Security Administration;

(2) other Federal, State, or local departments or agencies with jurisdiction over a mode of surface transportation;

(3) critical infrastructure entities;

(4) the Transportation Systems Sector Coordinating Council; and

(5) relevant stakeholders.

SEC. 575. TRANSPARENCY.

(a) REGULATIONS.—Not later than 180 days after the date of the enactment of this Act and every 180 days thereafter, the Administrator of the Transportation Security Administration shall make available through a public website information regarding the status of each regulation relating to surface transportation security that is directed by law to be issued but that has not been issued if more than two years have passed since the date of enactment of each such law.

(b) INSPECTOR GENERAL REVIEW.—Not later than 180 days after the date of the enactment of this Act and every two years thereafter until all of the requirements under titles XIII, XIV, and XV of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1111 et seq.) and under this Act have been fully implemented, the Inspector General of the Department of Homeland Security shall submit to the appropriate congressional committees a report that—

(1) identifies the requirements under such titles of such Act and under this Act that have not been fully implemented;

(2) describes what, if any, additional action is necessary; and

(3) includes recommendations regarding whether any of such requirements should be amended or repealed.

SEC. 576. TSA COUNTERTERRORISM ASSET DEPLOYMENT.

(a) IN GENERAL.—The Administrator of the Transportation Security Administration is authorized to maintain 30 Visible Intermodal Prevention and Response (VIPR) teams for deployment, at the request of and in collaboration with Federal, State, and local transportation stakeholders, to prevent and deter acts of terrorism against United States transportation systems and for other counterterrorism purposes. Starting in January 2019 and for five years thereafter, the Administrator shall annually assess whether the number of VIPR teams is adequate to respond to requests for collaboration from Federal, State, and local transportation stakeholders and to carry out counterterrorism activities with respect to United States transportation systems.

(b) CONGRESSIONAL NOTIFICATION.—If the Administrator of the Transportation Security Administration determines that the number of VIPR teams should be reduced below 30, the Administrator shall notify the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate not later than 90 days prior to such a determination.

(c) REPORT TO CONGRESS.—Not later than 60 days after the development and implementation of the performance measures and objectives required under subsection (f), the Administrator of the Transportation Security Administration shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on the appropriate number of VIPR teams needed by the Administration.

(d) STAKEHOLDER NOTIFICATION.—If the Transportation Security Administration deploys any counterterrorism personnel or resource, such as explosive detection assets, property inspections, or patrols by VIPR teams, to enhance security at a surface transportation system or surface transportation facility for a period of not less than 180 consecutive days, the Administrator shall provide sufficient notification to the system or facility operator, as applicable, not less than 14 days prior to terminating the deployment.

(e) EXCEPTION.—Subsection (d) shall not apply if the Administrator of the Transportation Security Administration—

(1) determines there is an urgent security need for the personnel or resource described in such subsection; and

(2) notifies the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

(f) VIPR TEAMS.—Section 1303 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1112) is amended—

(1) in subsection (a)(4), by striking "team," and inserting "team as to specific locations and times within the facilities of such entities at which VIPR teams are to be deployed to maximize the effectiveness of such deployment,"; and

(2) by striking subsection (b) and inserting the following new subsections:

"(b) PERFORMANCE MEASURES.—Not later than one year after the date of the enactment of this subsection, the Administrator shall develop and implement a system of qualitative performance measures and objectives by which to assess the roles, activities, and effectiveness of VIPR team operations on an ongoing basis, including a mechanism through which the transportation entities referred to in subsection (a)(4) may submit feedback on VIPR team operations involving their systems or facilities.

"(c) PLAN.—Not later than one year after the date of the enactment of this section, the Administrator shall develop and implement a plan for ensuring the interoperability of communications among VIPR team participants and between VIPR teams and any transportation entities with systems or facilities that are involved in VIPR team operations. Such plan shall include an analysis of the costs and resources required to carry out such plan.".

SEC. 577. SURFACE TRANSPORTATION SECURITY ADVISORY COMMITTEE.

(a) IN GENERAL.—Subchapter II of chapter 449 of title 49, United States Code, is amended by adding at the end the following new section:

"§ 44947. Surface Transportation Security Advisory Committee

"(a) ESTABLISHMENT.—The Administrator of the Transportation Security Administration (referred to in this section as the '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; and

"(iii) 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, 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 two 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 CERTAIN INFORMATION.—The Administrator may remove any member of the Advisory Committee who 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 may not receive any compensation from the Government by reason of their service on the Advisory Committee.

"(6) MEETINGS.—

"(A) IN GENERAL.—The Advisory Committee shall meet at least semiannually in person or through web conferencing, and may convene additional meetings as necessary.

"(B) PUBLIC MEETINGS.—At least one 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 Federal law, minutes of the meetings of the Advisory Committee 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 information or sensitive security information in accordance with law.

"(7) VOTING MEMBER ACCESS TO CLASSIFIED INFORMATION 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 but before such voting member may be granted any access to classified information or sensitive security information, the Administrator shall determine if such 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, such voting member may be granted access to sensitive security information that is relevant to such 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 of such information.

"(8) JOINT COMMITTEE MEETINGS.—The Advisory Committee may meet with one 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 to the Administrator reports 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 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 annual report that provides information on the activities, findings, and recommendations of the Advisory Committee during the preceding year.

"(B) PUBLICATION.—Not later than six months after the date that the Administrator receives an annual report under subparagraph (A), the Administrator shall publish a public version of such 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 efforts.

"(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 such recommendation, including—

"(A) if the Administrator agrees with such 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 such recommendation; or

"(B) if the Administrator disagrees with such recommendation, a justification for such disagreement.

"(3) NOTICES.—Not later than 30 days after the date the Administrator submits feedback under paragraph (2), the Administrator shall—

"(A) notify 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 of such feedback, including the agreement or disagreement under subparagraph (A) or subparagraph (B) of such paragraph, as applicable; and

"(B) provide the committees specified in subparagraph (A) 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 such recommendation is fully implemented, the Administrator shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a report or post on the public website under paragraph (5) an update on the status of such recommendation.

"(5) WEBSITE.—The Administrator shall maintain a public website that—

"(A) lists the members of the Advisory Committee;

"(B) provides the contact information for the Advisory Committee; and

"(C) information relating to meetings, minutes, annual reports, and the implementation of recommendations under this section.

"(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.".

(b) ADVISORY COMMITTEE MEMBERS.—

(1) VOTING MEMBERS.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall appoint the voting members of the Surface Transportation Security Advisory Committee established under section 44947 of title 49, United States Code, as added by subsection (a) of this section.

(2) NONVOTING MEMBERS.—Not later than 90 days after the date of the enactment of this Act, each Federal Government department and agency with regulatory authority over a mode of surface transportation, as the Administrator of the Transportation Security Administration considers appropriate, shall designate an appropriate representative to serve as a nonvoting member of the Surface Transportation Security Advisory Committee.

(c) CLERICAL AMENDMENT.—The analysis for chapter 449 of title 49, United States Code, is amended by inserting after the item relating to section 44946 the following new item:

"44947. Surface Transportation Security Advisory Committee.".

SEC. 578. REVIEW OF THE EXPLOSIVES DETECTION CANINE TEAM PROGRAM.

(a) IN GENERAL.—Not later than 90 days after the date that the Inspector General of the Department of Homeland Security receives the report under section 572(c), the Inspector General shall—

(1) review the explosives detection canine team program of the Department, including—

(A) the development by the Transportation Security Administration of a deployment strategy for explosives detection canine teams;

(B) the national explosives detection canine team training program, including canine training, handler training, refresher training, and updates to such training; and

(C) the use of the canine assets during an urgent security need, including the reallocation of such program resources outside the transportation systems sector during an urgent security need; and

(2) submit to the appropriate congressional committees a report on such review, including any recommendations.

(b) CONSIDERATIONS.—In conducting the review of the deployment strategy under subsection (a)(1)(A), the Inspector General of the Department of Homeland Security shall consider whether the Transportation Security Administration's method to analyze the risk to transportation facilities and transportation systems is appropriate.

SEC. 579. EXPANSION OF NATIONAL EXPLOSIVES DETECTION CANINE TEAM PROGRAM.

(a) IN GENERAL.—The Secretary of Homeland Security, where appropriate, shall encourage State, local, and tribal governments and private owners of high-risk transportation facilities to strengthen security through the use of explosives detection canine teams.

(b) INCREASED CAPACITY.—

(1) IN GENERAL.—Before the date the Inspector General of the Department of Homeland Security submits the report under section 578, the Administrator of the Transportation Security Administration may increase the number of State and local surface and maritime transportation explosives detection canine teams by not more than 70 such teams.

(2) ADDITIONAL TEAMS.—Beginning on the date the Inspector General of the Department of Homeland Security submits the report under section 578, the Secretary of Homeland Security may increase the State and local surface and maritime transportation explosives detection canine teams by not more than 200 such teams unless more of such teams are needed as identified in the risk-based security strategy under section 572(b)(1)(A), consistent with section 573 or with the President's most recent budget submitted under section 1105 of title 31, United States Code.

(3) RECOMMENDATIONS.—Before initiating any increase in the number of explosives detection teams under paragraph (2), the Secretary of Homeland Security shall consider any recommendations in the report under section 578 on the efficacy and management of the explosives detection canine program of the Department of Homeland Security.

(c) DEPLOYMENT.—The Secretary of Homeland Security shall—

(1) use any additional explosives detection canine teams, as described in subsection (b)(1), as part of the Department of Homeland Security's efforts to strengthen security across the Nation's surface and maritime transportation systems;

(2) make available explosives detection canine teams to all modes of transportation, subject to the requirements under section 576, to address specific vulnerabilities or risks, on an as-needed basis and as otherwise determined appropriate by the Secretary; and

(3) consider specific needs and training requirements for explosives detection canine teams to be deployed across the Nation's surface and maritime transportation systems, including in venues of multiple modes of transportation, as the Secretary considers appropriate.

SEC. 580. EXPLOSIVE DETECTION TECHNOLOGY.

The Secretary of Homeland Security shall prioritize the research and facilitation of next generation technologies to detect explosives in the Nation's surface transportation systems.

SEC. 581. STUDY ON SECURITY STANDARDS AND BEST PRACTICES FOR UNITED STATES AND FOREIGN PASSENGER TRANSPORTATION SYSTEMS.

(a) IN GENERAL.—The Comptroller General of the United States shall conduct a study of how the Transportation Security Administration—

(1) identifies and compares—

(A) United States and foreign passenger transportation system security standards; and

(B) best practices for protecting passenger transportation systems, including shared terminal facilities, and cyber systems; and

(2) disseminates to stakeholders the findings under paragraph (1).

(b) REPORT.—Not later than 18 months after the date of the enactment of this Act, the Comptroller General of the United States shall issue a report that contains—

(1) the findings of the study conducted under subsection (a); and

(2) any recommendations for improving relevant processes or procedures.

SEC. 582. AMTRAK SECURITY UPGRADES.

(a) RAILROAD SECURITY ASSISTANCE.—Subsection (b) of section 1513 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1163) is amended—

(1) in paragraph (1), by inserting before the period at the end the following: ", including communications interoperability where appropriate with relevant outside agencies and entities";

(2) in paragraph (5), by striking "security of" and inserting "security and preparedness of";

(3) in paragraph (7), by striking "security threats" and inserting "security threats and preparedness, including connectivity to the National Terrorist Screening Center"; and

(4) in paragraph (9), by striking "and security officers" and inserting ", security, and preparedness officers".

(b) SPECIFIC PROJECTS.—Subsection (a)(3) of section 1514 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1164) is amended—

(1) in subparagraph (D) by inserting before the semicolon at the end the following: ", or to connect to the National Terrorism Screening Center watchlist";

(2) in subparagraph (G), by striking "and" after the semicolon;

(3) in subparagraph (H) by striking the period at the end and inserting a semicolon; and

(4) by adding at the end the following new subparagraphs:

"(I) for improvements to passenger verification systems;

"(J) for improvements to employee and contractor verification systems, including identity verification technology; or

"(K) for improvements to the security of Amtrak computer systems, including cybersecurity assessments and programs.".

SEC. 583. STUDY ON SURFACE TRANSPORTATION INSPECTORS.

Not later than 180 days after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the appropriate congressional committees a report that—

(1) identifies any duplication or redundancy between the Transportation Security Administration and the Department of Transportation relating to surface transportation security inspections or oversight; and

(2) provides recommendations, if any, relating to—

(A) improvements to the surface transportation security inspectors program, including—

(i) changes in organizational and supervisory structures;

(ii) coordination procedures to enhance consistency; and

(iii) effectiveness in inspection and compliance activities; and

(B) whether each transportation mode needs inspectors trained and qualified for each such specific mode.

SEC. 584. SECURITY AWARENESS PROGRAM.

(a) ESTABLISHMENT.—The Administrator of the Transportation Security Administration shall establish a program to promote surface transportation security through the training of surface transportation operators and frontline employees on each of the skills identified in subsection (c).

(b) APPLICATION.—The program established under subsection (a) shall apply to all modes of surface transportation, including public transportation, rail, highway, motor carrier, and pipeline.

(c) TRAINING.—The program established under subsection (a) shall cover, at a minimum, the skills necessary to observe, assess, and respond to suspicious items or actions that could indicate a threat to transportation.

(d) ASSESSMENT.—

(1) IN GENERAL.—The Administrator of the Transportation Security Administration shall conduct an assessment of current training programs for surface transportation operators and frontline employees.

(2) CONTENTS.—The assessment under paragraph (1) shall identify—

(A) whether other training is being provided, either voluntarily or in response to other Federal requirements; and

(B) whether there are any gaps in existing training.

(e) UPDATES.—The Administrator of the Transportation Security Administration shall ensure the program established under subsection (a) is updated as necessary to address changes in risk and terrorist methods and to close any gaps identified in the assessment under subsection (d).

(f) SUSPICIOUS ACTIVITY REPORTING.—

(1) IN GENERAL.—The Secretary of Homeland Security shall ensure there exists a national mechanism for an individual to use to report to the Department of Homeland Security suspicious activity in transportation systems.

(2) PROCEDURES.—The Secretary of Homeland Security shall establish procedures for the Department of Homeland Security—

(A) to review and follow-up, as necessary, on each report received under paragraph (1); and

(B) to share, as necessary and in accordance with law, such reports with appropriate Federal, State, local, and tribal entities.

(3) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

(A) replace or affect in any way the use of 9-1-1 services in an emergency; or

(B) replace or affect in any way the security training program requirements specified in sections 1408, 1517, and 1534 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1137, 1167, and 1184; Public Law 110–53).

(g) FRONTLINE EMPLOYEE DEFINED.—In this section, the term "frontline employee" includes—

(1) an employee of a public transportation agency who is a transit vehicle driver or operator, dispatcher, maintenance and maintenance support employee, station attendant, customer service employee, security employee, or transit police, or any other employee who has direct contact with riders on a regular basis, and any other employee of a public transportation agency that the Administrator of the Transportation Security Administration determines should receive security training under this section or who is receiving security training under other law;

(2) over-the-road bus drivers, security personnel, dispatchers, maintenance and maintenance support personnel, ticket agents, other terminal employees, and other employees of an over-the-road bus operator or terminal owner or operator who the Administrator determines should receive security training under this section or who is receiving security training under other law; or

(3) security personnel, dispatchers, locomotive engineers, conductors, trainmen, other onboard employees, maintenance and maintenance support personnel, bridge tenders, and any other employees of railroad carriers who the Administrator determines should receive security training under this section or who is receiving security training under other law.

SEC. 585. VOLUNTARY USE OF CREDENTIALING.

(a) IN GENERAL.—An individual who is subject to credentialing or a background investigation under section 5103a of title 49, United States Code, may satisfy such requirement by obtaining a valid transportation security card issued under section 70105 of title 46, United States Code.

(b) FEES.—The Secretary of Homeland Security may charge reasonable fees, in accordance with section 520(a) of the Department of Homeland Security Appropriations Act, 2004 (6 U.S.C. 469(a)), for providing the necessary credentialing and background investigation under this section.

(c) DEFINITIONS.—In this section:

(1) INDIVIDUAL WHO IS SUBJECT TO CREDENTIALING OR A BACKGROUND INVESTIGATION.—The term "individual who is subject to credentialing or a background investigation" means an individual who—

(A) because of employment is regulated by the Transportation Security Administration, Department of Transportation, or Coast Guard and is required to have a background records check to obtain a hazardous materials endorsement on a commercial driver's license issued by a State under section 5103a of title 49, United States Code; or

(B) is required to have a credential and background records check under section 2102(d)(2) of the Homeland Security Act of 2002 (6 U.S.C. 622(d)(2)) at a facility with activities that are regulated by the Transportation Security Administration, Department of Transportation, or Coast Guard.

(2) VALID TRANSPORTATION SECURITY CARD ISSUED UNDER SECTION 70105 OF TITLE 46, UNITED STATES CODE.—The term "valid transportation security card issued under section 70105 of title 46, United States Code" means a transportation security card issued under section 70105 of title 46, United States Code, that is—

(A) not expired;

(B) shows no signs of tampering; and

(C) bears a photograph of the individual representing such card.

SEC. 586. BACKGROUND RECORDS CHECKS FOR ISSUANCE OF HAZMAT LICENSES.

(a) ISSUANCE OF LICENSES.—Paragraph (1) of section 5103a(a) of title 49, United States Code, is amended—

(1) by striking "unless" and inserting "unless—";

(2) by striking "the Secretary of Homeland Security" and inserting the following:

"(A) the Secretary of Homeland Security";

(3) in subparagraph (A), as designated pursuant to paragraph (2) of this subsection, by striking the period at the end and inserting "; or"; and

(4) by adding at the end the following new subparagraph:

"(B) the individual holds a valid transportation security card issued under section 70105 of title 46.".

(b) TRANSPORTATION SECURITY CARD.—Paragraph (1) of section 5103a(d) of title 49, United States Code, is amended, in the matter preceding subparagraph (A), by striking "described in subsection (a)(1)" and inserting "under subsection (a)(1)(A)".

SEC. 587. RECURRENT VETTING FOR SURFACE TRANSPORTATION CREDENTIAL-HOLDERS.

Section 70105 of title 46, United States Code, is amended by adding at the end the following new subsection:

"(r) RECURRENT VETTING.—

"(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this subsection, the Secretary shall develop and implement a plan to utilize the Federal Bureau of Investigation's Rap Back Service in order to establish recurrent vetting capabilities for individuals holding valid transportation security cards under this section.

"(2) EXEMPTION.—Individuals holding valid transportation security cards under this section who are subject to recurrent vetting under the plan to utilize the Rap Back Service referred to in paragraph (1) shall be exempt from any recurrent determinations or background checks under this section to which such individuals would otherwise be subject every five years in the absence of such utilization.".

SEC. 588. PIPELINE SECURITY STUDY.

(a) STUDY.—The Comptroller General of the United States shall conduct a study regarding the roles and responsibilities of the Department of Homeland Security and the Department of Transportation with respect to pipeline security. Such study shall address whether—

(1) the Annex to the Memorandum of Understanding executed on August 9, 2006, between the Department of Homeland Security and the Department of Transportation adequately delineates strategic and operational responsibilities for pipeline security, including whether it is clear which department is responsible for—

(A) protecting against intentional pipeline breaches and cyber attacks;

(B) responding to intentional pipeline breaches and cyber attacks; and

(C) planning to recover from the impact of intentional pipeline breaches and cyber attacks;

(2) the respective roles and responsibilities of each department are adequately conveyed to relevant stakeholders and to the public; and

(3) the processes and procedures for determining whether a particular pipeline breach is a terrorist incident are clear and effective.

(b) REPORT ON STUDY.—Not later than 180 days after the date of the enactment of this section, the Comptroller General of the United States shall submit to the Secretary of Homeland Security and the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report containing the findings of the study conducted under subsection (a).

(c) REPORT TO CONGRESS.—Not later than 90 days after the submission of the report under subsection (b), the Secretary of Homeland Security shall review and analyze the study and submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on such review and analysis, including any recommendations for—

(1) changes to the Annex to the Memorandum of Understanding referred to in subsection (a)(1); and

(2) other improvements to pipeline security activities at the Department.

SEC. 589. REPEAL OF LIMITATION RELATING TO MOTOR CARRIER SECURITY-SENSITIVE MATERIAL TRACKING TECHNOLOGY.

Section 1554 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1204) is amended by striking subsection (d).

Subtitle H—Security Enhancements in Public Areas of Transportation Facilities

SEC. 591. WORKING GROUP.

(a) IN GENERAL.—The Secretary of Homeland Security may establish a working group to promote collaborative engagement between the Department of Homeland

Security and public and private stakeholders to develop non-binding recommendations for enhancing the security in public areas of transportation facilities.

(b) ANNUAL REPORT.—If the Secretary of Homeland Security establishes a working group pursuant to subsection (a), not later than one year after such establishment and annually thereafter for five years, the Secretary shall report on the working group's organization, participation, activities, findings, and non-binding recommendations for the immediately preceding 12 month period. The Secretary may publish a public version describing the working group's activities and such related matters as would be informative to the public, consistent with section 552(b) of title 5, United States Code.

(c) INAPPLICABILITY OF THE FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the working group or any subsidiary thereof.

SEC. 592. TECHNICAL ASSISTANCE; VULNERABILITY ASSESSMENT TOOLS.

(a) IN GENERAL.—The Secretary of Homeland Security shall—

(1) inform public and private sector stakeholders regarding the availability of Department of Homeland Security technical assistance, including vulnerability assessment tools, to help enhance the security in public areas of transportation facilities; and

(2) subject to availability of appropriations, provide such technical assistance, upon request, to such a stakeholder.

(b) BEST PRACTICES.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall publish and widely disseminate best practices for protecting and enhancing the resilience of public areas of transportation facilities, including associated frameworks or templates for implementation. As appropriate, such best practices shall be updated periodically.

SEC. 593. OPERATIONS CENTERS.

Not later than 120 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration, in consultation with the heads of other appropriate offices or components of the Department of Homeland Security, shall make available to public and private stakeholders a framework for establishing an operations center within a transportation facility to promote interagency response and coordination.

SEC. 594. REVIEW OF REGULATIONS.

(a) REVIEW.—Not later than one year after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall submit to the Committee on Homeland Security of the House and the Committee on Commerce, Science, and Transportation of the Senate a report that includes a review of regulations, directives, policies, and procedures issued by the Administrator regarding the transportation of a firearm and ammunition by an aircraft passenger, and, as appropriate, information on plans to modify any such regulation, directive, policy, or procedure based on such review.

(b) CONSULTATION.—In preparing the report required under subsection (a), the Administrator of the Transportation Security Administration shall consult with the Aviation Security Advisory Committee (established pursuant to section 44946 of title 49, United States Code) and appropriate public and private sector stakeholders.

SEC. 595. DEFINITION.

In this subtitle, the term "public and private sector stakeholders" has the meaning given such term in section 114(u)(1)(C) of title 49, United States Code.

TITLE VI—EMERGENCY PREPAREDNESS, RESPONSE, AND COMMUNICATIONS

Subtitle A—Grants, Training, Exercises, and Coordination

SEC. 601. URBAN AREA SECURITY INITIATIVE.

Section 2003 of the Homeland Security Act of 2002 (6 U.S.C. 604) is amended—

(1) in subsection (b)(2)(A), in the matter preceding clause (i), by inserting ", using the most up-to-date data available," after "assessment";

(2) in subsection (d)(2), by amending subparagraph (B) to read as follows:

"(B) FUNDS RETAINED.—To ensure transparency and avoid duplication, a State shall provide each relevant high-risk urban area with a detailed ac-

counting of the items, services, or activities on which any funds retained by the State under subparagraph (A) are to be expended. Such accounting shall be provided not later than 90 days after the date of which such funds are retained."; and

(3) by striking subsection (e) and inserting the following new subsections:

"(e) THREAT AND HAZARD IDENTIFICATION RISK ASSESSMENT AND CAPABILITY ASSESSMENT.—As a condition of receiving a grant under this section, each high-risk urban area shall submit to the Administrator a threat and hazard identification and risk assessment and capability assessment—

"(1) at such time and in such form as is required by the Administrator; and

"(2) consistent with the Federal Emergency Management Agency's Comprehensive Preparedness Guide 201, Second Edition, or such successor document or guidance as is issued by the Administrator.

"(f) 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.

"(g) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for grants under this section $800,000,000 for each of fiscal years 2018 through 2022.".

SEC. 602. STATE HOMELAND SECURITY GRANT PROGRAM.

Section 2004 of the Homeland Security Act of 2002 (6 U.S.C. 605) is amended by striking subsection (f) and inserting the following new subsections:

"(f) THREAT AND HAZARD IDENTIFICATION AND RISK ASSESSMENT AND CAPABILITY ASSESSMENT.—

"(1) IN GENERAL.—As a condition of receiving a grant under this section, each State shall submit to the Administrator a threat and hazard identification and risk assessment and capability assessment—

"(A) at such time and in such form as is required by the Administrator; and

"(B) consistent with the Federal Emergency Management Agency's Comprehensive Preparedness Guide 201, Second Edition, or such successor document or guidance as is issued by the Administrator.

"(2) COLLABORATION.—In developing the threat and hazard identification and risk assessment under paragraph (1), a State shall solicit input from local and tribal governments, including first responders, and, as appropriate, non-governmental and private sector stakeholders.

"(3) FIRST RESPONDERS DEFINED.—In this subsection, the term 'first responders' includes representatives of local governmental and nongovernmental fire, law enforcement, emergency management, and emergency medical personnel.

"(g) 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.

"(h) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for grants under this section $600,000,000 for each of fiscal years 2018 through 2022.".

SEC. 603. GRANTS TO DIRECTLY ELIGIBLE TRIBES.

Section 2005 of the Homeland Security Act of 2002 (6 U.S.C. 606) is amended by—

(1) redesignating subsections (h) through (k) as subsections (i) through (l), respectively; and

(2) inserting after subsection (g) the following new subsection:

"(h) PERIOD OF PERFORMANCE.—The Secretary 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.".

SEC. 604. LAW ENFORCEMENT TERRORISM PREVENTION.

(a) LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM.—Subsection (a) of section 2006 of the Homeland Security Act of 2002 (6 U.S.C. 607) is amended—

(1) in paragraph (1)—

(A) by inserting "States and high-risk urban areas expend" after "that"; and

(B) by striking "is used";

(2) in paragraph (2), by amending subparagraph (I) to read as follows:

"(I) activities as determined appropriate by the Administrator, in coordination with the Assistant Secretary for State and Local Law Enforcement within the Office of Partnership and Engagement of the Department, through outreach to relevant stakeholder organizations; and"; and

(3) by adding at the end the following new paragraph:

"(4) ANNUAL REPORT.—The Administrator, in coordination with the Assistant Secretary for State and Local Law Enforcement, shall report annually from fiscal year 2018 through fiscal year 2022 on the use of grants under sections 2003 and 2004 for law enforcement terrorism prevention activities authorized under this section, including the percentage and dollar amount of funds used for such activities and the types of projects funded.".

(b) OFFICE FOR STATE AND LOCAL LAW ENFORCEMENT.—Subsection (b) section 2006 of the Homeland Security Act of 2002 (6 U.S.C. 607) is amended—

(1) in paragraph (1), by striking "Policy Directorate" and inserting "Office of Partnership and Engagement"

(2) in paragraph (4)—

(A) in subparagraph (B), by inserting ", including through consultation with such agencies regarding Department programs that may impact such agencies" before the semicolon at the end; and

(B) in subparagraph (D), by striking "ensure" and inserting "certify".

SEC. 605. PRIORITIZATION.

(a) IN GENERAL.—Subsection (a) of section 2007 of the Homeland Security Act of 2002 (6 U.S.C. 608) is amended—

(1) in paragraph (1)—

(A) by amending subparagraph (A) to read as follows:

"(A) its population, including consideration of domestic and international tourists, commuters, and military populations, including military populations residing in communities outside military installations;";

(B) in subparagraph (E), by inserting ", including threat information from other relevant Federal agencies and field offices, as appropriate" before the semicolon at the end; and

(C) in subparagraph (I), by striking "target" and inserting "core"; and

(2) in paragraph (2), by striking "target" and inserting "core".

(b) REVIEW.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, through the Administrator of the Federal Emergency Management Agency, shall review and report to 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 on the risk formula and methodology used to award grants under sections 2003 and 2004 of the Homeland Security Act of 2002 (6 U.S.C. 604 and 605), including a discussion of any necessary changes to such formula to ensure grant awards are appropriately based on risk.

(c) COMPTROLLER GENERAL REVIEW.—Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall review and assess the risk formula and methodology used to award grants under sections 2003 and 2004 of the Homeland Security Act of 2002, including—

(1) the process utilized by the Department of Homeland Security to gather threat information for each potential State and high-risk urban area;

(2) the extent to which such risk formula and methodology considers the factors specified in section 2007 of the Homeland Security Act of 2002 (6 U.S.C. 608), in particular—

(A) the extent to which the jurisdiction has unmet core capabilities due to resource constraints;

(B) the degree to which a jurisdiction has been able to address capability gaps with previous grant awards; and

(C) in the case of a high-risk urban area, the extent to which such high-risk urban area includes—

(i) 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

(3) how grant award amounts are determined.

SEC. 606. ALLOWABLE USES.

Section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609) is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1), by striking "target" and inserting "core";

(B) by redesignating paragraphs (6) through (14) as paragraphs (8) through (16), respectively;

(C) in paragraph (5), by inserting before the semicolon at the end the following: ", provided such purchases align with the Statewide Communication Interoperability Plan and are coordinated with the Statewide Interoperability Coordinator or Statewide interoperability governance body of the State of the recipient"; and

(D) by inserting after paragraph (5) the following new paragraphs:

"(6) enhancing medical preparedness, medical surge capacity, and mass prophylaxis capabilities, including the development and maintenance of an initial pharmaceutical stockpile, including medical kits and diagnostics sufficient to protect first responders, their families, immediate victims, and vulnerable populations from a chemical or biological event;

"(7) enhancing cybersecurity, including preparing for and responding to cybersecurity risks and incidents (as such terms are defined in section 227) and developing statewide cyber threat information analysis and dissemination activities;";

(E) in paragraph (8), as so redesignated, by striking "Homeland Security Advisory System" and inserting "National Terrorism Advisory System"; and

(F) in paragraph (14), as so redesignated, by striking "3" and inserting "5";

(2) in subsection (b)—

(A) in paragraph (3)(B), by striking "(a)(10)" and inserting "(a)(12)"; and

(B) in paragraph (4)(B)(i), by striking "target" and inserting "core"; and

(3) in subsection (c), by striking "target" and "core".

SEC. 607. APPROVAL OF CERTAIN EQUIPMENT.

(a) IN GENERAL.—Section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609), as amended by this Act, is further amended—

(1) in subsection (f)—

(A) by striking "If an applicant" and inserting the following:

"(1) APPLICATION REQUIREMENT.—If an applicant"; and

(B) by adding at the end the following new paragraphs:

"(2) REVIEW PROCESS.—The Administrator shall implement a uniform process for reviewing applications that, in accordance with paragraph (1), contain explanations to use grants provided under section 2003 or 2004 to purchase 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).

"(3) FACTORS.—In carrying out the review process under paragraph (2), the Administrator shall consider the following:

"(A) Current or past use of proposed equipment or systems by Federal agencies or the Armed Forces.

"(B) The absence of a national voluntary consensus standard for such equipment or systems.

"(C) The existence of an international consensus standard for such equipment or systems, and whether such equipment or systems meets such standard.

"(D) The nature of the capability gap identified by the applicant, and how such equipment or systems will address such gap.

"(E) The degree to which such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed existing consensus standards.

"(F) Any other factor determined appropriate by the Administrator."; and

(2) by adding at the end the following new subsection:

"(g) REVIEW PROCESS.—The Administrator shall implement a uniform process for reviewing applications to use grants provided under section 2003 or 2004 to purchase equipment or systems not included on the Authorized Equipment List maintained by the Administrator.".

(b) INSPECTOR GENERAL REPORT.—Not later than three years after the date of the enactment of this Act, the Inspector General of the Department of Homeland Security 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 assessing the implementation of the review process established under paragraph (2) of subsection (f) of section 2008 of the Homeland Security Act of 2002 (as added by subsection (a) of this section), including information on the following:

(1) The number of requests to purchase equipment or systems that do not meet or exceed any applicable consensus standard evaluated under such review process.

(2) The capability gaps identified by applicants and the number of such requests granted or denied.

(3) The processing time for the review of such requests.

SEC. 608. MEMORANDA OF UNDERSTANDING.

(a) IN GENERAL.—Subtitle B of title XX of the Homeland Security Act of 2002 (6 U.S.C. 611 et seq.) is amended by adding at the end the following new section:

"SEC. 2024. MEMORANDA OF UNDERSTANDING WITH DEPARTMENTAL COMPONENTS AND OFFICES.

"The Administrator shall enter into memoranda of understanding with the heads of the following departmental components and offices delineating the roles and responsibilities of such components and offices regarding the policy and guidance for grants under section 1406 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1135), sections 2003 and 2004 of this Act, and section 70107 of title 46, United States Code, as appropriate:

"(1) The Commissioner of U.S. Customs and Border Protection.

"(2) The Administrator of the Transportation Security Administration.

"(3) The Commandant of the Coast Guard.

"(4) The Under Secretary for Intelligence and Analysis.

"(5) The Director of the Office of Emergency Communications.

"(6) The Assistant Secretary for State and Local Law Enforcement.

"(7) The Countering Violent Extremism Coordinator.

"(8) The Officer for Civil Rights and Civil Liberties.

"(9) The Chief Medical Officer.

"(10) The heads of other components or offices of the Department, as determined by the Secretary.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2023 the following new item:

"Sec. 2024. Memoranda of understanding with departmental components and offices.".

SEC. 609. GRANTS METRICS.

(a) IN GENERAL.—To determine the extent to which grants under sections 2003 and 2004 of the Homeland Security Act of 2002 (6 U.S.C. 603 and 604) have closed capability gaps identified in State Preparedness Reports required under subsection (c) of section 652 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 752; title VI of the Department of Homeland Security Appropriations Act, 2007; Public Law 109–295) and Threat and Hazard Identification and Risk Assessments required under subsections (e) and (f) of such sections 2003 and 2004, respectively, as added by this Act, from each State and high-risk urban area, the Administrator of the Federal Emergency Management Agency shall conduct and 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 of the Senate an assessment of information provided in such Reports and Assessments.

(b) ASSESSMENT REQUIREMENTS.—The assessment required under subsection (a) shall include a comparison of successive State Preparedness Reports and Threat and Hazard Identification and Risk Assessments that aggregates results across the States and high-risk urban areas.

SEC. 610. GRANT MANAGEMENT BEST PRACTICES.

The Administrator of the Federal Emergency Management Agency shall include in the annual Notice of Funding Opportunity relating to grants under sections 2003 and 2004 of the Homeland Security Act of 2002 (6 U.S.C. 604 and 605) an appendix that includes the following:

(1) A summary of findings identified by the Office of the Inspector General of the Department of Homeland Security in audits of such grants and methods to address areas identified for improvement, including opportunities for technical assistance.

(2) Innovative projects and best practices instituted by grant recipients.

SEC. 611. PROHIBITION ON CONSOLIDATION.

The Secretary of Homeland Security may not implement the National Preparedness Grant Program or any successor consolidated grant program unless the Secretary receives prior authorization from Congress permitting such implementation.

SEC. 612. MAINTENANCE OF GRANT INVESTMENTS.

Section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609), as amended by this Act, is further amended by adding at the end the following new subsection:

"(h) MAINTENANCE OF EQUIPMENT.—Any applicant for a grant under section 2003 or 2004 seeking to use funds to purchase equipment, including pursuant to paragraphs (3), (4), (5), or (12) of subsection (a) of this section, shall by the time of the receipt of such grant develop a plan for the maintenance of such equipment over its life-cycle that includes information identifying which entity is responsible for such maintenance.".

SEC. 613. TRANSIT SECURITY GRANT PROGRAM.

Section 1406 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1135) is amended—

(1) in subsection (b)(2)(A), by inserting "and associated backfill" after "security training"; and

(2) by striking subsection (m) and inserting the following new subsections:

"(m) PERIODS OF PERFORMANCE.—

"(1) IN GENERAL.—Except as provided in paragraph (2), funds provided pursuant to a grant awarded under this section for a use specified in subsection (b) shall remain available for use by a grant recipient for a period of not fewer than 36 months.

"(2) EXCEPTION.—Funds provided pursuant to a grant awarded under this section for a use specified in subparagraph (M) or (N) of subsection (b)(1) shall remain available for use by a grant recipient for a period of not fewer than 55 months.

"(n) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for grants under this section $200,000,000 for each of fiscal years 2018 through 2022.".

SEC. 614. PORT SECURITY GRANT PROGRAM.

Section 70107 of title 46, United States Code, is amended by—

(1) striking subsection (l);

(2) redesignating subsection (m) as subsection (l); and

(3) by adding at the end the following new subsections:

"(n) PERIOD OF PERFORMANCE.—The Secretary 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.

"(o) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for grants under this section $200,000,000 for each of the fiscal years 2018 through 2022.".

SEC. 615. NATIONAL DOMESTIC PREPAREDNESS CONSORTIUM.

Section 1204 of the Implementing Recommendations of the 9/11 Commission Act (6 U.S.C. 1102) is amended—

(1) in subsection (c), by inserting "to the extent practicable, provide training in settings that stimulate real response environments, such as urban areas," after "levels,".;

(2) in subsection (d), by amending paragraphs (1) and (2) to read as follows:

"(1) for the Center for Domestic Preparedness, $63,939,000 for each of fiscal years 2018 and 2019; and

"(2) for the remaining Members of the National Domestic Preparedness Consortium, $101,000,000 for each of fiscal years 2018 and 2019."; and

(3) in subsection (e), in the matter preceding paragraph (1), by striking "2007" and inserting "2017".

SEC. 616. RURAL DOMESTIC PREPAREDNESS CONSORTIUM.

(a) IN GENERAL.—The Secretary of Homeland Security is authorized to establish a Rural Domestic Preparedness Consortium within the Department of Homeland Security consisting of universities and nonprofit organizations qualified to provide training to emergency response providers from rural communities.

(b) DUTIES.—The Rural Domestic Preparedness Consortium authorized under subsection (a) shall identify, develop, test, and deliver training to State, local, and tribal emergency response providers from rural communities, provide on-site and mobile training, and facilitate the delivery of training by the training partners of the Department of Homeland Security.

(c) AUTHORIZATION OF APPROPRIATIONS.—Of amounts appropriated for Continuing Training Grants of the Department of Homeland Security, $5,000,000 is authorized to be used for the Rural Domestic Preparedness Consortium authorized under subsection (a).

SEC. 617. EMERGENCY SUPPORT FUNCTIONS.

(a) UPDATE.—Paragraph (13) of section 504(a) of the Homeland Security Act of 2002 (6 U.S.C. 314(a)) is amended by inserting ", periodically updating (but not less often than once every five years)," after "administering".

(b) EMERGENCY SUPPORT FUNCTIONS.—Section 653 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 753; title VI of the Department of Homeland Security Appropriations Act, 2007; Public Law 109–295) is amended—

(1) by redesignating subsections (d) and (e) as subsections (e) and (f), respectively; and

(2) by inserting after subsection (c) the following new subsection:

"(d) COORDINATION.—The President, acting through the Administrator, shall develop and provide to Federal departments and agencies with coordinating, primary, or supporting responsibilities under the National Response Framework performance metrics to ensure readiness to execute responsibilities under the emergency support functions of such Framework.".

SEC. 618. REVIEW OF NATIONAL INCIDENT MANAGEMENT SYSTEM.

Paragraph (2) of section 509(b) of the Homeland Security Act of 2002 (6 U.S.C. 319(b)) is amended, in the matter preceding subparagraph (A), by inserting ", but not less often than once every five years," after "periodically".

SEC. 619. REMEDIAL ACTION MANAGEMENT PROGRAM.

Section 650 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 750; title VI of the Department of Homeland Security Appropriations Act, 2007; Public Law 109–295) is amended to read as follows:

"SEC. 650. REMEDIAL ACTION MANAGEMENT PROGRAM.

"(a) IN GENERAL.—The Administrator, in coordination with the National Council on Disability and the National Advisory Council, shall establish a remedial action management program to—

"(1) analyze training, exercises, and real world events to identify lessons learned, corrective actions, and best practices;

"(2) generate and disseminate, as appropriate, the lessons learned, corrective actions, and best practices referred to in paragraph (1); and

"(3) conduct remedial action tracking and long term trend analysis.

"(b) FEDERAL CORRECTIVE ACTIONS.—The Administrator, in coordination with the heads of appropriate Federal departments and agencies, shall utilize the program established pursuant to subsection (a) to collect information on corrective actions identified by such Federal departments and agencies during exercises and the response to natural disasters, acts of terrorism, and other man-made disasters, and shall, not later than one year after the date of the enactment of this section and annually thereafter for each of the next four years, submit to Congress a report on the status of such corrective actions.

"(c) DISSEMINATION OF AFTER ACTION REPORTS.—The Administrator shall provide electronically, to the maximum extent practicable, to Congress and Federal, State, local, tribal, and private sector officials after-action reports and information on lessons learned and best practices from responses to acts of terrorism, natural disasters, capstone exercises conducted under the national exercise program under section 648(b), and other emergencies or exercises.".

SEC. 620. CYBER PREPAREDNESS.

(a) INFORMATION SHARING.—Title II of the Homeland Security Act of 2002 is amended—

(1) in section 210A (6 U.S.C. 124h)—

(A) in subsection (b)—

(i) in paragraph (10), by inserting before the semicolon at the end the following: ", including, in coordination with the national cybersecurity and communications integration center under section 227, access to timely technical assistance, risk management support, and incident response capabilities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents (as such terms are defined in such section), which may include attribution, mitigation, and remediation, and the provision of information and recommendations on security and resilience, including implications of cybersecurity risks to equipment and technology related to the electoral process";

(ii) in paragraph (11), by striking "and" after the semicolon;

(iii) by redesignating paragraph (12) as paragraph (14); and

(iv) by inserting after paragraph (11) the following new paragraphs:

"(12) review information relating to cybersecurity risks that is gathered by State, local, and regional fusion centers, and incorporate such information, as appropriate, into the Department's own information relating to cybersecurity risks;

"(13) ensure the dissemination to State, local, and regional fusion centers of the information described in paragraph (12); and";

(B) in subsection (c)(2)—

(i) by redesignating subparagraphs (C) through (G) as subparagraphs (D) through (H), respectively; and

(ii) by inserting after subparagraph (B) the following new subparagraph:

"(C) The national cybersecurity and communications integration center under section 227.";

(C) in subsection (d)—

(i) in paragraph (3), by striking "and" after the semicolon;

(ii) by redesignating paragraph (4) as paragraph (5); and

(iii) by inserting after paragraph (3) the following new paragraph:

"(4) assist, in coordination with the national cybersecurity and communications integration center under section 227, fusion centers in using information relating to cybersecurity risks to develop a comprehensive and accurate threat picture; and"; and

(D) in subsection (j)—

(i) by redesignating paragraphs (1) through (5) as paragraphs (2) through (6), respectively; and

(ii) by inserting before paragraph (2), as so redesignated, the following new paragraph:

"(1) the term 'cybersecurity risk' has the meaning given such term in section 227;"; and

(2) in section 227 (6 U.S.C. 148)—

(A) in subsection (c)—

(i) in paragraph (5)(B), by inserting ", including State, local, and regional fusion centers, as appropriate" before the semicolon at the end;

(ii) in paragraph (7), in the matter preceding subparagraph (A), by striking "information and recommendations" each place it appears and inserting "information, recommendations, and best practices"; and

(iii) in paragraph (9), by inserting "best practices," after "defensive measures,"; and

(B) in subsection (d)(1)(B)(ii), by inserting "and State, local, and regional fusion centers, as appropriate" before the semicolon at the end.

(b) SENSE OF CONGRESS.—It is the sense of Congress that to facilitate the timely dissemination to appropriate State, local, and private sector stakeholders of homeland security information related to cyber threats, the Secretary of Homeland Security should, to the greatest extent practicable, work to share actionable information in an unclassified form related to such threats.

SEC. 621. MAJOR METROPOLITAN AREA COUNTERTERRORISM TRAINING AND EXERCISE GRANT PROGRAM.

(a) IN GENERAL.—Subtitle A of title XX of the Homeland Security Act of 2002 (6 U.S.C. 603 et seq.) is amended by adding at the end the following new section:

"SEC. 2009. MAJOR METROPOLITAN AREA COUNTERTERRORISM TRAINING AND EXERCISE GRANT PROGRAM.

"(a) ESTABLISHMENT.—

"(1) IN GENERAL.—The Secretary, acting through the Administrator and the heads of other relevant components of the Department, shall carry out a program to make grants to emergency response providers to prevent, prepare for, and respond to emerging terrorist attack scenarios, including complex, coordinated terrorist attacks and active shooters, as determined by the Secretary, against major metropolitan areas.

"(2) INFORMATION.—In establishing the program pursuant to paragraph (1), the Secretary shall provide to eligible applicants—

"(A) information, in an unclassified format, on emerging terrorist attack scenarios, including complex, coordinated terrorist attacks and active shooters, which grants under such program are intended to address; and

"(B) information on training and exercises best practices.

"(b) ELIGIBLE APPLICANTS.—

"(1) IN GENERAL.—Jurisdictions that receive, or that previously received, funding under section 2003 may apply for a grant under the program established pursuant to subsection (a).

"(2) ADDITIONAL JURISDICTIONS.—Eligible applicants receiving funding under the program established pursuant to subsection (a) may include in activities funded by such program neighboring jurisdictions that would be likely to provide mutual aid in response to emerging terrorist attack scenarios, including complex, coordinated terrorist attacks and active shooters.

"(c) PERMITTED USES.—The recipient of a grant under the program established pursuant to subsection (a) may use such grant to—

"(1) identify capability gaps related to preparing for, preventing, and responding to emerging terrorist attack scenarios, including complex, coordinated terrorist attacks and active shooters;

"(2) develop or update plans, annexes, and processes to address any capability gaps identified pursuant to paragraph (1);

"(3) conduct training to address such identified capability gaps;

"(4) conduct exercises, including at locations such as mass gathering venues, places of worship, or educational institutions, as appropriate, to validate capabilities; and

"(5) pay for backfill associated with personnel participating in training and exercises under paragraphs (3) and (4).

"(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 fewer than 36 months.

"(e) INFORMATION SHARING.—The Administrator shall, to the extent practicable, aggregate, analyze, and share with relevant emergency response providers information on best practices and lessons learned from—

"(1) the planning, training, and exercises conducted using grants authorized under the program established pursuant to subsection (a); and

"(2) responses to actual terrorist attacks around the world.

"(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for grants under this section $39,000,000 for each of fiscal years 2018 through 2022.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2008 the following new item:

"Sec. 2009. Major metropolitan area counterterrorism training and exercise grant program.".

SEC. 622. CENTER FOR DOMESTIC PREPAREDNESS.

(a) IMPLEMENTATION PLAN.—The Administrator of the Federal Emergency Management Agency shall develop an implementation plan, including benchmarks and milestones, to address the findings and recommendations of the 2017 Management Review Team that issued a report on May 8, 2017, regarding live agent training at the Chemical, Ordnance, Biological and Radiological Training Facility and provide 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 of the Senate updates and information on efforts to implement recommendations related to the management review of the Chemical, Ordnance, Biological, and Radiological Training Facility of the Center for Domestic Preparedness of the Federal Emergency Management Agency, including, as necessary, information on additional resources or authority needed to implement such recommendations.

(b) COMPTROLLER GENERAL REVIEW.—Not later than one-year after the date of the enactment of this section, the Comptroller General of the United States shall review and report to Congress on the status of the implementation plan required by subsection (a) and the governance structure at the Chemical, Ordnance, Biological and Radiological Training Facility of the Center for Domestic Preparedness of the Federal Emergency Management Agency.

SEC. 623. OPERATION STONEGARDEN.

(a) IN GENERAL.—Subtitle A of title XX of the Homeland Security Act of 2002 (6 U.S.C. 601 et seq.), as amended by this Act, is further amended by adding at the end the following new section:

"SEC. 2010. OPERATION STONEGARDEN.

"(a) ESTABLISHMENT.—There is established in the Department a program to be known as 'Operation Stonegarden'. Under such program, the Secretary, acting through the Administrator, shall make grants to eligible law enforcement agencies, through the State Administrative Agency, to enhance border security in accordance with this section.

"(b) ELIGIBLE RECIPIENTS.—To be eligible to receive a grant under this section, a law enforcement agency shall—

"(1) be located in—

"(A) a State bordering either Canada or Mexico; or

"(B) a State or territory with a maritime border; and

"(2) be involved in an active, ongoing U.S. Customs and Border Protection operation coordinated through a sector office.

"(c) PERMITTED USES.—The recipient of a grant under this section may use such grant for any of the following:

"(1) Equipment, including maintenance and sustainment costs.

"(2) Personnel, including overtime and backfill, in support of enhanced border law enforcement activities.

"(3) Any activity permitted for Operation Stonegarden under the Department of Homeland Security's Fiscal Year 2016 Homeland Security Grant Program Notice of Funding Opportunity.

"(4) Any other appropriate activity, as determined by the Administrator, in consultation with the Commissioner of U.S. Customs and Border Protection.

"(d) PERIOD OF PERFORMANCE.—The Secretary 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.

"(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $110,000,000 for each of fiscal years 2018 through 2022 for grants under this section.

"(e) REPORT.—The Administrator shall annually for each of the fiscal years specified in subsection (d) 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 expenditure of grants made under this section by each grant recipient.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002, as amended by this Act, is further amended by inserting after the item relating to section 2009 the following new item:

"Sec. 2010. Operation Stonegarden.".

SEC. 624. NON-PROFIT SECURITY GRANT PROGRAM.

(a) IN GENERAL.—Subtitle A of title XX of the Homeland Security Act of 2002 (6 U.S.C. 601 et seq.), as amended by this Act, is further amended by adding at the end the following new section:

"SEC. 2011. NON-PROFIT SECURITY GRANT PROGRAM.

"(a) ESTABLISHMENT.—There is established in the Department a program to be known as the 'Non-Profit 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.

"(b) ELIGIBLE RECIPIENTS.—Eligible nonprofit organizations described in this subsection (a) 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 to be at risk of a terrorist attack by the Administrator.

"(c) PERMITTED USES.—The recipient of a grant under this section may use such grant for any of the following uses:

"(1) Target hardening activities, including physical security enhancement equipment and inspection and screening systems.

"(2) Fees for security training relating to physical security and cybersecurity, target hardening, terrorism awareness, and employee awareness.

"(3) Any other appropriate activity, as determined by the Administrator.

"(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 2018 through 2022 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 expenditure by each grant recipient of grant funds made under this section.

"(f) AUTHORIZATION OF APPROPRIATIONS.—

"(1) IN GENERAL.—There is authorized to be appropriated $50,000,000 for each of fiscal years 2018 through 2022 to carry out this section.

"(2) SPECIFICATION.—Of the amounts authorized to be appropriated pursuant to paragraph (1)—

"(A) $35,000,000 is authorized for eligible recipients located in jurisdictions that receive funding under section 2003; and

"(B) $15,000,000 is authorized for eligible recipients in jurisdictions not receiving funding under section 2003.".

(b) CONFORMING AMENDMENT.—Subsection (a) of section 2002 of the Homeland Security Act of 2002 (6 U.S.C. 603) is amended by striking "sections 2003 and 2004" and inserting "sections 2003, 2004, and 2011".

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2008 the following new item:

"Sec. 2011. Non-Profit Security Grant Program.".

SEC. 625. FEMA SENIOR LAW ENFORCEMENT ADVISOR.

(a) IN GENERAL.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.), as amended by this Act, is further amended by adding at the end the following new section:

"SEC. 529. SENIOR LAW ENFORCEMENT ADVISOR.

"(a) ESTABLISHMENT.—There is established in the Agency a Senior Law Enforcement Advisor to serve as a qualified expert to the Administrator for the purpose of strengthening the Agency's coordination among State, local, and tribal law enforcement.

"(b) QUALIFICATIONS.—The Senior Law Enforcement Advisor shall have an appropriate background with experience in law enforcement, intelligence, information sharing, and other emergency response functions.

"(c) RESPONSIBILITIES.—The Senior Law Enforcement Advisor shall—

"(1) coordinate on behalf of the Administrator with the Office for State and Local Law Enforcement under section 2006 for the purpose of ensuring State, local, and tribal law enforcement receive consistent and appropriate consideration in policies, guidance, training, and exercises related to preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other man-made disasters within the United States;

"(2) work with the Administrator and the Office for State and Local Law Enforcement under section 2006 to ensure grants to State, local, and tribal government agencies, including programs under sections 2003, 2004, and 2006(a) appropriately focus on terrorism prevention activities; and

"(3) serve other appropriate functions as determined by the Administrator.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002, as amended by this Act, is further amended by inserting after the item relating to section 528 the following new item:

"Sec. 529. Senior Law Enforcement Advisor.".

SEC. 626. STUDY OF THE USE OF GRANT FUNDS FOR CYBERSECURITY.

Not later than 120 days after the enactment of this section, the Administrator, in consultation with relevant components of the Department, shall conduct a study on the use of grant funds awarded pursuant to section 2003 and section 2004 of the Homeland Security Act of 2002 (6 U.S.C. 604 and 605), including information on the following:

(1) The amount of grant funds invested or obligated annually during fiscal years 2006 through 2016 to support efforts to prepare for and respond to cybersecurity risks and incidents (as such terms are defined in section 227 of such Act (6 U.S.C. 148).

(2) The degree to which grantees identify cybersecurity as a capability gap in the Threat and Hazard Identification and Risk Assessment carried out pursuant to the amendment made by sections 601 and 602 of this title.

(3) Obstacles and challenges related to using grant funds to improve cybersecurity.

(4) Plans for future efforts to encourage grantees to use grant funds to improve cybersecurity capabilities.

SEC. 627. TECHNICAL EXPERT AUTHORIZED.

Paragraph (2) of section 503(b) of the Homeland Security Act of 2002 (6 U.S.C. 313(b)) is amended—

(1) in subparagraph (G), by striking "and" at the end;

(2) in subparagraph (H), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following new subparagraph:

"(I) identify and integrate the needs of children into activities to prepare for, protect against, respond to, recover from, and mitigate against natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents, including by appointing a technical expert, who may consult with relevant outside organizations and experts, as necessary, to coordinate such activities, as necessary.".

Subtitle B—Communications

SEC. 631. OFFICE OF EMERGENCY COMMUNICATIONS.

The Secretary of Homeland Security may not change the location or reporting structure of the Office of Emergency Communications of the Department of Homeland Security unless the Secretary receives prior authorization from the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate permitting such change.

SEC. 632. RESPONSIBILITIES OF OFFICE OF EMERGENCY COMMUNICATIONS DIRECTOR.

(a) IN GENERAL.—Subsection (c) of section 1801 of the Homeland Security Act of 2002 (6 U.S.C. 571) is amended—

(1) by striking paragraph (3);

(2) by redesignating paragraphs (4) through (15) as paragraphs (3) through (14), respectively;

(3) in paragraph (8), as so redesignated, by striking ", in cooperation with the National Communications System,";

(4) in paragraph (12) by striking "Assistant Secretary for Grants and Training" and inserting "Administrator of the Federal Emergency Management Agency";

(5) in paragraph (13), as so redesignated, by striking "and" at the end;

(6) in paragraph (14), as so redesignated, by striking the period at the end and inserting a semicolon; and

(7) by adding at the end the following new paragraphs:

"(15) administer the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) programs, or successor programs; and

"(16) assess the impact of emerging technologies on interoperable emergency communications.".

(b) PERFORMANCE OF PREVIOUSLY TRANSFERRED FUNCTIONS.—Subsection (d) of section 1801 of the Homeland Security Act of 2002 is amended by—

(1) striking paragraph (2); and

(2) redesignating paragraph (3) as paragraph (2).

SEC. 633. ANNUAL REPORTING ON ACTIVITIES OF THE OFFICE OF EMERGENCY COMMUNICATIONS.

Subsection (f) of section 1801 of the Homeland Security Act of 2002 (6 U.S.C. 571) is amended to read as follows:

"(f) ANNUAL REPORTING OF OFFICE ACTIVITIES.—The Director of the Office of Emergency Communications shall, not later than one year after the date of the enactment of this subsection and annually thereafter for each of the next four years, report to the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on the activities and programs of the Office, including specific information on efforts to carry out paragraphs (4), (5), and (6) of subsection (c).".

SEC. 634. NATIONAL EMERGENCY COMMUNICATIONS PLAN.

Section 1802 of the Homeland Security Act of 2002 (6 U.S.C. 572) is amended—

(1) in subsection (a), in the matter preceding paragraph (1)—

(A) by striking ", and in cooperation with the Department of National Communications System (as appropriate),"; and

(B) by inserting ", but not less than once every five years," after "periodically"; and

(2) in subsection (c)—

(A) by redesignating paragraphs (3) through (10) as paragraphs (4) through (11), respectively; and

(B) by inserting after paragraph (2) the following new paragraph:

"(3) consider the impact of emerging technologies on the attainment of interoperable emergency communications;".

SEC. 635. TECHNICAL EDIT.

Paragraph (1) of section 1804(b) of the Homeland Security Act of 2002 (6 U.S.C. 574(b)), in the matter preceding subparagraph (A), by striking "Assistant Secretary for Grants and Planning" and inserting "Administrator of the Federal Emergency Management Agency".

SEC. 636. PUBLIC SAFETY BROADBAND NETWORK.

The Undersecretary of the National Protection and Programs Directorate of the Department of Homeland Security shall provide to the Committee on Homeland Se-

curity and the Committee on Energy and Commerce of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the Department of Homeland Security's responsibilities related to the development of the nationwide Public Safety Broadband Network authorized in section 6202 of the Middle Class Tax Relief and Job Creation Act of 2012 (47 U.S.C. 1422; Public Law 112–96), including information on efforts by the Department to work with the First Responder Network Authority of the Department of Commerce to identify and address cyber risks that could impact the near term or long term availability and operations of such network and recommendations to mitigate such risks.

SEC. 637. COMMUNICATIONS TRAINING.

The Under Secretary for Management of the Department of Homeland Security, in coordination with the appropriate component heads, shall develop a mechanism, consistent with the strategy required pursuant to section 4 of the Department of Homeland Security Interoperable Communications Act (Public Law 114–29; 6 U.S.C. 194 note), to verify that radio users within the Department receive initial and ongoing training on the use of the radio systems of such components, including interagency radio use protocols.

Subtitle C—Medical Preparedness

SEC. 641. CHIEF MEDICAL OFFICER.

Section 516 of the Homeland Security Act of 2002 (6 U.S.C. 321e) is amended—

(1) in subsection (c)—

(A) in the matter preceding paragraph (1), by inserting "and shall establish medical and human, animal, and occupational health exposure policy, guidance, strategies, and initiatives," before "including—";

(B) in paragraph (1), by inserting before the semicolon at the end the following: ", including advice on how to prepare for, protect against, respond to, recover from, and mitigate against the medical effects of terrorist attacks or other high consequence events utilizing chemical, biological, radiological, or nuclear agents or explosives";

(C) in paragraph (2), by inserting before the semicolon at the end the following: ", including coordinating the Department's policy, strategy and preparedness for pandemics and emerging infectious diseases";

(D) in paragraph (5), by inserting "emergency medical services and medical first responder stakeholders," after "the medical community,";

(E) in paragraph (6), by striking "and" at the end;

(F) in paragraph (7), by striking the period and inserting a semicolon; and

(G) by adding at the end the following new paragraphs:

"(8) ensuring that the workforce of the Department has evidence-based policy, standards, requirements, and metrics for occupational health and operational medicine programs;

"(9) directing and maintaining a coordinated system for medical support for the Department's operational activities;

"(10) providing oversight of the Department's medical programs and providers, including—

"(A) reviewing and maintaining verification of the accreditation of the Department's health provider workforce;

"(B) developing quality assurance and clinical policy, requirements, standards, and metrics for all medical and health activities of the Department;

"(C) providing oversight of medical records systems for employees and individuals in the Department's care and custody; and

"(D) providing medical direction for emergency medical services activities of the Department; and

"(11) as established under section 530, maintaining a medical countermeasures stockpile and dispensing system, as necessary, to facilitate personnel readiness, and protection for the Department's employees and working animals and individuals in the Department's care and custody in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, or pandemic."; and

(2) by adding at the end the following new subsection:

"(d) MEDICAL LIAISONS.—The Chief Medical Officer may provide medical liaisons to the components of the Department to provide subject matter expertise on medical

and public health issues and a direct link to the Chief Medical Officer. Such expertise may include the following:

"(1) Providing guidance on health and medical aspects of policy, planning, operations, and workforce health protection.

"(2) Identifying and resolving component medical issues.

"(3) Supporting the development and alignment of medical and health systems.

"(4) Identifying common gaps in medical and health standards, policy, and guidance, and enterprise solutions to bridge such gaps.".

SEC. 642. MEDICAL COUNTERMEASURES PROGRAM.

(a) IN GENERAL.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.), as amended by this Act, is further amended by adding at the end the following new section:

"SEC. 530. MEDICAL COUNTERMEASURES.

"(a) IN GENERAL.—The Secretary shall establish a medical countermeasures program to facilitate personnel readiness, and protection for the Department's employees and working animals and individuals in the Department's care and custody, in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, or pandemic, and to support Department mission continuity.

"(b) OVERSIGHT.—The Chief Medical Officer of the Department shall provide programmatic oversight of the medical countermeasures program established pursuant to subsection (a), and shall—

"(1) develop Department-wide standards for medical countermeasure storage, security, dispensing, and documentation;

"(2) maintain a stockpile of medical countermeasures, including antibiotics, antivirals, and radiological countermeasures, as appropriate;

"(3) preposition appropriate medical countermeasures in strategic locations nationwide, based on threat and employee density, in accordance with applicable Federal statutes and regulations;

"(4) provide oversight and guidance on dispensing of stockpiled medical countermeasures;

"(5) ensure rapid deployment and dispensing of medical countermeasures in a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, or pandemic;

"(6) provide training to Department employees on medical countermeasure dispensing; and

"(7) support dispensing exercises.

"(c) MEDICAL COUNTERMEASURES WORKING GROUP.—The Chief Medical Officer shall establish a medical countermeasures working group comprised of representatives from appropriate components and offices of the Department to ensure that medical countermeasures standards are maintained and guidance is consistent.

"(d) MEDICAL COUNTERMEASURES MANAGEMENT.—Not later than 180 days after the date of the enactment of this section, 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) STOCKPILE ELEMENTS.—In determining the types and quantities of medical countermeasures to stockpile under subsection (d), the Chief Medical Officer shall utilize, if available—

"(1) Department chemical, biological, radiological, and nuclear risk assessments; and

"(2) Centers for Disease Control and Prevention guidance on medical countermeasures.

"(f) REPORT.—Not later than 180 days after the date of the enactment of this section, the Chief Medical Officer shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on progress in achieving the requirements of this section.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002, as amended by this Act, is further amended by inserting after the item relating to section 529 the following new item:

"Sec. 530. Medical countermeasures.".

Subtitle D—Management

SEC. 651. MISSION SUPPORT.

(a) ESTABLISHMENT.—The Administrator of the Federal Emergency Management Agency shall designate an individual to serve as the chief management official and principal advisor to the Administrator on matters related to the management of the Federal Emergency Management Agency, including management integration in support of emergency management operations and programs.

(b) MISSION AND RESPONSIBILITIES.—The Administrator of the Federal Emergency Management Agency, acting through the official designated pursuant to subsection (a), shall be responsible for the management and administration of the Federal Emergency Management Agency, including with respect to the following:

(1) Procurement.

(2) Human resources and personnel.

(3) Information technology and communications systems.

(4) Real property investment and planning, facilities, accountable personal property (including fleet and other material resources), records and disclosure, privacy, safety and health, and sustainability and environmental management.

(5) Security for personnel, information technology and communications systems, facilities, property, equipment, and other material resources.

(6) Any other management duties that the Administrator may designate.

(c) MOUNT WEATHER EMERGENCY OPERATIONS AND ASSOCIATED FACILITIES.—Nothing in this section shall be construed as limiting or otherwise affecting the role or responsibility of the Assistant Administrator for National Continuity Programs with respect to the matters described in subsection (b) as such matters relate to the Mount Weather Emergency Operations Center and associated facilities. The management and administration of the Mount Weather Emergency Operations Center and associated facilities remains the responsibility of the Assistant Administrator for National Continuity Programs.

(d) REPORT.—Not later than 270 days after the date of the enactment of this Act, the Administrator of the Federal Emergency Management Agency 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 of the Senate a report that includes—

(1) a review of financial, human capital, information technology, real property planning, and acquisition management of headquarters and all regional offices of the Federal Emergency Management Agency; and

(2) a strategy for capturing financial, human capital, information technology, real property planning, and acquisition data.

SEC. 652. SYSTEMS MODERNIZATION.

Not later than 180 days after the date of the enactment of this Act, the Administrator of the Federal Emergency Management Agency 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 of the Senate a report on the Federal Emergency Management Agency's efforts to modernize its grants and financial information technology systems, including the following:

(1) A summary of all previous efforts to modernize such systems.

(2) An assessment of long term cost savings and efficiencies gained through such modernization effort.

(3) A capability needs assessment.

(4) Estimated quarterly costs.

(5) Estimated acquisition life cycle dates, including acquisition decision events.

SEC. 653. STRATEGIC HUMAN CAPITAL PLAN.

Subsection (c) of section 10102 of title 5, United States Code, is amended by striking "2007" and inserting "2018".

SEC. 654. OFFICE OF DISABILITY INTEGRATION AND COORDINATION OF DEPARTMENT OF HOMELAND SECURITY.

(a) OFFICE OF DISABILITY INTEGRATION AND COORDINATION.—

(1) IN GENERAL.—Section 513 of the Homeland Security Act of 2002 (6 U.S.C. 321b) is amended to read as follows:

"SEC. 513. OFFICE OF DISABILITY INTEGRATION AND COORDINATION.

"(a) IN GENERAL.—There is established within the Federal Emergency Management Agency an Office of Disability Integration and Coordination, which shall be headed by a Director.

"(b) MISSION.—The mission of the Office is to ensure that individuals with disabilities and other access and functional needs are included in emergency management activities throughout the Agency by providing guidance, tools, methods, and strategies for the purpose of equal physical program and effective communication access.

"(c) RESPONSIBILITIES.—In support of the mission of the Office, the Director shall—

"(1) provide 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) oversee Office staff and personnel responsible for disability integration in each regional office with respect to carrying out the mission of the Office;

"(3) liaise with the staff of the Agency including non-permanent employees, organizations representing individuals with disabilities, 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;

"(4) coordinate with the technical expert on the needs of children within the Agency to provide guidance and coordination on matters related to children with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

"(5) consult with organizations representing individuals with disabilities about access and functional needs in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

"(6) ensure the coordination and dissemination of best practices and model evacuation plans for individuals with disabilities;

"(7) collaborate with Agency leadership responsible for training to ensure that qualified experts develop easily accessible training materials and a curriculum for the training of emergency response providers, State, local, and tribal government officials, and others on the needs of individuals with disabilities;

"(8) coordinate with the Emergency Management Institute, Center for Domestic Preparedness, the Center for Homeland Defense and Security, U.S. Fire Administration, National Exercise Program, and National Domestic Preparedness Consortium to ensure that content related to persons with disabilities, access and functional needs, and children are integrated into existing and future emergency management trainings;

"(9) promote the accessibility of telephone hotlines and websites regarding emergency preparedness, evacuations, and disaster relief;

"(10) work 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;

"(11) ensure the availability of accessible transportation options for individuals with disabilities in the event of an evacuation;

"(12) provide guidance and implement policies to ensure that the rights and feedback of individuals with disabilities regarding post-evacuation residency and relocation are respected;

"(13) ensure 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 (Public Law 109–295; 120 Stat. 1425; 6 U.S.C. 744); and

"(14) any other duties as assigned by the Administrator.

"(d) DIRECTOR.—After consultation with organizations representing individuals with disabilities, the Administrator shall appoint a Director. The Director 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.

"(e) ORGANIZATIONS REPRESENTING INDIVIDUALS WITH DISABILITIES DEFINED.—For purposes of this section, 'organizations representing individuals with disabilities' shall mean the National Council on Disabilities and the Interagency Coordination Council on Preparedness and Individuals with Disabilities, among other appropriate disability organizations.".

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 513 and inserting the following new item:

"513. Office of Disability Integration and Coordination.".

(b) REPORTING.—

(1) REPORT TO CONGRESS.—Not later than 120 days after the date of the enactment of this section, the Administrator shall submit to Congress a report on the funding and staffing needs of the Office of Disability Integration and Coordination under section 513 of the Homeland Security Act of 2002, as amended by subsection (a).

(2) COMPTROLLER GENERAL REVIEW.—Not later than 120 days after the date of the submittal of the report under paragraph (1), the Comptroller General of the United States shall review the report to evaluate whether the funding and staffing needs described in the report are sufficient to support the activities of the Office of Disability Integration and Coordination.

TITLE VII—OTHER MATTERS

SEC. 701. DECISION REGARDING CERTAIN EXECUTIVE MEMORANDA.

Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security shall review existing Department of Homeland Security policy memoranda, including memoranda approved by prior Secretaries that remain in effect, to determine whether such memoranda should remain in effect and, if so, whether any of such memoranda should be modified.

SEC. 702. PERMANENT AUTHORIZATION FOR ASIA-PACIFIC ECONOMIC COOPERATION BUSINESS TRAVEL CARD PROGRAM.

Section 2(a) of the Asia-Pacific Economic Cooperation Business Travel Cards Act of 2011 (Public Law 112–54; 8 U.S.C. 1185 note) is amended by striking "During the 7-year period ending on September 30, 2018, the Secretary" and inserting "The Secretary".

SEC. 703. AUTHORIZATION OF APPROPRIATIONS FOR OFFICE OF INSPECTOR GENERAL.

There is authorized to be appropriated for the Office of the Inspector General of the Department of Homeland Security $175,000,000 for each of fiscal years 2018 and 2019.

SEC. 704. CANINE TEAMS.

The Commissioner of U.S. Customs and Border Protection may request additional canine teams when there is a justified and documented shortage and such additional canine teams would be effective for drug detection at the border.

SEC. 705. TECHNICAL AMENDMENTS TO THE HOMELAND SECURITY ACT OF 2002.

(a) TITLE I.—Section 103 of the Homeland Security Act of 2002 (6 U.S.C. 113), as amended by this Act, is further amended as follows:

(1) In subsection (a)(1)—

(A) in subparagraph (E), by striking "the Bureau of" and inserting "U.S."; and

(B) by adding at the end the following new subparagraph:

"(L) An Administrator of the Transportation Security Administration.".

(2) In subsection (d)(5), by striking "section 708" and inserting "section 707".

(b) TITLE II.—Title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended as follows:

(1) In section 202 (6 U.S.C. 122)—

(A) in subsection (c), in the matter preceding paragraph (1), by striking "Director of Central Intelligence" and inserting "Director of National Intelligence"; and

(B) in subsection (d)(2), by striking "Director of Central Intelligence" and inserting "Director of National Intelligence".

(2) In section 210E (6 U.S.C. 124l)—

(A) by striking subsection (e); and

(B) by redesignating subsection (f) as subsection (e).

(3) In section 223(1)(B) (6 U.S.C. 143(1)(B)), by striking "and" after the semicolon at the end.

(4) In section 225 (6 U.S.C. 145), by striking subsections (c) and (d).

(5) In section 228A(c)(1)(C), by striking "section 707" and inserting "section 706".

(c) TITLE III.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended as follows:

(1) In section 302 (6 U.S.C. 182), by striking "biological,," each places it appears and inserting "biological,".

(2) By redesignating the second section 319 (relating to EMP and GMD mitigation research and development) as section 320.

(d) TITLE IV.—Title IV of the Homeland Security Act of 2002 (6 U.S.C. 201 et seq.) is amended as follows:

(1) By redesignating section 402 (6 U.S.C. 202) as section 401.

(2) In section 401(4), as so redesignated, by striking "section 428" and inserting "section 426".

(3) By redesignating section 417 as section 416.

(4) By redesignating section 427 (6 U.S.C. 235) as section 425.

(5) In section 425, as so redesignated, by striking subsection (c).

(6) By redesignating section 428 (6 U.S.C. 236) as section 426.

(7) In section 426, as so redesignated, in—

(A) in subsection (e), by striking paragraphs (7) and (8);

(B) by striking subsections (g) and (h); and

(C) by redesignating subsection (i) as subsection (g).

(8) By redesignating section 429 (6 U.S.C. 237) as section 427.

(9) By redesignating section 430 (6 U.S.C. 238) as section 428.

(10) By striking section 431 (6 U.S.C. 239).

(11) By redesignating section 432 (6 U.S.C. 240) as section 429.

(12) By redesignating section 433 (6 U.S.C. 241) as section 430.

(13) By amending the subtitle D heading to read as follows: "**U.S. Immigration and Customs Enforcement**".

(14) In section 442 (6 U.S.C. 252)—

(A) in the section heading, by striking "**BUREAU OF BORDER SECURITY**" and inserting "**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT**";

(B) by striking "the Bureau of Border Security" each place it appears and inserting "U.S. Immigration and Customs Enforcement";

(C) by striking "Under Secretary for Border and Transportation Security" each place it appears and inserting "Secretary";

(D) by striking "Assistant Secretary" each place it appears and inserting "Director";

(E) by striking "the Bureau of Citizenship and Immigration Services" both places it appears and inserting "United States Citizenship and Immigration Services";

(F) in subsection (a)—

(i) in the subsection heading, by striking "OF BUREAU";

(ii) in paragraph (1) by striking "a bureau to be known as the 'Bureau of Border Security'" and inserting "U.S. Immigration and Customs Enforcement"; and

(iii) by amending paragraph (5) to read as follows:

"(5) MANAGERIAL ROTATION PROGRAM.—The Director of U.S. Immigration and Customs Enforcement shall implement a managerial rotation program under which employees of U.S. Immigration and Customs Enforcement holding positions involving supervisory or managerial responsibility and classified, in accordance with chapter 51 of title 5, United States Code, as a GS–14 or above, shall—

"(A) gain experience in all the major functions performed by U.S. Immigration and Customs Enforcement; and

"(B) work in at least one local office of U.S. Immigration and Customs Enforcement.".

(15) By striking section 445 (6 U.S.C. 255).

(16) By striking section 446 (6 U.S.C. 256).

(17) In the subtitle E heading, by inserting "**United States**" before "**Citizenship and Immigration Services**".

(18) In section 451 (6 U.S.C. 271)—

(A) in the section heading, by striking "**BUREAU OF**" and inserting "**UNITED STATES**";

(B) by striking "the Bureau of Citizenship and Immigration Services" each place it appears and inserting "United States Citizenship and Immigration Services";

(C) by striking "the Bureau of Border Security" each place it appears and inserting "U.S. Immigration and Customs Enforcement";

(D) in subsection (a)—

(i) in the subsection heading, by striking "OF BUREAU";

(ii) in paragraph (1), by striking "a bureau to be known as the 'Bureau of Citizenship and Immigration Services'" and inserting "the United States Citizenship and Immigration Services"; and

(iii) in paragraph (2)(C), by striking "Assistant Secretary" and inserting "Director"; and

(iv) by amending paragraph (4) to read as follows:

"(4) MANAGERIAL ROTATION PROGRAM.—The Director of United States Citizenship and Immigration Services shall implement a managerial rotation program under which employees of United States Citizenship and Immigration Services 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—

"(A) gain experience in all the major functions performed by United States Citizenship and Immigration Services; and

"(B) work in at least one field office and one service center of United States Citizenship and Immigration Services."; and

(E) in subsection (c)(2), in the matter preceding subparagraph (A), by striking "Bureau of Citizenship and Immigration Services" and inserting "United States Citizenship and Immigration Services".

(19) In section 452 (6 U.S.C. 272)—

(A) by striking "the Bureau of" each place it appears and inserting "United States"; and

(B) in subsection (f), in the subsection heading, by striking "BUREAU OF" and inserting "UNITED STATES".

(20) In section 453 (6 U.S.C. 273)—

(A) by striking "the Bureau of" each place it appears and inserting "United States"; and

(B) in subsection (a)(2), by striking "such bureau" and inserting "United States Citizenship and Immigration Services".

(21) In section 454 (6 U.S.C. 274)—

(A) by striking "the Bureau of" each place it appears and inserting "United States"; and

(B) by striking "pursuant to policies and procedures applicable to employees of the Federal Bureau of Investigation,".

(22) By striking section 455 (6 U.S.C. 271 note).

(23) By striking section 456 (6 U.S.C. 275).

(24) By striking section 459 (6 U.S.C. 276).

(25) By striking section 460 (6 U.S.C. 277).

(26) By striking section 461 (6 U.S.C. 278).

(27) By redesignating section 462 (6 U.S.C. 279) as section 455.

(28) In section 455, as so redesignated, in subsection (b)(2)(A), in the matter preceding clause (i)—

(A) by striking "the Bureau of Citizenship and Immigration Services" and inserting "United States Citizenship and Immigration Services"; and

(B) by striking "Assistant Secretary of the Bureau of Border Security" and inserting "Director of U.S. Immigration and Customs Enforcement".

(29) In section 471 (6 U.S.C. 291)—

(A) by striking the section heading and inserting "**REORGANIZATION AND PROHIBITION**";

(B) by striking subsection (a);

(C) by striking "(b) PROHIBITION.—";

(D) by striking "Bureau of Border Security or the Bureau of" and inserting "U.S. Immigration and Customs Enforcement and United States"; and

(E) by striking "two bureaus" each place it appears and inserting "two components".

(30) By striking section 472 (6 U.S.C. 292).

(31) By striking section 473 (6 U.S.C. 293).

(32) By striking section 474 (6 U.S.C. 294).

(33) By redesignating section 476 (6 U.S.C. 296) as section 472.

(34) In section 472, as so redesignated—

(A) by striking "the Bureau of Citizenship and Immigration Services" each place it appears and inserting "United States Citizenship and Immigration Services"; and

(B) by striking "the Bureau of Border Security" each place it appears and inserting "U.S. Immigration and Customs Enforcement".

(35) By striking section 477 (6 U.S.C. 297).

(36) By redesignating section 478 (6 U.S.C. 298) as section 473.

(37) In section 473, as so redesignated—

(A) in the section heading, by inserting "**ANNUAL REPORT ON**" before "**IMMIGRATION**";

(B) by striking subsection (b); and

(C) in subsection (a)—

(i) by striking "REPORT.—" and all that follows through "One year" and inserting "REPORT.—One year";

(ii) by redesignating paragraph (2) as subsection (b) and moving such subsection two ems to left; and

(iii) in subsection (b), as so redesignated—

(I) in the heading, by striking "INCLUDED" and inserting "INCLUDED"; and

(II) by redesignating subparagraphs (A) through (H) as paragraphs (1) through (8), respectively, and moving such paragraphs two ems to the left.

(e) TITLE V.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.) is amended as follows:

(1) In section 501 (6 U.S.C. 311)—

(A) in paragraph (8), by striking "section 502(a)(6)" and inserting "section 504(a)(6)";

(B) by redesignating paragraphs (9) through (14) as paragraphs (10) through (15), respectively; and

(C) by inserting after paragraph (8) the following new paragraph:

"(9) the term 'Nuclear Incident Response Team' means a resource that includes—

"(A) those entities of the Department of Energy that perform nuclear or radiological emergency support functions (including accident response, search response, advisory, and technical operations functions), radiation exposure functions at the medical assistance facility known as the Radiation Emergency Assistance Center/Training Site (REAC/TS), radiological assistance functions, and related functions; and

"(B) those entities of the Environmental Protection Agency that perform such support functions (including radiological emergency response functions) and related functions.".

(2) By striking section 502 (6 U.S.C. 312).

(3) In section 504(a)(3)(B) (6 U.S.C. 314(a)(3)(B)), by striking ", the National Disaster Medical System,".

(4) In section 506(c) (6 U.S.C. 316(c)), by striking "section 708" each place it appears and inserting "section 707".

(5) In section 509(c)(2) (6 U.S.C. 319(c)(2)), in the matter preceding subparagraph (A), by striking "section 708" and inserting "section 707".

(6) By striking section 524 (6 U.S.C. 321m).

(f) TITLE VI.—Section 601 of the Homeland Security Act of 2002 (6 U.S.C. 331) is amended by striking "Director of Central Intelligence" each place it appears and inserting "Director of National Intelligence".

(g) TITLE VII.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.) is amended as follows:

(1) By striking section 706 (6 U.S.C. 346).

(2) By redesignating section 707 (6 U.S.C. 347) as section 706.

(3) By redesignating section 708 as section 707.

(4) By redesignating section 709 as section 708.

(5) In section 708, as so redesignated, in subsection (c)(3), by striking "section 707" and inserting "section 706".

(h) TITLE VIII.—Title VIII of the Homeland Security Act of 2002 (6 U.S.C. 361 et seq.) is amended as follows:

(1) By redesignating section 812 as section 811.

(2) In section 811, as so redesignated—

(A) by striking subsections (a) and (c); and

(B) in subsection (b)—

(i) by striking "(as added by subsection (a) of this section)" each place it appears;

(ii) by redesignating paragraphs (2) through (4) as subsections (b) through (d), respectively, and by moving such subsections, as so redesignated, two ems to the left;

(iii) in paragraph (1), by redesignating subparagraphs (A) and (B) as paragraphs (1) and (2), respectively, and by moving such paragraphs, as so redesignated, two ems to the left; and

(iv) by striking "(b) PROMULGATION OF INITIAL GUIDELINES.—" and all that follows through "In this subsection" and inserting the following:

"(a) DEFINITION.—In this section";

(C) in subsection (b), as so redesignated, by striking "IN GENERAL" and inserting "IN GENERAL";

(D) in subsection (c), as so redesignated, by striking "MINIMUM REQUIREMENTS" and inserting "MINIMUM REQUIREMENTS"; and

(E) in subsection (d), as so redesignated, by striking "NO LAPSE OF AUTHORITY" and inserting "NO LAPSE OF AUTHORITY".

(3) In section 843(b)(1)(B) (6 U.S.C. 413(b)(1)(B)), by striking "as determined by" and all that follows through "; and" and inserting "as determined by the Secretary; and".

(4) By striking section 857 (6 U.S.C. 427).

(5) By redesignating section 858 (6 U.S.C. 428) as section 857.

(6) By striking section 872 (6 U.S.C. 452).

(7) By striking section 881 (6 U.S.C. 461).

(8) In section 892 (6 U.S.C. 482)—

(A) in subsection (b)(7), by striking "Director of Central Intelligence" and inserting "Director of National Intelligence"; and

(B) in subsection (c)(3)(D), by striking "Director of Central Intelligence" and inserting "Director of National Intelligence".

(9) By striking section 893 (6 U.S.C. 483).

(10) By redesignating section 894 (6 U.S.C. 484) as section 893.

(i) TITLE IX.—Section 903(a) of the Homeland Security Act of 2002 (6 U.S.C. 493(a)) is amended in the subsection heading by striking "MEMBERS—" and inserting "MEMBERS.—".

(j) TITLE X.—Section 1001(c)(1) of the Homeland Security Act of 2002 (6 U.S.C. 511(c)(1)) is amended by striking "Director of Central Intelligence" and inserting "Director of National Intelligence".

(k) TITLE XV.—Title XV of the Homeland Security Act of 2002 (6 U.S.C. 541 et seq.) is amended as follows:

(1) By striking section 1502 (6 U.S.C. 542).

(2) By redesignating section 1503 (6 U.S.C. 543) as section 1502.

(l) TITLE XVI.—Section 1611(d)(1) of the Homeland Security Act of 2002 (6 U.S.C. 563(d)(1)) is amended by striking "section 707" and inserting "section 706".

(m) TITLE XIX.—Section 1902(b)(3) of the Homeland Security Act of 2002 (6 U.S.C. 592(b)(3)) is amended—

(1) in the paragraph heading, by striking "HAWAIIAN NATIVE-SERVING" and inserting "NATIVE HAWAIIAN-SERVING"; and

(2) by striking "Hawaiian native-serving" and inserting "Native Hawaiian-serving".

(n) TITLE XX.—Section 2021 of the Homeland Security Act of 2002 (6 U.S.C. 611) is amended—

(1) by striking subsection (c); and

(2) by redesignating subsection (d) as subsection (c).

(o) TABLE OF CONTENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended as follows:

(1) By striking the items relating to sections 317, 319, 318, and 319 and inserting the following new items:

"Sec. 317. Promoting antiterrorism through international cooperation program.
"Sec. 318. Social media working group.
"Sec. 319. Transparency in research and development.
"Sec. 320. EMP and GMD mitigation research and development.".

(2) By striking the items relating to sections 401 and 402 and inserting the following new item:

"Sec. 401. Border, maritime, and transportation responsibilities.".

(3) By striking the item relating to section 417 and inserting the following new item:

"Sec. 416. Allocation of resources by the Secretary.".

(4) By striking the items relating to sections 427 through 433 and inserting the following new items:

"Sec. 425. Coordination of information and information technology.
"Sec. 426. Visa issuance.
"Sec. 427. Information on visa denials required to be entered into electronic data system.
"Sec. 428. Office for Domestic Preparedness.
"Sec. 429. Border Enforcement Security Task Force.
"Sec. 430. Prevention of international child abduction.".

(5) By striking the items relating to sections 445 and 446.

(6) By amending the item relating to subtitle E of title IV to read as follows:

"Subtitle E—United States Citizenship and Immigration Services".

(7) By amending the item relating to section 451 to read as follows:

"Sec. 451. Establishment of United States Citizenship and Immigration Services.".

(8) By striking the items relating to sections 455, 456, 459, 460, and 461 and inserting before the item relating to section 457 the following new item:

"Sec. 455. Children's affairs.".

(9) By amending the item relating to section 471 to read as follows:

"Sec. 471. Reorganization and prohibition.".

(10) By striking the items relating to sections 472 through 478 and inserting the following new items:

"Sec. 472. Separation of funding.
"Sec. 473. Annual report on immigration functions.".

(11) By striking the item relating to section 502.

(12) By striking the item relating to section 524.

(13) By striking the items relating to sections 706 through 709 and inserting the following new items:

"Sec. 706. Quadrennial Homeland Security Review.
"Sec. 707. Joint Task Forces.
"Sec. 708. Office of Strategy, Policy, and Plans.".

(14) By striking the items relating to sections 811 and 812 and inserting the following new item:

"Sec. 811. Law enforcement powers of Inspector General agents.".

(15) By striking the items relating to sections 857 and 858 and inserting the following new item:

"Sec. 857. Identification of new entrants into the Federal marketplace.".

(16) By striking the item relating to section 872.

(17) By striking the item relating to section 881.

(18) By striking the items relating to sections 893 and 894 and inserting the following new item:

"Sec. 893. Authorization of appropriations.".

(19) By striking the items relating to sections 1502 and 1503 and inserting the following new item:

"Sec. 1502. Review of congressional committee structures.".

PURPOSE AND SUMMARY

The purpose of H.R. 2825 is to authorize the activities of the Department of Homeland Security (DHS) by asserting Congress's Article I authority to legislate and provide authority and direction to DHS. It is the proper role of Congress to provide proper guidance to ensure that the Department's structure and focus are best linked to securing the homeland. This bill provides oversight of and direction to the Department in numerous areas to ensure that it is effectively carrying out the mission of securing the homeland.

H.R. 2825 aims to create efficiencies and streamline programs and offices by clarifying and uniting the offices that constitute "DHS Headquarters."

Further, this legislation integrates existing DHS intelligence systems and data sets into the data framework; creates a FEMA Chief Management Official to achieve further efficiencies and accountability modernizing internal functions; strengthens the role of the Under Secretary for Management to implement efficiencies across components to better ensure proper oversight and accountability; and requires DHS to review the organization of its offices with research and development and chemical, biological, radiological, nuclear and explosives activities to ensure an efficient and streamlined organizational structure that eliminates duplication.

This legislation protects taxpayer dollars and holds DHS accountable by directing the Department to develop a multi-year acquisition strategy resulting in major acquisitions programs be subject to greater Departmental oversight throughout the acquisition process to ensure they meet key cost, schedule and performance requirements.

Further, H.R. 2825 mandates DHS to find cost savings through real property consolidation and other common sense efforts, strengthens the role of the Chief Information Officer to forge stronger information technology collaboration to save taxpayer dollars; empowers the Chief Financial Officer to continue progress made on the Department's financial statement audits and improve internal controls to better safeguard against waste, fraud, and abuse; and ensures terrorism grant funds are used efficiently to close identified capability gaps while mandating a transparent system that measures the return on these investments.

Finally, H.R. 2825 support America's front-line defenders and first responders and improves the security of our Nation.

The legislation provides resources, including training and equipment, to first responders to counter existing and evolving terrorist threats; improves agency morale by implementing workforce planning efforts; eliminates unnecessary and duplicative human capital policies; better addresses employee misconduct; maintains support for State and local law enforcement presence at airports; ensures the FEMA Administrator has the benefit of expert law enforcement advice; and allows DHS to better focus on recruiting, retraining, and training a qualified workforce.

The legislation makes important enhancements to information sharing efforts within DHS and between the Department and State, local, Tribal and territorial partners. It provides resources to secure passenger surface transportation and improve security at our Nation's ports; directs the Department to share with State, local and regional fusion centers release information of certain individuals convicted of terrorism; improves airport access controls, employee vetting, perimeter security, and insider threat mitigation efforts; and expands the use of explosive–detecting K-9 teams.

BACKGROUND AND NEED FOR LEGISLATION

In the aftermath of the September 11th terrorist attacks on our Nation, President Bush and Congress examined ways to improve our national security. This led to the creation of the Department of Homeland Security through the passage of the Homeland Security Act of 2002 (Pub. L. 107–296). Since this original authorization 15 years ago, DHS has never been reauthorized. It has received guidance from annual appropriations legislation, but it has not received the thorough guidance that comes from a comprehensive authorization of its activities.

One of the most important responsibilities of Congress is to assert its Article I authority and pass authorizing legislation that provides direction to key offices and missions of Federal agencies.

The United States faces dynamic national security challenges brought forth by terrorists, human traffickers, drug smugglers, and state and non-state actors waging a silent war in cyberspace. America's enemies are agile and are constantly looking for ways to inflict damage. Our government and our nation must stay ahead of

these ever-evolving threats by reforming and improving the Department of Homeland Security through a first ever reauthorization.

HEARINGS

No hearings were held on H.R. 2825 in the 115th Congress. However, the Committee held the following oversight hearings which informed the legislation:

115th Congress

The Committee held a hearing on June 7, 2017, entitled "Department of Homeland Security Reauthorization and the President's FY 2018 Budget Request." The Committee received testimony by Hon. John F. Kelly, Secretary, U.S. Department of Homeland Security.

On February 28, 2017, the Subcommittee on Emergency Preparedness, Response, and Communications held a hearing entitled "The Future of FEMA: Recommendations of Former Administrators." The Subcommittee received testimony from Hon. W. Craig Fugate, Former Administrator, Federal Emergency Management Agency, U.S. Department of Homeland Security; and Hon. R. David Paulison, Former Administrator, Federal Emergency Management Agency, U.S. Department of Homeland Security.

On February 16, 2017, the Subcommittee on Oversight and Management Efficiency held a hearing entitled "Watchdog Recommendations: A Better Way Ahead to Manage the Department of Homeland Security." The Subcommittee received testimony from Hon. John Roth, Inspector General, U.S. Department of Homeland Security; and Ms. Rebecca Gambler, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office.

On February 14, 2017, the Subcommittee on Emergency Preparedness, Response, and Communications held a hearing entitled "The Future of the FEMA: Stakeholder Recommendations for the Next Administrator." The Subcommittee received testimony from Captain Chris A. Kelenske, Deputy State Director/Commander, Emergency Management and Homeland Security, Michigan State Police, *testifying on behalf of the National Governors Association*; Chief John Sinclair, Fire Chief, Kittitas Valley Fire and Rescue (WA), *testifying on behalf of the International Association of Fire Chiefs*; and Richard F. Bland, J.D., M.T.S. National Director, Policy, Advocacy and Development, Save the Children.

On February 2, 2017, the Subcommittee on Transportation and Protective Security held a hearing entitled "The Future of the Transportation Security Administration." The Subcommittee received testimony from Mr. Roger Dow, CEO, U.S. Travel Association; Ms. Nina E. Brooks, Head of Security, Airports Council International; and Mr. J. David Cox, National President, American Federation of Government Employees.

114th Congress

On September 8, 2016, the Subcommittee on Counterterrorism and Intelligence held a hearing entitled "State and Local Perspectives on Federal Information Sharing." The Subcommittee received testimony from Chief Richard Beary, Immediate Past President, International Association of Chiefs of Police; Mr. Mike Sena, President, National Fusion Center Association; and Dr. Cedric Alex-

ander, National President, National Organization of Black Law Enforcement Executives (NOBLE).

On July 13, 2016, the Subcommittee on Counterterrorism and Intelligence held a hearing entitled "Counterintelligence and Insider Threats: How Prepared is the Department of Homeland Security?" The Subcommittee received testimony from Hon. Francis X. Taylor, Under Secretary, Office of Intelligence and Analysis, U.S. Department of Homeland Security; Col. Richard D. McComb, Chief Security Officer, U.S. Department of Homeland Security; and Rdml. Robert Hayes, Assistant Commandant for Intelligence, U.S. Coast Guard, U.S. Department of Homeland Security.

On July 7, 2016, the Subcommittee on Coast Guard and Maritime Transportation of the Committee on Transportation and Infrastructure and the Subcommittee on Border and Maritime Security held a joint hearing entitled "An Examination of the Maritime Nuclear Smuggling Threat." The Subcommittees received testimony from Rear Admiral Linda L. Fagan, Deputy Commandant for Operations, Policy, and Capabilities, U.S. Coast Guard, U.S. Department of Homeland Security; Dr. Todd C. Owen, Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection, U.S. Department of Homeland Security; Dr. Wayne Brasure, Acting Director, Domestic Nuclear Detection Office; Ms. Anne Harrington, Deputy Administrator, Defense Nuclear Nonproliferation, National Nuclear Security Administration; Ms. Jennifer Grover, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office; Dr. Gregory H. Canavan, Senior Fellow, Los Alamos National Laboratories; Mr. David A. Espie, Director of Security, Maryland Port Administration, Port of Baltimore; and Mr. James H.I. Weakley, President, Lake Carriers' Association.

On June 21, 2016, the Subcommitteeon Emergency Preparedness, Response, and Communications held a field hearing in Jersey City, New Jersey entitled "Protecting Our Passengers: Perspectives on Securing Surface Transportation in New Jersey and New York." The Subcommittee received testimony from Ms. Sonya Proctor, Director, Surface Division, Office of Security Policy and Industry Engagement, Transportation Security Administration, U.S. Department of Homeland Security; Mr. Thomas Belfiore, Chief Security Officer, The Port Authority of New York and New Jersey; Mr. Raymond Diaz, Director of Security, Metropolitan Transportation Authority (New York); Mr. Christopher Trucillo, Chief of Police, New Jersey Transit Police Department; Mr. Martin Conway, Deputy Police Chief, National Railroad Passenger CorporationAMTRAK; Sergeant W. Greg Kierce, Director, Office of Emergency Management and Homeland Security, City of Jersey City, New Jersey; Mr. Rick Sposa, Operations Coordinator, Emergency Medical Services, Jersey City Medical Center; Lieutenant Vincent Glenn, Commander, Emergency Services Unit, Police Department, Jersey City, New Jersey; Captain Richard D. Gorman, Department of Fire and Emergency Services, Office of Emergency Management and Homeland Security, Jersey City, New Jersey; and Mr. Mike Mollahan, Trustee, Port Authority Police Benevolent Association.

On May 24, 2016, the Subcommittee on Emergency Preparedness, Response, and Communications and the Subcommittee on Cy-

bersecurity, Infrastructure Protection, and Security Technologies held a joint hearing entitled "Enhancing Preparedness and Response Capabilities to Address Cyber Threats." The Subcommittees received testimony from Mr. Mark Ghilarducci, Director, Emergency Services, Office of the Governor, State of California; Lt. Col. Daniel J. Cooney, Assistant Deputy Superintendent, Office of Counter Terrorism, New York State Police; Brig. Gen. Steven Spano (Ret.—USAF), President and Chief Operating Officer, Center for Internet Security; Mr. Mark Raymond, Vice President, National Association of State Chief Information Officers; and Mr. Robert Galvin, Chief Technology Officer, Port Authority of New York and New Jersey.

On March 15, 2016, the Subcommittee held a hearing entitled "State of Emergency: The Disaster of Cutting Preparedness Grants." The Subcommittee received testimony from the Hon. Bill de Blasio, Mayor, City of New York, New York; Mr. Jim Butterworth, Director, Emergency Management/Homeland Security, State of Georgia, *testifying on behalf of the National Emergency Management Association*, Ms. Rhoda Mae Kerr, Fire Chief, City of Austin Fire Department, Austin, Texas, *testifying on behalf of the International Association of Fire Chiefs*, Mr. George Turner, Chief of Police, Atlanta Police Department, Atlanta, Georgia, *testifying on behalf of the Major Cities Chiefs Association*; Mr. Mike Sena, Director, Northern California Regional Intelligence Center, *testifying on behalf of the National Fusion Center Association*; and Sergeant W. Greg Kierce, Director, Office of Emergency Management and Homeland Security, City of Jersey City, New Jersey.

On March 2, 2016, the Subcommittee on Transportation Security held a hearing entitled "The Transportation Security Administration's FY2017 Budget Request." The Subcommittee received testimony from Hon. Peter V. Neffenger, Administrator, Transportation Security Administration, U.S. Department of Homeland Security.

On February 11, 2016, the Subcommittee held a hearing entitled, "Improving the Department of Homeland Security's Biological Detection and Surveillance Programs." The Subcommittee received testimony from Dr. Kathryn Brinsfield, Assistant Secretary, Office of Health Affairs, U.S. Department of Homeland Security; Dr. Reginald Brothers, Under Secretary for Science and Technology, U.S. Department of Homeland Security; Mr. Chris P. Currie, Director, Emergency Management, National Preparedness, and Critical Infrastructure Protection, Homeland Security and Justice Team, U.S. Government Accountability Office.

On December 8, 2015, the Subcommittee on Transportation Security held a hearing entitled "Examining TSA's Global Efforts to Protect the Homeland from Aviation Threats and Enhance Security at Last Point of Departure Airports." The Subcommittee received testimony from Mr. Joseph P. Terrell, Deputy Assistant Administrator, Office of Global Strategies, Transportation Security Administration, U.S. Department of Homeland Security.

On November 3, 2015, the Committee held a hearing entitled "Defending Against Bioterrorism: How Vulnerable is America?" The Committee received testimony from Hon. Thomas J. Ridge, Co–Chair, Blue Ribbon Study Panel on Biodefense; Hon. Joseph I. Lieberman, Co–Chair, Blue Ribbon Study Panel on Biodefense; and Leonard A. Cole, PhD, Director, Terror Medicine and Security Pro-

gram, Department of Emergency Medicine, Rutgers New Jersey Medical School.

On October 28, 2015, the Subcommittee on Counterterrorism and Intelligence held a hearing entitled "Terror Inmates: Countering Violent Extremism in Prison and Beyond." The Subcommittee received testimony from Mr. Jerome P. Bjelopera, Specialist in Organized Crime and Terrorism, Congressional Research Service, Library of Congress; Mr. Tony C. Parker, Assistant Commissioner, Department of Correction, State of Tennessee; and Mr. Brian Levin, Professor, Department of Criminal Justice, Director, Center for Study of Hate and Extremism, California State University, San Bernardino.

On October 22, 2015, the Subcommittee held a hearing entitled "Ready and Resilient?: Examining Federal Emergency Preparedness and Response Capabilities." The Subcommittee received testimony from the Hon. W. Craig Fugate, Administrator, Federal Emergency Management Agency, U.S. Department of Homeland Security; Mr. Bryan Koon, Director, Florida Division of Emergency Management, *testifying on behalf of the National Emergency Management Association*; and Mr. Chris P. Currie, Director, Emergency Management, National Preparedness, and Critical Infrastructure Protection, Homeland Security and Justice Team, U.S. Government Accountability Office.

On October 8, 2015, the Subcommittee on Border and Maritime Security held a hearing entitled "Reform and Improvement: Assessing the Path Forward for the Transportation Security Administration." The Subcommittee received testimony from The Honorable John Roth, Inspector General, Office of Inspector General, U.S. Department of Homeland Security; and The Honorable Peter Neffenger, Administrator, Transportation Security Administration, U.S. Department of Homeland Security.

On September 18, 2015, the Subcommittee on Oversight and Management Efficiency held a hearing entitled "Making DHS More Efficient: Industry Recommendations to Improve Homeland Security." The Subcommittee received testimony from Mr. Marc A. Pearl, President and Chief Executive Officer, Homeland Security and Defense Business Council; Mr. Harry Totonis, Board Director, Business Executives for National Security; and Hon. Elaine Duke, Principal, Elaine Duke & Associates, LLC.

On September 17, 2015, the Subcommittee on Transportation Security and the Subcommittee on Counterterrorism and Intelligence held a joint hearing entitled "Safeguarding our Nation's Surface Transportation Systems Against Evolving Terrorist Threats." The Subcommittees received testimony from Mr. Eddie Mayenschein, Assistant Administrator, Office of Security Policy and Industry Engagement, Transportation Security Administration, U.S. Department of Homeland Security; Ms. Jennifer Grover, Director, Transportation Security and Coast Guard Issues, Homeland Security and Justice Team, U.S. Government Accountability Office; Mr. Raymond Diaz, Director of Security, Metropolitan Transportation Authority (New York); and Ms. Polly Hanson, Chief of Police, National Railroad Passenger Corporation (Amtrak).

On July 14, 2015, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and the Subcommittee on Emergency Preparedness, Response, and Commu-

nications held a joint hearing entitled "Weapons of Mass Destruction: Bolstering DHS to Combat Persistent Threats to America." The Subcommittees received testimony from Dr. Reginald Brothers, Under Secretary for Science and Technology, U.S. Department of Homeland Security; Dr. Kathryn Brinsfield, Assistant Secretary, Office of Health Affairs, U.S. Department of Homeland Security; Dr. Huban Gowadia, Director, Domestic Nuclear Detection Office, U.S. Department of Homeland Security; Mr. Alan D. Cohn, Counsel, Steptoe & Johnson LLP; Mr. Rick "Ozzie" Nelson, Senior Associate, Homeland Security and Counterterrorism Program, Center for Strategic and International Studies; and Mr. Warren Stern, Former Director, Domestic Nuclear Detection Office, U.S. Department of Homeland Security.

On April 30, 2015, the Subcommittee on Transportation Security held a hearing entitled "A Review of Access Control Measures at Our Nation's Airports, Part II." The Subcommittee received testimony from Mr. Melvin J. Carraway, Acting Administrator, Transportation Security Administration, U.S. Department of Homeland Security; Jeanne M. Olivier, A.A.E., Assistant Director, Aviation Security and Technology, Security Operations and Programs Department, The Port Authority of New York & New Jersey, *testifying on behalf of The American Association of Airport Executives*; and Mr. Steven Grossman, Chief Executive Officer/Executive Director, Jacksonville International Airport, Jacksonville Aviation Authority, *testifying on behalf of The Airports Council International, North America*.

On April 22, 2015, the Subcommittee on Oversight and Management Efficiency held a hearing entitled "Acquisition Oversight: How Effectively Is DHS Safeguarding Taxpayer Dollars?" The Subcommittee received testimony from Ms. Michele Mackin, Director, Acquisition and Sourcing Management, U.S. Government Accountability Office; Hon. Chip Fulghum, Chief Financial Officer, U.S. Department of Homeland Security; and Dr. Cedric Sims, Partner, Evermay Consulting Group.

On April 22, 2015, the Subcommittee on Emergency Preparedness, Response, and Communications held a hearing entitled "Strategic Perspectives on the Bioterrorism Threat." The Subcommittee received testimony from the Hon. Jim Talent, Former Senator from the State of Missouri and Co–Chair, the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism; Dr. Charles B. Cairns, Interim Dean, Health Sciences Center, University of Arizona College of Medicine; and Marisa Raphael, MPH, Deputy Commissioner, Office of Emergency Planning and Response, Department of Health and Mental Hygiene, New York City, New York.

On March 18, 2015, the Subcommittee on Emergency Preparedness, Response, and Communications held a hearing entitled "Unmanned Aerial System Threats: Exploring Security Implications and Mitigation Technologies." The Subcommittee received testimony from Dr. Todd E. Humphreys, Assistant Professor, Cockrell School of Engineering, The University of Texas at Austin; Major General Frederick Roggero, (USAF–Ret.), President and Chief Executive Officer, Resilient Solutions, Ltd.; Chief Richard Beary, President, International Association of Chiefs of Police; and Greg-

ory S. McNeal, JD/PhD, Associate Professor, School of Law, Pepperdine University.

On February 26, 2015, the Subcommittee on Counterterrorism and Intelligence held a hearing entitled "Addressing Remaining Gaps in Federal, State, and Local Information Sharing." The Subcommittee received testimony from Mr. Mike Sena, President, National Fusion Center Association; Chief Richard Beary, President, International Association of Chiefs of Police; and Dr. Cedric Alexander, National President, National Organization of Black Law Enforcement Executives (NOBLE).

On February 26, 2015, the Subcommittee on Oversight and Management Efficiency held a hearing entitled "Assessing DHS's Performance: Watchdog Recommendations to Improve Homeland Security." The Subcommittee received testimony from Hon. John Roth, Inspector General, U.S. Department of Homeland Security; Ms. Rebecca Gambler, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office; and Dr. Daniel M. Gerstein, Senior Policy Researcher, The RAND Corporation.

113th Congress

On November 18, 2014, the Subcommittee on Emergency Preparedness, Response, and Communications held a hearing entitled "Interoperable Communications: Assessing Progress Since 9/11." The Subcommittee received testimony from RdAM Ronald Hewitt, (USCG Ret.), Director, Office of Emergency Communications, U.S. Department of Homeland Security; Mr. TJ Kennedy, Acting General Manager, First Responder Network Authority; and Mr. Mark A. Grubb, Director, Division of Communications, Department of Safety and Homeland Security, State of Delaware.

On October 10, 2014, the Committee held a field hearing in Dallas, Texas, entitled "Ebola in the Homeland: The Importance of Effective International, Federal, State and Local Coordination." The Committee received testimony from Dr. Toby Merlin, Director, Division of Preparedness and Emerging Infection, National Center for Emerging and Zoonotic Infectious Diseases, Center for Disease Control and Prevention; Kathryn Brinsfield, MD, MPH, FACEP, Acting Assistant Secretary and Chief Medical Officer, Office of Health Affairs, U.S. Department of Homeland Security; Mr. John P. Wagner, Acting Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection, U.S. Department of Homeland Security; Dr. David L. Lakey, Commissioner of Health, Texas Department of State Health Services; Dr. Brett P. Giroir, Executive Vice President and CEO, Texas A&M Health Science Center, Texas A&M University, Director, Texas Task Force on Infectious Disease Preparedness and Response; Hon. Clay Lewis Jenkins, Judge, Dallas County, Texas; and Catherine L. Troisi, Ph.D., Associate Professor, Division of Management, Policy, and Community Health, Center for Infectious Diseases, The University of Texas.

On June 10, 2014, the Subcommittee on Emergency Prepardness, Response, and Communications held a hearing entitled "BioWatch: Lessons Learned and the Path Forward." The Subcommittee received testimony from Dr. Kathryn Brinsfield, Acting Assistant Secretary, Office of Health Affairs, U.S. Department of Homeland Security; Dr. Reginald Brothers, Under Secretary, Science and

Technology Directorate, U.S. Department of Homeland Security; Mr. Chris Cummiskey, Acting Under Secretary, Management Directorate, U.S. Department of Homeland Security; Mr. Chris Currie, Acting Director, Homeland Security and Justice Issues, U.S. Government Accountability Office; and Dr. Deena S. Disraelly, Research Staff, Strategy, Forces and Resources Division, Institute for Defense Analyses.

On April 8, 2014, the Subcommittee on Border and Maritime Security held a hearing entitled "Authorizing U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement." The Subcommittee received testimony from Mr. Kevin K. McAleenan, Acting Deputy Commissioner, U.S. Customs and Border Protection, U.S. Department of Homeland Security; and Mr. Daniel H. Ragsdale, Acting Director, U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security.

On February 11, 2014, the Subcommittee on Emergency Prepardness, Response, and Communications held a hearing entitled "Bioterrorism: Assessing the Threat." The Subcommittee received testimony from Dr. Robert P. Kadlec, Former Special Assistant to the President for Biodefense; Dr. Tom Inglesby, CEO and Director, University of Pittsburgh Medical Center for Health Security; and Dr. Leonard Cole, Director, Terror Medicine and Security, Department of Emergency Medicine, Rutgers New Jersey Medical School.

COMMITTEE CONSIDERATION

The Committee met on June 14, 2017, to consider H.R. 2825, and ordered the measure to be reported to the House with a favorable recommendation, amended, by voice vote. The Committee took the following actions:

The following amendments were offered:

An Amendment in the Nature of a Substitute offered by MR. MCCAUL (#1); was AGREED TO, as amended by voice vote.

An en bloc amendment to the Amendment in the Nature of a Substitute to H.R. 2825 offered by MR. MCCAUL (#1A); was AGREED TO by voice vote.

Consisting of the following amendments:

An amendment to the Amendment in the Nature of a Substitute offered by MR. PERRY (en bloc amendment 1):

Page 16, line 12, strike "and".

Page 16, line 15, strike the first period, the closing quotes, and the second period, and insert "; and".

Page 16, beginning line 16, insert the following:

"(10) track, approve, oversee, and make public information on expenditures by components of the Department for conferences, as appropriate, including by requiring each component to-

"(A) report to the Inspector General of the Department the expenditures by such component for each conference hosted or attended by Department employees for which the total expenditures of the Department exceed $20,000, within 15 days after the date of the conference; and "(B) with respect to such expenditures, provide to the Inspector General-

"(i) the information described in subsections (a), (b), and (c) of section 739 of title VII of division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Public Law 113-235); and "(ii) documentation of such expenditures.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON of Mississippi (en bloc amendment 2):

Page 6, beginning line 7, insert the following : "Subtitle A-Headquarters Operations"

Page 60, beginning line 14, insert a new subtitle entitled "Subtitle B-Human Resources".

An amendment to the Amendment in the Nature of a Substitute offered by MR. FITZPATRICK (en bloc amendment 3):
In section 111, redesignate subsections (a) and (b) as subsections (b) and (c).
In section 111, insert before subsection (b), a new subsection entitled "(a) Sense of Congress."

An amendment to the Amendment in the Nature of a Substitute offered by MS. JACKSON LEE (en bloc amendment 4):
Page 9, beginning line 24, insert the following:
"(H) establish and implement, in consultation with the Office of Civil Rights and Civil Liberties, policies which preserve individual liberty, fairness, and equality under the law;".
Page 29, line 16 insert before the semicolon the following: ", in consultation with the Office for Civil Rights and Civil Liberties".

An amendment to the Amendment in the Nature of a Substitute offered by MR. RICHMOND (en bloc amendment 5):
In title I, insert after section 111 a new section (and redesignate subsequent sections accordingly) the following "Sec. 112. Office for Civil Rights and Civil Liberties."
Page 173, line 22, insert "OMBUDSMAN," before "AND".
Page 173, line 25, insert "Ombudsman," before "and".
Page 174, line 5, insert "Ombudsman," before "and".
Page 174, line 10, strike "ensuring that the traveling public" and insert "managing allegations of violations of civil rights and civil liberties from the public, carrying out the Administration's equal employment opportunity and diversity policies and programs, including complaint management and adjudication, and helping to ensure that employees and the traveling public".

An amendment to the Amendment in the Nature of a Substitute offered by MR. PAYNE (en bloc amendment 6):
At the end of title I, add a new section entitled "Sec. 118. Activities Related to Children."
At the end of subtitle A of title VI, add a new section entitled "Sec. 623. Technical Expert Authorized.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. PAYNE (en bloc amendment 7):
Page 58, line 13, after "Department" insert ", including a specific description of operational challenges resulting from the current organizational structure and a detailed explanation of how the proposed organizational structure will address such challenges".
Page 58, line 18, strike "the" and insert "any".
Page 58, line 22, after "changes" insert ", an explanation of why no statutory or organizational changes are necessary, or a request for additional time to complete the organizational justification".
Page 60, line 8, after "Department" insert ", including a specific description of operational challenges resulting from the current organizational structure and a detailed explanation of how the proposed organizational structure will address such challenges".
Page 60, line 9, strike "the" and insert "any".
Page 60, line 13, after "changes" insert ", an explanation of why no statutory or organizational changes are necessary, or a request for additional time to complete the organizational justification.".
Page 60, after line 13, a new subsection entitled "(c) Review Required.-"

An amendment to the Amendment in the Nature of a Substitute offered by MRS. WATSON COLEMAN (en bloc amendment 8):
Page 37, line 12, after "matters" insert the following: ", including advice with respect to the preparation of the Quadrennial Homeland Security Review".

An amendment to the Amendment in the Nature of a Substitute offered by MRS. WATSON COLEMAN (en bloc amendment 9):
Page 60, after line 13, insert a new section entitled "Sec. ____. Center for Faith-based Neighborhood Partnerships.".

An amendment to the Amendment in the Nature of a Substitute offered by MISS RICE of New York (en bloc amendment 10):
Add at the end to title I a new section entitled "Sec. 118. Timely Guidance to DHS Personnel Regarding Executive Orders."

An amendment to the Amendment in the Nature of a Substitute offered by MR. RICHMOND (en bloc amendment 11):
At the end of title I, add a new section entitled "Sec. 118. Secretaries' Responsibilities Regarding Election Infrastructure."

An en bloc amendment to the Amendment in the Nature of a Substitute to H.R. 2825 offered by MR. MCCAUL (#1B); was AGREED TO by voice vote.

Consisting of the following amendments:

An amendment to the Amendment in the Nature of a Substitute offered by MR. DUNCAN (en bloc amendment 1):
Page 114, line 6, redesignate subsection (b) as subsection (c).
Page 114, beginning line 6, insert a new subsection entitled "(b) Level 3 Acquisition Programs of Components of the Department.-"

An amendment to the Amendment in the Nature of a Substitute offered by MS. JACKSON LEE (en bloc amendment 2):
Page 99, line 23, insert "to keep pace with changes in technology that could impact deliverables," after "risks,".

An amendment to the Amendment in the Nature of a Substitute offered by MR. CORREA (en bloc amendment 3):
After section 222 insert a new section entitled "Sec. 223. Department Leadership Council."

An amendment to the Amendment in the Nature of a Substitute offered by MR. CORREA (en bloc amendment 4):
Page 65, after line 8, insert the following:
"(11) The term 'life cycle cost' means the total ownership cost of an acquisition, including all relevant costs related to acquiring, owning, operating, maintaining, and disposing of the system, project, or product over a specified period of time.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. CORREA (en bloc amendment 5):
At the end of subtitle A of title II, add a new section entitled "Sec. 215. Acquisition Innovation.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. CORREA (en bloc amendment 6):
Page 68, after line 9, insert the following:
"(F) Providing additional scrutiny and oversight for an acquisition that is not a major acquisition if-
"(i) the acquisition is for a program that is important to departmental strategic and performance plans;
"(ii) the acquisition is for a program with significant program or policy implications; and
"(iii) the Secretary determines that such scrutiny and oversight for the acquisition is proper and necessary.".
Page 68, line 10, strike "(F)" and insert "(G)".
Page 68, line 14, strike "(G)" and insert "(H)".
Page 68, line 22, strike "(H)" and insert "(I)".

An amendment to the Amendment in the Nature of a Substitute offered by MR. CORREA (en bloc amendment 6):
Page 69, beginning line 3, insert the following:
"(I) Ensuring acquisition decision memoranda adequately document decisions made at acquisition decision events, including any affirmative determination of contractor responsibility at the down selection phase and any other significant procurement decisions related to the acquisition at issue.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON of Mississippi (#1C); was NOT AGREED TO by a recorded vote of 12 yeas and 14 nays (Roll Call Vote No. 9).

At the end of subtitle C of title II add a new section entitled "Sec. 234. Exercise of Eminent Domain in Major Acquisitions.".

An amendment to the Amendment in the Nature of a Substitute offered by MRS. WATSON COLEMAN (#1D); was NOT AGREED TO by a recorded vote of 11 yeas and 15 nays (Roll Call Vote No. 10).

At the end of subtitle B of title II, add a new section entitled "Sec. 226. Acquisition Management Directive."

An en bloc amendment to the Amendment in the Nature of a Substitute to H.R. 2825 offered by MR. MCCAUL (#1E); was AGREED TO by voice vote.

Consisting of the following amendments:

An amendment to the Amendment in the Nature of a Substitute offered by MR. KING of New York (en bloc amendment 1):
At the end of subtitle A of title III, add a new section entitled "Sec. 308. Border and Gang Threat Assessment."

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON of Mississippi (en bloc amendment 2):
At the end of subtitle A of title III, add a new section entitled "Sec. 208. Security Clearance Management and Administration."

An amendment to the Amendment in the Nature of a Substitute offered by MR. HURD (en bloc amendment 3):
In section 304(b)(3), insert "promulgate data standards and" before "instruct".
In section 304(b)(3), insert "standard" before "format".
Amend subsection (e) of section 304 "(e) Deadline for Implementation.-"
In subsection (g) of section 304, strike paragraphs (1) and (2) (and redesignate subsequent paragraphs accordingly).

An amendment to the Amendment in the Nature of a Substitute offered by MS. JACKSON LEE (en bloc amendment 4):
Page 156, line 14, strike " inserting '; and' " and insert "inserting a semicolon".
Page 156, line 16, strike "paragraph" and insert "paragraphs".
Page 157, line 14, strike the first period and insert "; and".
Page 157, line 14, strike the closing quotes and the second period.
Page 157, beginning line 15, insert the following:
"(H) in coordination with appropriate components and offices of the Department and other Federal agencies, develop, maintain, and make available information on Federal resources intended to support fusion center access to Federal information and resources.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. FITZPATRICK (en bloc amendment 5):
Page 139, beginning line 1, insert the following (and make subsequent conforming changes):
"(15) promote and facilitate, to the greatest extent practicable, nationwide suspicious activity report training of fire, emergency medical services, emergency management, and public heath personnel;".

An amendment to the Amendment in the Nature of a Substitute offered by MR. LANGEVIN (en bloc amendment 6):
Page 142, line 12, insert the following (and redesignate subsequent clauses accordingly):
"(vii) The national cybersecurity and communications integration center under section 227.".

An en bloc amendment to the Amendment in the Nature of a Substitute to H.R. 2825 offered by MR. MCCAUL (#1F); was AGREED TO by voice vote.

Consisting of the following amendments:

An amendment to the Amendment in the Nature of a Substitute offered by MR. RUTHERFORD (en bloc amendment 1):
Strike section 405.

An amendment to the Amendment in the Nature of a Substitute offered by MR. CORREA (en bloc amendment 2):
Redesignate section 410 as section 411.
After 409 insert a new section entitled "Sec. 410. Maritime Security Capabilities Assessments.".

An en bloc amendment to the Amendment in the Nature of a Substitute to H.R. 2825 offered by MR. MCCAUL (#1G); was AGREED TO by voice vote.

Consisting of the following amendments:

An amendment to the Amendment in the Nature of a Substitute offered by MR. ROGERS of Alabama (en bloc amendment 1):
In section 521, add at the end a new subsection entitled "(d) Briefing to Congress."

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON of Mississippi (en bloc amendment 2):
Amend paragraph (3) of section 584 (f) to read as follows:
(3) Rule of Construction.-Nothing in this section may be construed to-
(A) replace or affect in any way the use of 9-1-1 services in an emergency; or
(B) replace or affect in any way the security training program requirements specified in section 1408, 1517, and 1534 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1137, 1167, and 1184; Public Law 110-53).

An amendment to the Amendment in the Nature of a Substitute offered by MR. KATKO (en bloc amendment 3):
In subtitle C of title V, add at the end a new section entitled "Sec. 533. Prohibition of Advance Notice of Covert Testing to Security Screeners."

An amendment to the Amendment in the Nature of a Substitute offered by MR. KATKO (en bloc amendment 4):
Page 173, line 22, insert "OMBUDSMAN," before "AND".
Page 173, line 25, insert "Ombudsman," before "and".
Page 174, line 5, insert "Ombudsman," before "and".
Page 174, line 9, strike "(2)" and insert "(3)".
Page 174, line 10, strike "the traveling public is" and insert "Transportation Security Administration employees and the traveling public are".
Amend subsection (pp) of section 502 to read as follows:
(pp) SECTION 45107.-Section 45107 of title 49, United States Code, is amended-
(1) in subsection (a), by striking "Under Secretary of Transportation for Security" and inserting "Administrator of the Transportation Security Administration"; and
(2) in subsection (b), by striking the second sentence.

An amendment to the Amendment in the Nature of a Substitute offered by MRS. WATSON COLEMAN (en bloc amendment 5):
At the end of subtitle B of title V, add a new section entitled "Sec. 529. Innovation Task Force.".

An amendment to the Amendment in the Nature of a Substitute offered by MRS. WATSON COLEMAN (en bloc amendment 6):
At the end of title V add a new subtitle entitled "Subtitle H-Security Enhancements in Public Areas of Transportation Facilities".

An amendment to the Amendment in the Nature of a Substitute offered by MR. DONOVAN (en bloc amendment 7):
At the end of subtitle B of title V, add a new section entitled "Sec. 529. Airport Law Enforcement Reimbursement.".

An amendment to the Amendment in the Nature of a Substitute offered by MISS RICE of New York (en bloc amendment 8):
At the end of title V, insert a new subtitle entitled "Subtitle H-Strategic 5-year Technology Investment Plan of the Transportation Security Administration."

An amendment to the Amendment in the Nature of a Substitute offered by MISS RICE of New York (en bloc amendment 9):
At the end of title V, insert a new subtitle entitled "Subtitle H-Maintenance of Security-Related Technology".

An amendment to the Amendment in the Nature of a Substitute offered by MISS RICE of New York (en bloc amendment 10):
Page 252, line 18, insert "for aviation security" after "model".
Page 254, line 11, insert "upon request," before "conduct".
Page 254, beginning line 12, strike "and share the results of such assessments with relevant stakeholders".
Page 254, after line 14, insert a new paragraph entitled "(3) TSA Database Cyber Assessment.-"
Page 254, line 15, strike "(3)" and insert "(4)".

An amendment to the Amendment in the Nature of a Substitute offered by MR. GALLAGHER (en bloc amendment 11):
At the end of subtitle A of title V, add a new section entitled "Sec. 504. Transportation Security Administration Efficiency."

An amendment to the Amendment in the Nature of a Substitute offered by MRS. DEMINGS (en bloc amendment 12):
At the end of subtitle D of title V, add a new section entitled "Sec. 543. Exit Lane Security."

An amendment to the Amendment in the Nature of a Substitute offered by MR. GARRETT (en bloc amendment 13):
At the end of subtitle A of title V, add a new section entitled "Sec. 505. Transportation Senior Executive Service Accountability."

An amendment to the Amendment in the Nature of a Substitute offered by MS. BARRAGÁN (en bloc amendment 14):
At the end of subtitle D of title V, add a new section entitled "Sec. 543. Reimbursement for Deployment of Armed Law Enforcement Personnel at Airports.".

An amendment to the Amendment in the Nature of a Substitute offered by MRS. WATSON COLEMAN (en bloc amendment 15):
In section 576, redesignate subsections (a) through (c) as subsections (d) through (f), respectively.
In section 576, insert before subsection (d), as so redesignated, a new subsection entitled "(a) In General."
In section 576, in subsection (d), as so redesignated, strike "IN GENERAL.-If" and insert "STAKEHOLDER NOTIFICATION.-When".
In section 576, in subsection (d), as so redesignated, strike "Visible Intermodal Prevention and Response (VIPR)" and insert "VIPR".
In section 576, in subsection (e), as so redesignated, strike "This section" and insert "Subsection (d)".
In section 576, in subsection (e), as so redesignated, strike "subsection (a)" and insert "such subsection".

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON of Mississippi (#1H); was NOT AGREED TO by a recorded vote of 12 yeas and 14 nays (Roll Call Vote No. 11).

At the end of subtitle B of title V, add a new section entitled "Sec. 529. Repeal of Requirement Regarding Diversion of Aviation Security Fees.".

An en bloc amendment to the Amendment in the Nature of a Substitute to H.R. 2825 offered by MR. MCCAUL (#1I); was AGREED TO by voice vote.

Consisting of the following amendments:

An amendment to the Amendment in the Nature of a Substitute offered by MS. MCSALLY (en bloc amendment 1):
At the end of subtitle A of title VI, add a new section entitled "Sec. 623. Operation Stonegarden."
Page 319, line 14, strike "for" and insert "to make grants to".

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON of Mississippi (en bloc amendment 2):
Page 322, line 10, before "The" insert "(a) Implementation Plan.-".
Page 322, line 11, after "shall" insert "develop an implementation plan, including benchmarks and milestones, to address the findings and recommendations of the 2017 Management Review Team that issued a report on May 8, 2017 regarding live agent training at the Chemical, Ordnance, Biological and Radiological Training Facility and".
Page 322, after line 22, insert a new subsection entitled "(b) Comptroller General Review.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. THOMPSON of Mississippi (en bloc amendment 3):
At the end of subtitle A of title VI, add a new section entitled "Sec. 623. Nonprofit Security Grant Program."

An amendment to the Amendment in the Nature of a Substitute offered by MR. RUTHERFORD (en bloc amendment 4):
At the end of subtitle A of title VI, add a new section entitled "Sec. 623. FEMA Senior Law Enforcement Advisor."
Page 329, line 21, strike "528" and insert "529".
Page 331, line 1, strike "528" and insert "529".
Page 333, after line 22, strike "528" with respect to the item being added and insert "529".

An amendment to the Amendment in the Nature of a Substitute offered by MS. JACKSON LEE (en bloc amendment 5):
Page 306, beginning line 20, insert the following: "(9) The Chief Medical Officer.".

An amendment to the Amendment in the Nature of a Substitute offered by MS. JACKSON LEE (en bloc amendment 6):
Page 311, beginning line 8, insert the following: (1) in subsection (c), insert "to the extent practicable, provide training in settings that simulate real response environments, such as urban areas," after "levels,".

An amendment to the Amendment in the Nature of a Substitute offered by MR. GARRETT (en bloc amendment 9):
Page 299, line 3, strike "and".
Page 299, line 12, strike the period and insert "; and".
Page 299, beginning line 13, insert the following:
(3) by adding at the end the following new paragraph:
"(4) ANNUAL REPORT.-The Administrator, in coordination with the Assistant Secretary for State and Local Law Enforcement, shall report annually from fiscal year 2018 through fiscal year 2022 on the use of grants under sections 2003 and 2004 for law enforcement terrorism prevention activities authorized under this section, including the percentage and dollar amount of funds used for such activities and the types of projects funded.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. LANGEVIN (en bloc amendment 8):
At the end of subtitle A of title VI (page 322, after line 22), insert a new section entitled "Sec. ———. Study of the Use of Grant Funds for Cybersecurity.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. LANGEVIN (en bloc amendment 9):
Page 337, after line 7, insert a new section entitled "Sec. 654. Office of Disability Integration and Co-ordination of Department of Homeland Security.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. PAYNE (en bloc amendment 10):
Page 301, line 19, strike "and".
Page 301, after line 19, insert the following:
(C) in paragraph (5), by adding at the end the following: ", provided such purchases align with the Statewide Communication Interoperability Plan and are coordinated with the Statewide Interoperability Coordinator or Statewide interoperability governance body of the State of the recipient"; and

An amendment to the Amendment in the Nature of a Substitute offered by MRS. DEMINGS (en bloc amendment 11):
Page 301, beginning line 11, insert a new subtitle entitled "(c) Comptroller General Review.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. PAYNE (#1J); was NOT AGREED TO by a recorded vote of 11 yeas and 15 nays (Roll Call Vote No. 12).
Page 296, line 19, strike "$800,000,000" and insert "$900,000,000".
Page 298, line 7, strike "$600,000,000" insert "$900,000,000".

An amendment to the Amendment in the Nature of a Substitute offered by MRS. WATSON COLEMAN (#1K); was NOT AGREED TO by a recorded vote of 11 yeas and 15 nays (Roll Call Vote No. 13).
Page 310, line 10, strike "$200,000,000" and insert "$400,000,000".

An amendment to the Amendment in the Nature of a Substitute offered by MRS. DEMINGS (#1L); was WITHDRAWN by unanimous consent.
Page 322, after line 22, insert a new section entitled "Sec. 6——. Preservation of Urban Area Security Initiative Security Gains."

An amendment to the Amendment in the Nature of a Substitute offered by MS. BARRAGÁN (#1M); was NOT AGREED TO by a recorded vote of 11 yeas and 15 nays (Roll Call Vote No. 14).
Page 311, line 1, strike "$200,000,000" insert "$400,000,000".

An en bloc amendment to the Amendment in the Nature of a Substitute to H.R. 2825 offered by MR. MCCAUL (#1N); was AGREED TO by voice vote.

Consisting of the following amendments:

An amendment to the Amendment in the Nature of a Substitute offered by MR. PERRY (en bloc amendment 1):
Page 351, line 11, insert the following (and make necessary conforming changes):
(6) By striking section 872 (6 U.S.C. 452).
Page 355, line 15, insert the following (and make necessary conforming changes):
(16) By striking the item relating to section 872.

An amendment to the Amendment in the Nature of a Substitute offered by MR. PERRY (en bloc amendment 2):
At the end of the bill, add a new section entitled "Sec. 702. Decision Regarding Certain Executive Memoranda."

An amendment to the Amendment in the Nature of a Substitute offered by MISS RICE of New York (en bloc amendment 3):
At the end of title VII insert a new section entitled "Sec. 702. Permanent Authorization for Asia-Pacific Economic Cooperation Business Travel Card Program."

An amendment to the Amendment in the Nature of a Substitute offered by MR. CORREA (en bloc amendment 4):
Page 356, after line 4, insert a new section entitled "Sec. 702. Authorization of Appropriations for Office of Inspector General.".

An amendment to the Amendment in the Nature of a Substitute offered by MR. CORREA (en bloc amendment 5):
Add at the end a new section entitled "Sec. 702. Canine Teams."

An amendment to the Amendment in the Nature of a Substitute offered by MR. CORREA (#1O); was WITHDRAWN by unanimous consent.

At the end, add a new section entitled 'Sec. 702. Conversion of Certain User Fee Airports to Ports of Entry."

COMMITTEE VOTES

Clause 3(b) of Rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

The Committee on Homeland Security considered H.R. 2825 on June 14, 2017, and took the following votes:

ROLL CALL NO. 9

On agreeing to the amendment to the Amendment in the Nature of a Substitute #1C offered by Mr. Thompson of Mississippi.
Not Agreed to: 12 yeas and 14 nays.

Representative	Yea	Nay	Representative	Yea	Nay
Mr. McCaul, Chair		X	Mr. Thompson of Mississippi, Ranking Member.	X	
Mr. Smith of Texas			Ms. Jackson Lee	X	
Mr. King of New York		X	Mr. Langevin	X	
Mr. Rogers of Alabama		X	Mr. Richmond	X	
Mr. Duncan of South Carolina			Mr. Keating	X	
Mr. Marino			Mr. Payne	X	
Mr. Barletta		X	Mr. Vela		
Mr. Perry		X	Mrs. Watson Coleman	X	
Mr. Katko		X	Miss Rice of New York	X	
Mr. Hurd	X		Mr. Correa	X	

Representative	Yea	Nay	Representative	Yea	Nay
Ms. McSally		X	Mrs. Demings	X	
Mr. Ratcliffe		X	Ms. Barragán	X	
Mr. Donovan		X			
Mr. Gallagher		X			
Mr. Higgins of Louisiana		X			
Mr. Rutherford		X			
Mr. Garrett		X			
Mr. Fitzpatrick		X			
			Vote Total:	**12**	**14**

ROLL CALL NO. 10

On agreeing to the amendment to the Amendment in the Nature of a Substitute #1D offered by Mrs. Watson Coleman.
Not Agreed to: 11 yeas and 15 nays.

Representative	Yea	Nay	Representative	Yea	Nay
Mr. McCaul, Chair		X	Mr. Thompson of Mississippi, Ranking Member.	X	
Mr. Smith of Texas			Ms. Jackson Lee	X	
Mr. King of New York		X	Mr. Langevin	X	
Mr. Rogers of Alabama		X	Mr. Richmond	X	
Mr. Duncan of South Carolina			Mr. Keating	X	
Mr. Marino			Mr. Payne	X	
Mr. Barletta		X	Mr. Vela		
Mr. Perry		X	Mrs. Watson Coleman	X	
Mr. Katko		X	Miss Rice of New York	X	
Mr. Hurd		X	Mr. Correa	X	
Ms. McSally		X	Mrs. Demings	X	
Mr. Ratcliffe		X	Ms. Barragán	X	
Mr. Donovan		X			
Mr. Gallagher		X			
Mr. Higgins of Louisiana		X			
Mr. Rutherford		X			
Mr. Garrett		X			
Mr. Fitzpatrick		X			
			Vote Total:	**11**	**15**

ROLL CALL NO. 11

On agreeing to the amendment to the Amendment in the Nature of a Substitute #1H offered by Mr. Thompson of Mississippi.
Not Agreed to: 12 yeas and 14 nays.

Representative	Yea	Nay	Representative	Yea	Nay
Mr. McCaul, Chair		X	Mr. Thompson of Mississippi, Ranking Member.	X	
Mr. Smith of Texas			Ms. Jackson Lee	X	
Mr. King of New York		X	Mr. Langevin	X	
Mr. Rogers of Alabama		X	Mr. Richmond	X	
Mr. Duncan of South Carolina			Mr. Keating	X	

Representative	Yea	Nay	Representative	Yea	Nay
Mr. Marino			Mr. Payne	X	
Mr. Barletta		X	Mr. Vela		
Mr. Perry		X	Mrs. Watson Coleman	X	
Mr. Katko	X		Miss Rice of New York	X	
Mr. Hurd		X	Mr. Correa	X	
Ms. McSally		X	Mrs. Demings	X	
Mr. Ratcliffe		X	Ms. Barragán	X	
Mr. Donovan		X			
Mr. Gallagher		X			
Mr. Higgins of Louisiana		X			
Mr. Rutherford		X			
Mr. Garrett		X			
Mr. Fitzpatrick		X			
			Vote Total:	**11**	**15**

ROLL CALL NO. 12

On agreeing to the amendment to the Amendment in the Nature of a Substitute #1J offered by Mr. Payne.
Not Agreed to: 11 yeas and 15 nays.

Representative	Yea	Nay	Representative	Yea	Nay
Mr. McCaul, Chair		X	Mr. Thompson of Mississippi, Ranking Member.	X	
Mr. Smith of Texas			Ms. Jackson Lee	X	
Mr. King of New York		X	Mr. Langevin	X	
Mr. Rogers of Alabama		X	Mr. Richmond	X	
Mr. Duncan of South Carolina			Mr. Keating	X	
Mr. Marino			Mr. Payne	X	
Mr. Barletta		X	Mr. Vela		
Mr. Perry		X	Mrs. Watson Coleman	X	
Mr. Katko		X	Miss Rice of New York	X	
Mr. Hurd		X	Mr. Correa	X	
Ms. McSally		X	Mrs. Demings	X	
Mr. Ratcliffe		X	Ms. Barragán	X	
Mr. Donovan		X			
Mr. Gallagher		X			
Mr. Higgins of Louisiana		X			
Mr. Rutherford		X			
Mr. Garrett		X			
Mr. Fitzpatrick		X			
			Vote Total:	**11**	**15**

ROLL CALL NO. 13

On agreeing to the amendment to the Amendment in the Nature of a Substitute #1K offered by Mrs. Watson Coleman.
Not Agreed to: 11 yeas and 15 nays.

Representative	Yea	Nay	Representative	Yea	Nay
Mr. McCaul, Chair		X	Mr. Thompson of Mississippi, Ranking Member.	X	
Mr. Smith of Texas			Ms. Jackson Lee	X	
Mr. King of New York		X	Mr. Langevin	X	
Mr. Rogers of Alabama		X	Mr. Richmond	X	
Mr. Duncan of South Carolina			Mr. Keating	X	
Mr. Marino			Mr. Payne	X	
Mr. Barletta		X	Mr. Vela		
Mr. Perry		X	Mrs. Watson Coleman	X	
Mr. Katko		X	Miss Rice of New York	X	
Mr. Hurd		X	Mr. Correa	X	
Ms. McSally		X	Mrs. Demings	X	
Mr. Ratcliffe		X	Ms. Barragán	X	
Mr. Donovan		X			
Mr. Gallagher		X			
Mr. Higgins of Louisiana		X			
Mr. Rutherford		X			
Mr. Garrett		X			
Mr. Fitzpatrick		X			
			Vote Total:	**11**	**15**

ROLL CALL NO. 14

On agreeing to the amendment to the Amendment in the Nature of a Substitute #1M offered by Ms. Barragán.
Not Agreed to: 11 yeas and 15 nays.

Representative	Yea	Nay	Representative	Yea	Nay
Mr. McCaul, Chair		X	Mr. Thompson of Mississippi, Ranking Member.	X	
Mr. Smith of Texas			Ms. Jackson Lee	X	
Mr. King of New York		X	Mr. Langevin	X	
Mr. Rogers of Alabama		X	Mr. Richmond	X	
Mr. Duncan of South Carolina			Mr. Keating	X	
Mr. Marino			Mr. Payne	X	
Mr. Barletta		X	Mr. Vela		
Mr. Perry		X	Mrs. Watson Coleman	X	
Mr. Katko		X	Miss Rice of New York	X	
Mr. Hurd		X	Mr. Correa	X	
Ms. McSally		X	Mrs. Demings	X	
Mr. Ratcliffe		X	Ms. Barragán	X	
Mr. Donovan		X			
Mr. Gallagher		X			
Mr. Higgins of Louisiana		X			
Mr. Rutherford		X			
Mr. Garrett		X			
Mr. Fitzpatrick		X			
			Vote Total:	**11**	**15**

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of Rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of Rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 2825, the Department of Homeland Security Authorization Act of 2017, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of Rule XIII of the Rules of the House of Representatives, a cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974 was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the *Congressional Record* upon its receipt by the Committee.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of Rule XIII of the Rules of the House of Representatives, H.R. 2825 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

The goals and objective of H.R. 2825 is to provide a comprehensive reauthorization of the Department of Homeland Security for the first time since its creation. This includes a reform and reauthorization of the Department's headquarters, acquisitions reform, improvements to the Department's information sharing and counterterrorism efforts, important maritime security improvements, a complete reauthorization of the Transportation Security Administration, comprehensive authorization and congressional guidance on DHS grants, and technical corrections to the Homeland Security Act of 2002.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of Rule XIII, the Committee finds that H.R. 2825 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with Rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of the Rule XXI.

FEDERAL MANDATES STATEMENT

An estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the *Congressional Record upon its receipt by the Committee.*

PREEMPTION CLARIFICATION

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 2825 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 2825 would require no directed rule makings.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

TITLE V-TRANSPORTATION SECURITY ADMINISTRATION

SUBTITLE A-ADMINISTRATION

Sec. 1. Short title; Table of contents.

This section provides that this bill may be cited as the "Department of Homeland Security Authorization Act of 2017" or the "DHS Authorization Act of 2017".

This section also details the table of contents for the bill.

TITLE I-DEPARTMENT OF HOMELAND SECURITY HEADQUARTERS

SUBTITLE A-HEADQUARTERS OPERATIONS

Sec. 101. Homeland security enterprise defined.

Section 101 amends the Homeland Security Act of 2002 to include a definition of "homeland security enterprise"

Sec. 102. Functions and components of Headquarters of Department of Homeland Security.

Section 102 identifies the offices that constitute DHS's headquarters and outlines Headquarters' functions, including, but not limited to, establishing an overall strategy to successfully further the mission of the Department, establishing initiatives that improve Department-wide operational performance, managing and encouraging shared services across Department components, and establishing and implementing policies, in consultation with the Office of Civil Rights and Civil Liberties, which preserve individual liberty, fairness, and equality under the law.

Sec. 103. Repeal of Director of Shared Services and Office of Counternarcotics Enforcement of Department of Homeland Security.

Section 103 abolishes the Director of Shared Services position as well as the now defunct Office of Counternarcotics Enforcement.

Sec. 104. Responsibilities and functions of Chief Privacy Officer.

Section 104 amends the Homeland Security Act of 2002 by authorizing the Chief Privacy Officer and requiring that official to report directly to the Secretary. Section 104 establishes responsibilities for the Chief Privacy Officer to include, among other things, developing privacy-related policies and guidance, establishing mechanisms to ensure components are in compliance with privacy policies and laws, serving as the Department's central office for managing and processing Freedom of Information Act (FOIA) requests, and preparing an annual report to Congress on the activities of the Department that affect privacy during the Fiscal Year covered by the report. Section 104 allows the Secretary to reassign the functions related to FOIA to another official within the Department, if necessary.

Sec. 105. Responsibilities of Chief Financial Officer.

Section 105 amends the Homeland Security Act of 2002 by including additional responsibilities for the Chief Financial Officer (CFO). Specifically, Section 105 requires the CFO to oversee the Department's budget formulation and execution, lead cost-estimating and performance-based budgeting practices for the Department, oversee coordination of the Department's budget into strategic planning, develop financial management policy, develop financial system modernization guidance, establish internal controls over financial reporting systems, lead assessments of internal controls, lead financial oversight, ensure components identify and report all acquisition program costs, oversee budget formulation and execution, and implement a common accounting structure by Fiscal Year 2020.

Additionally, this section requires the Chief Financial Officer to oversee, approve, and make public information on Department expenditures for conferences, including requiring each component to report such expenditures in excess of $20,000 to the Inspector General of the Department.

Sec. 106. Chief Information Officer.

Section 106 amends the Homeland Security Act of 2002 by requiring the Chief Information Officer (CIO) to report directly to the USM and establishes areas of responsibility relating to information technology. The section also requires the CIO to develop an information technology strategic plan every 5 years. Additionally, the CIO must inventory DHS' software licenses within 180 days and every 2 years thereafter until 2022 to assess the Department's needs for software licenses, examine how to achieve cost savings related to the purchase of software licenses, determine whether cloud-based services will impact the need for software licenses, and establish plans and estimated costs for eliminated unused software licenses. Finally, it requires a Comptroller General review of these actions by Fiscal Year 2019.

Sec. 107. Quadrennial Homeland Security review.

Section 107 amends the Homeland Security Act of 2002 by making a few technical changes to DHS' requirements relating to the Quadrennial Homeland Security Review (QHSR), such as collaboration with the Homeland Security Advisory Committee and the use of a risk assessment when evaluating the threats facing the homeland. It also requires the Secretary to retain, and upon request, provide to Congress certain documentation relating to the preparation of the QHSR.

Sec. 108. Office of Strategy, Policy, and Plans.

Section 108 States that the Office of Strategy, Policy, and Plans shall include the following components: the Office of Partnership and Engagement, the Office of International Affairs, the Office of Cyber, infrastructure, and Resilience Policy, the Office of Strategy, Planning, Analysis, and Risk, the Office of Threat Prevention and Security Policy, and the Office of Border, Immigration, and Trade Policy. The section also lays out various responsibilities and duties of the Assistant Secretary for Partnership and Engagement, such as leading efforts to incorporate external feedback from stakeholders and lays out responsibilities of the Assistant Secretary for International Affairs, including coordinating international activities within the Department.

The current Office of International Affairs is abolished, with all of its assets and personnel transferred to the like office in the Office of Strategy, Policy, and Plans. The following offices have their functions, assets, and personnel transferred to the Office of Partnership and Engagement: the Office for State and Local Law Enforcement, the Office for State and Local Law Government Coordination, and the Special Assistant to the Secretary authorized by section 102(f) of the Homeland Security Act of 2002.

Section 108 further specifies 13 Assistant Secretary positions and States that no other Assistant Secretary position may be created or designated by DHS. It also requires DHS to conduct a duplication review within 1 year relating to components responsible for international affairs.

Section 108 amends the Homeland Security Act of 2002 by authorizing the Secretary to establish the Homeland Security Advisory Council to provide advice and recommendations on homeland

security-related matters, including advice with respect to the preparation of the Quadrennial Homeland Security Review.

Sec. 109. Chief Procurement Officer.

Section 109 amends the Homeland Security Act of 2002 by establishing the Chief Procurement Officer (CPO). The CPO is required to report directly to the USM and will be a senior business advisor of the Department on procurement related matters. Section 109 establishes responsibilities for the CPO, to include, among other things, issuing procurement policies, serving as the primary liaison to industry, and collecting data and establishing performance measures on the impact of strategic sourcing initiatives on the private sector. Section 109 includes a clerical amendment to include the CPO in the Homeland Security Act's table of contents.

Sec. 110. Chief Security Officer.

Section 110 amends the Homeland Security Act of 2002 by authorizing the Chief Security Officer and requiring that official to report directly to the USM. Section 110 establishes responsibilities for the Chief Security Officer to include (1) developing DHS's security policies, (2) providing security-related training, and (3) providing support to components on security-related matters.

Sec. 111. Office of Inspector General.

Section 111 provides a sense of Congress, with findings, that the Inspector General of the Department of Homeland Security plays a vital role in fulfilling the Department's daily missions.

Additionally, section 111 requires the heads of offices and components of DHS to advise the DHS Inspector General of all allegations of misconduct that they receive over which the Inspector General has jurisdiction.

Sec. 112. Office for Civil Rights and Civil Liberties.

Section 112 lays out the responsibilities for the Office for Civil Rights and Civil Liberties, under the direction of the Officer for Civil Rights and Civil Liberties, including integrating civil rights and civil liberties into activities of the Department, investigating public allegations of civil rights and civil liberties violations, carrying out the Department's equal employment and diversity policies and programs, and communicating with individuals and communities whose civil rights and civil liberties may be affected by Department activities.

Additionally, this section authorizes to be appropriated $22,571,000 for fiscal years 2018 and 2019 to carry out section 705 of the Homeland Security Act of 2002, as amended.

Sec. 113. Department of Homeland Security Rotation Program.

Section 113 enhances the DHS Security Rotation Program to require greater focus on departmental integration and unity of effort as well as personnel development. It also requires the Secretary to disseminate information on the program widely throughout the Department and to protect various rights of employees participating in the program.

Subsection (g) of Section 113 requires the Secretary to establish the "Intelligence Rotational Assignment Program" to be adminis-

tered by the Department's Chief Human Capital Officer, in conjunction with the Chief Intelligence Officer. The rotation program shall to be open to employees serving in existing analyst positions with the Department's Intelligence Enterprise (DHS IE), as well as other DHS employees, as appropriate. The responsibilities and requirements that apply to the DHS Rotation Program shall also apply to the Intelligence Rotational Assignment Program.

The DHS IRAP was created in 2014 to promote a broader understanding of the various intelligence missions and functions across the DHS IE, to enhance career development of DHS intelligence personnel, and promote DHS-wide intelligence competencies. Despite its important mission, the Committee found that numerous intelligence components were not aware of this program's existence and that it was not being coordinated with other rotational programs offered by the Department or the Intelligence Community.

A joint Intelligence Community, DHS, and Department of Justice OIG review of "Domestic Sharing of Counterterrorism Information," published in March 2017, specifically referenced the creation of the IRAP as an important step to help unify the DHS IE, but noted the lack of incentives to encourage participation in this initiative. Section 113 will provide certainty in the future of the IRAP, raise much-needed awareness of the program, and promote participation by all intelligence components.

Consolidating the IRAP into the Department's Homeland Security Rotation Program will ensure coordination with other DHS-wide rotation programs and that analyst participation in the IRAP will be factored into promotions and other career advancement opportunities. This promotes greater consistencies in the Department's policies for how to track and capitalize on intelligence analyst participation the Department's various rotation programs. Section 113 is also intended to encourage the Chief Human Capital Officer and Chief Intelligence Officer to offer similar incentives and promotional opportunities to analysts participating in the IRAP as those afforded to DHS personnel who complete a rotation in the Intelligence Community's "Joint Duty Assignment."

Sec. 114. Future Years Homeland Security Program.

Section 114 amends the Homeland Security Act of 2002 by requiring DHS to submit to the House and Senate homeland security committees a Future Years Homeland Security Program report that provides detailed projected cost estimates of anticipated programs over 5 fiscal years. Section 114 also requires that the Future Years Homeland Security Program project acquisition cost and schedule estimates over that same 5-year period. These reports are to be made available to the public, to the extent that they do not contain classified information.

Sec. 115. Field efficiencies plan.

Section 115 requires DHS to submit a field efficiencies plan within 270 days of enactment of the Act, which examines DHS' real property portfolio and provides recommendations and a cost-benefit analysis for the consolidation of its facilities. The Committee does not intend for this provision or any other section of the legislation to be construed as providing new authorities to the Department of Homeland Security or any of its component agencies or programs

real property authorities, including leases, construction, or other acquisitions, and disposals.

Sec. 116. Submission to Congress of information regarding reprogramming or transfer of Department of Homeland Security resources to respond to operational surges.

Section 116 requires DHS to provide to Congress every year until 2023 information on any circumstances in which the Secretary exercised authority to reprogram or transfer funds to address unforeseen costs.

Sec. 117. Report to Congress on cost savings and efficiency.

Section 117 requires that the Secretary submit to the House and Senate homeland security committees reports on: (1) components' management and administrative costs; (2) an examination of the Department's major physical assets; (3) size, experience level, and geographic distribution of operational personnel; and (4) recommendations for how to address deficiencies, reduce costs, and enhance efficiencies.

Sec. 118. Research and development and CBRNE organizational review.

Section 118 requires the Secretary to assess the organization and management of DHS' research and development (R&D) activities, and then submit a plan to Congress with a proposed organization structure, which must also include a justification of that plan, including a description of the effects on specific directorates and offices, such as the Science and Technology Directorate and Domestic Nuclear Detection Office, based on any proposed relocation of their activities. Section 118 also requires the Secretary to do a similar assessment and plan for DHS' chemical, biological, radiological, nuclear, and explosives (CBRNE) activities, including those of the Office of Health Affairs, Domestic Nuclear Detection Office, and Office for Bombing Prevention. Additionally, this section requires the Government Accountability Office to review and report to Congress on the proposed organizational structure no later than 3 months after the submission of each plan.

The Committee believes that R&D and CBRNE activities are vital to the homeland security mission, and is committed to ensuring that those activities are carried out in the most effective, efficient way possible. By having the Secretary conduct a thorough review of the Department's R&D and CBRNE activities and having GAO review such plans, we can ensure the Department is operating efficiently and effectively, and that its R&D mission and CBRNE missions are structured in a manner that best supports the Department's mission.

Sec. 119. Activities related to children.

This section amends the Homeland Security Act of 2002 requiring the Department of Homeland Security to consider the needs of children in homeland security planning. This section is similar to H.R. 1372, which passed the House by voice vote on April 25, 2017.

SUBTITLE B-HUMAN RESOURCES

Sec. 121. Chief Human Capital Officer responsibilities.

Section 121 amends the Homeland Security Act of 2002 to improve morale, employee engagement, and communications within the Department of Homeland Security work force by conferring new responsibilities to the Chief Human Capital Officer and allowing for the designation of a Chief Learning and Engagement Officer, who will assist with work force planning and employee development. Additional responsibilities of the Chief Human Capital Officer include carrying out an assessment of the learning and developmental needs of employees in supervisory and non-supervisory roles across the Department and maintenance of a catalogue of available employee development opportunities and ensuring that employee discipline and adverse action programs comply with all pertinent laws, regulations, guidance, and ensure due process for employees.

Sec. 122. Employee engagement steering committee and action plan.

Section 122 establishes an employee engagement steering committee at the Department of Homeland Security to help improve employee morale. The Committee is to be comprised of representatives from operational components, headquarters, and field personnel that are supervisory and non-supervisory as well as labor organizations that represent Department employees. The committee is required to (1) identify factors that have a negative impact on employee engagement, morale and communications within the Department by collecting employee feedback; (2) identify, develop and distribute initiatives and best practices to improve employee engagement, morale and communications within the Department; (3) monitor component efforts to address these factors; and (5) advise to the Secretary on efforts to improve employee engagement, morale, and communications within the Department. It further requires the Secretary, acting through the Chief Human Capital Officer, to issue an action plan reflecting the input from the employee engagement steering committee, as well as require the head of each component to then develop and issue a component-specific employee engagement plan.

Additionally, this section shall terminate 5 years after the date of enactment of this section.

Sec. 123. Annual employee award program.

Section 123 authorizes an annual employee award program at the Department of Homeland Security to recognize employees who have made significant contributions to the Department's mission. An internal review board comprised of Department personnel shall submit to the Secretary award recommendations regarding specific employees or groups of employees. The internal review board shall consult with representatives from operational components and headquarters, including supervisory and non-supervisory personnel, and employee labor organizations that represent Department employees.

Sec. 124. Independent investigation and implementation plan.

Section 124 directs the Comptroller General to investigate whether discipline and adverse actions are handled in an equitable and consistent manner across the Department for misconduct by a non-supervisory or supervisory employee.

Sec. 125. Center for faith-based and neighborhood partnerships.

This section codifies the Center for Faith-Based and Neighborhood Partnerships, which coordinates outreach and collaboration efforts between the emergency management community and faith-based and community organizations, provides guidance to places of worship on how to secure their facilities, and engages with local communities on the Department's Blue Campaign, among other things.

Sec. 126. Timely guidance to DHS personnel regarding Executive Orders.

Section 126 requires, to the maximum extent practicable, the Secretary to, in coordination with relevant component heads, make every effort to provide to relevant Department personnel written guidance regarding how an Executive Order is to be implemented, before any Executive Order affecting Departmental functions, programs, or operations takes effect.

Sec. 127. Secretary's responsibilities regarding election infrastructure.

Section 127 requires the Secretary to continue to prioritize the provision of assistance, on a voluntary basis, to State and local election officials in recognition of the importance of election infrastructure.

TITLE II-DEPARTMENT OF HOMELAND SECURITY ACQUISITION ACCOUNTABILITY AND EFFICIENCY

Sec. 201. Definitions.

Section 201 adds a series of acquisition related definitions that will apply to the acquisitions title of the Act. These include: acquisition, acquisition decision authority, acquisition decision event, acquisition decision memorandum, acquisition program, acquisition program baseline, best practices, breach, congressional homeland security committees, life cycle cost-as currently defined in the Federal Acquisition Regulation, and major acquisition program.

SUBTITLE A-ACQUISITION AUTHORITIES

Sec. 211. Acquisition authorities for Under Secretary for Management of the Department of Homeland Security.

Section 211 codifies the Under Secretary for Management (USM) as the Chief Acquisitions Officer for the Department with the authority to approve, pause, modify, or cancel major acquisition programs. It also includes a requirement that each major acquisition program have documentation showing it has a Department-approved Acquisition Program Baseline (APB) and is meeting agreed-upon cost, schedule, and performance requirements. It also charges

the USM with overseeing the organizational structure for acquisitions operations throughout the Department. The USM is responsible for ensuring acquisition decision memoranda (ADM) adequately document decisions made at acquisition decision events (ADE) including any affirmative determination of contractor responsibility at the down selection phase, in addition to any other significant procurement decisions related the acquisition at issue. The Committee intends for the USM to only include information on any affirmative determination of contractor responsibility in ADMs at approval points for low rate production for testing purposes or for full production and deployment of a system. The USM or designee shall determine what actions meet the criteria for a "significant procurement decision." This must occur before the USM can delegate Acquisition Decision Authority to the relevant Component Acquisition Executive. Section 211 allows for additional scrutiny and oversight for certain non-major acquisitions.

Section 211 also requires the USM to cooperate with the Under Secretary for Science and Technology (S&T) in acquisitions, so that S&T can support current and future requirements more effectively. This section also requires that the USM ensures component heads comply with Federal law, Federal Acquisition Regulation (FAR), and Departmental acquisition directives.

Sec. 212. Acquisition authorities for Chief Financial Officer of the Department of Homeland Security.

Section 212 requires the Department's Chief Financial Officer to oversee acquisition program costs to ensure that acquisition programs are affordable over the program's life-cycle.

Sec. 213. Acquisition authorities for Chief Information Officer of the Department of Homeland Security.

Section 213 authorizes the Chief Information Officer (CIO) to oversee the management of the Homeland Security Enterprise Architecture and to provide recommendations to the Acquisition Review Board on IT programs and IT acquisition strategic guidance. Section 213 also requires the CIO to ensure, in consultation with the USM, that IT acquisition programs comply with IT management processes, technical requirements, and management directives.

Sec. 214. Acquisition authorities for Program Accountability and Risk Management.

Section 214 establishes the Program Accountability and Risk Management (PARM) office within the Department to provide accountability and consistency to components' major acquisition programs, as well as serve as the central oversight function for the Department and support the ARB. This section does not create a new office within DHS, as PARM is the current entity within DHS with these responsibilities.

Section 214 authorizes the PARM Executive Director to oversee PARM's role in monitoring the performance of DHS acquisition programs, assisting the USM in managing acquisition programs, and developing certification standards in consultation with CAEs for all acquisition program managers.

Section 214 also authorizes PARM to prepare and make available to Congress the DHS Comprehensive Acquisition Status Report (CASR). This section also requires Components to follow Federal law, the Federal Acquisition Regulation (FAR), and DHS acquisition management directives, among other things.

Section 214 further requires DHS components to submit certain acquisition documentation as part of the CASR, unless a waiver is granted. Any waiver must be submitted to Congress along with the grounds on which it was granted.

Sec. 215. Acquisition innovation.

Section 215 allows for the USM to designate an individual within the Department to manage acquisition innovation efforts; test, develop, and distribute acquisition best practices throughout the Department; establish performance metrics to evaluate the effectiveness of those efforts; and determine impacts of acquisition innovation efforts on the private sector, including small businesses.

Section 215 also allows for the USM to obtain feedback from the private sector on acquisition innovation efforts and incorporate such feedback into future activities. Further, this section effectively codifies innovation activities executed by the current Chief Procurement Officer of the Department, such as the Procurement Innovation Lab. Section 215 also requires the Department to provide a report to the House and Senate homeland security committees each year on acquisition innovation activities executed in the prior year. This will assist Congress in determining whether the Department is effectively executing its acquisition innovation efforts. The report must include information on (1) tested acquisition best practices, (2) efforts to distribute related best practices within the Department, (3) utilization of best practices by components, (4) results of performance metrics, (5) outcomes of efforts to distribute best practices throughout the Department, (6) any impacts of acquisition innovation activities on the private sector and small businesses, (7) the criteria used to identify specific acquisition programs or activities to be included in efforts and their associated outcomes, and (8) any recommendations that could improve acquisition practices in the Department.

The private sector is a vital element of the homeland security enterprise and it is essential that the Department proactively engage with industry partners, particularly as the Department's acquisition innovation efforts directly impact them. As a result, it is vital that DHS reach out to industry to identify areas for improvement as it relates to acquisition innovation efforts and incorporate its feedback as necessary. The Committee strongly believes that DHS should engage with the private sector, and in particular small businesses, when attempting to improve the very acquisition and procurement processes in which the Department seeks their participation.

SUBTITLE B-ACQUISITION PROGRAM MANAGEMENT DISCIPLINE

Sec. 221. Acquisition Review Board.

Section 221 codifies the Acquisition Review Board and requires the board to review, on a regular basis, foundational acquisition

documents of each major acquisition program, including the Acquisition Program Baseline (APB), which contain cost, schedule, and performance requirements. It does not create a new board within DHS because the ARB already exists. The board must meet at any time a major acquisition program requires authorization to proceed from one decision event to another, is in breach of its approved requirements, or requires additional review under determined by the Under Secretary for Management.

Section 221 includes provisions to strengthen accountability and uniformity within the DHS acquisition review process. Section 221 seeks to prevent delays in the acquisition process by requiring the ARB to meet regularly to ensure all major acquisition programs proceed through the acquisition process in a timely manner.

Section 221 authorizes the ARB to conduct systematic reviews of acquisitions and consider tradeoffs among cost, schedule, and performance objectives as part of the process for developing requirements, among other things.

If the USM approves a major acquisition program to proceed without an APB, Section 221 requires a report to Congress with the justification for the decision. To ensure component buy-in, this section also requires that at least two component heads or their designees permanently serve on the ARB.

Sec. 222. Requirements to reduce duplication in acquisition programs.

Section 222 requires DHS to establish policies to reduce unnecessary duplication and inefficiency for all DHS investments, including major acquisition programs. In fulfilling this requirement, the Deputy Secretary shall consult with the Under Secretary for Management, Component Acquisition Executives, other relevant DHS officials, advisors from Federal, State, Local, and Tribal governments, nonprofits, and the private sector. The Deputy Secretary is also given responsibilities to ensure that major acquisitions and investments decisions are well reasoned and are not unnecessarily duplicative or inefficient.

Sec. 223. Department leadership council.

Section 223 authorizes the Secretary to establish, if deemed necessary, a Departmental leadership council to ensure coordination of programs and activities of DHS. The mission of the leadership council shall be to (1) validate joint requirements to meet the mission needs of DHS, (2) ensure appropriate efficiencies are made among the life-cycle cost, scheduled, and performance objectives in the approval of joint requirements, (3) make prioritized capability recommendations for joint requirements, and (4) other matters assigned by the Secretary and Deputy Secretary. The leadership council shall be composed of senior officials representing components and a chairperson appointed by the Secretary. The Secretary would also be required to ensure that the Future Years of Homeland Security Program is consistent with any recommendations of a leadership council.

Sec. 224. Government Accountability Office review of Board and of requirements to reduce duplication in acquisition programs.

Section 224 requires the Government Accountability Office to conduct a review of the Acquisition Review Board established in Section 221.

Sec. 225. Excluded party list system waivers.

Section 225 requires the Secretary to submit to Congress within 5 days, notice and explanation for any waiver issued to a contractor in the Excluded Party List System.

Sec. 226. Inspector General oversight of suspension and debarment.

Section 226 allows the DHS Inspector General to audit decisions about grant and procurement awards to identify any improper awards to debarred entities. It also requires the DHS Inspector General to review the suspension and debarment program throughout DHS to assess whether criteria are consistently applied.

SUBTITLE C-ACQUISITION PROGRAM MANAGEMENT ACCOUNTABILITY AND TRANSPARENCY

Sec. 231. Congressional notification for major acquisition programs.

Section 231 requires internal notification reporting within DHS for breaches and a remediation plan (this is currently already required in DHS policy). This section also requires program managers (PMs) to conduct a root cause analysis to determine the cause(s) of the breach and requires congressional reporting for actual breaches that occur with cost overruns greater than 15 percent of the acquisition program baseline (APB), or with a schedule delay of more than 180 days in the delivery schedule specified in the acquisition program baseline, or with an anticipated failure for any key performance threshold or parameter specified in the APB. Additionally, if a likely cost overrun is greater than 20 percent or a likely delay is greater than 12 months from what is in the APB, then the USM must notify Congress.

Sec. 232. Multiyear Acquisition Strategy.

Section 232 requires the Secretary to submit to the House and Senate homeland security committees and the Comptroller General of the United States a multiyear acquisition strategy to guide the overall direction of DHS acquisitions within 1 year of the bill's enactment. Every year thereafter, the Secretary must update and include that strategy in each Future Years Homeland Security Program report already required by section 874 of the Homeland Security Act of 2002. Section 232 also requires the Secretary to consult with headquarters, components, employees in the field, industry, and the academic community when developing the strategy. The strategy must allow flexibility to deal with ever-changing threats, risks, and technology to help industry better understand, plan, and align resources to meet the future acquisition needs of DHS.

Section 232 requires the Secretary to include the following elements in the strategy:

- A prioritized list of acquisition investments;
- A plan to develop a reliable DHS-wide inventory of investments and real property assets;
- A plan to address known funding gaps between requirements and resources for acquisitions;
- An identification of test, evaluation, modeling, and simulation capabilities required to leverage emerging technology and R&D trends;
- A focus on flexible solutions to allow needed incentives and protections for appropriate risk-taking to meet acquisition needs with resiliency, agility, and responsiveness;
- A focus on incentives for program managers and senior Department acquisitions officials to achieve cost savings;
- An assessment of ways to address delays and bid protests;
- A focus on ways to increase outreach to key stakeholders that includes methods to engage small and disadvantaged businesses and guidance for interaction by program managers with key stakeholders to prevent misinterpretation of acquisition regulations;
- A plan to ensure competition or the option of competition for major acquisition programs; and
- A plan to address DHS acquisition work force accountability that identifies the acquisition work force needs of each Component and develops options for filling those needs. This plan shall also address ways to improve recruitment, hiring, training, and retention of DHS acquisition work force personnel to retain highly qualified personnel, among other things.

Section 232 also requires GAO to review the Department's multiyear acquisition strategy within 6 months of the Secretary submitting the first strategy. The review shall assess the Department compliance with Section 2's requirements, establishment of clear connections between DHS objectives and acquisition priorities, and demonstrate that acquisition policy reflects acquisition best practices, among other things.

Sec. 233. Acquisition reports.

Section 233 requires the Under Secretary of Management (USM) to submit to Congress an annual comprehensive acquisition status report. The report must include information required as part of the DHS Appropriations Act of 2013, a listing of programs canceled, modified, paused or referred to the USM or Deputy Secretary for additional oversight, and a listing of established Executive Steering Committees that are involved in certain acquisition decision events. For each major acquisition program, the report must include a narrative description, the Acquisition Review Board status of the acquisition, the most current and approved program baseline, a comparison of the original acquisition program baseline, the current program baseline and current cost estimate, whether independent verification and validation has been implemented, a rating of cost risk, schedule risk, and technical risk, the contract status, and lifecycle cost of the acquisition.

Section 233 also requires DHS component heads to identity to the USM all level of their respective level 3 acquisition programs, and the USM must certify to congressional homeland security committees whether such component heads have properly identified such programs no later than 30 days after receipt of such information. To do so, the USM would be required to establish a process with a repeatable methodology to continually identify level 3 acquisition programs. Component heads would also have to submit to the USM their respective polices and guidance for level 3 acquisition programs, and the USM would be required to certify to congressional homeland security committees that the respective policies and guidance adhere to Department-wide acquisition policies.

TITLE III-INTELLIGENCE AND INFORMATION SHARING

SUBTITLE A-DEPARTMENT OF HOMELAND SECURITY INTELLIGENCE ENTERPRISE

Sec. 301. Homeland intelligence doctrine.

A detailed evaluation of the Department's Intelligence Enterprise conducted by the Committee during the 114th Congress found that disparate guidance for the intelligence components within the Department of Homeland Security (DHS) undermined the Departments ability to fully utilize important data and analysis. On December 13, 2016, the Committee released a report recommending that the Department "should develop and issue a Departmental Intelligence Doctrine, using relevant Component policies and [Intelligence Community] Directives as a starting point."[1]

During the course of the Committee's oversight, series of senior current and former intelligence officials and experts specifically identified the Department's Chief Intelligence Officer (CINT) (which also serves as the DHS Undersecretary for Intelligence and Analysis) as the best individual within the Department to produce this doctrine.

This section requires the Secretary, acting through the Chief Intelligence Officer and in coordination with other DHS entities, to develop and disseminate a written Department-wide guidance regarding the processing, analysis, production, and dissemination of homeland security information and terrorism information. This section also requires that the guidance be submitted in unclassified form with a classified annex as appropriate.

Sec. 302. Analysts for the Chief Intelligence Officer.

This section amends section 201(e)(1) of the Homeland Security Act to include the requirement that the Secretary provide the Chief Intelligence Officer with an experienced and qualified staff. Currently, the Homeland Security Act only mandates staff for the Under Secretary of Intelligence and Analysis and the Under Secretary of Infrastructure Protection.

Though this section does not authorize any new funds for this staff, it recognizes the role of the CINT within the Department, including existing detailed staff to the CINT mission. The Depart-

[1] House Homeland Security Committee Majority Staff Report, "Reviewing the Department of Homeland Security's Intelligence Enterprise," December 2016.

ment has dedicated some existing staff within the Office of Intelligence and Analysis (I&A), Customs and Border Protection (CBP), Transportation Security Administration (TSA), and National Protection Programs Directorate (NPPD) to support the CINT's mission. This section will ensure that a small number of existing DHS personnel remain dedicated to carrying out CINT-related missions focused on coordinating and enhancing the DHS Intelligence Enterprise.

Sec. 303. Annual homeland terrorist threat assessments.

Throughout the Second Session of the 114th Congress, the Committee undertook a department-wide examination of the Department of Homeland Security's structure and mission. As part of this effort, numerous senior experts reiterated that the Department has a unique ability to draw data from multiple components, partner agencies, and State and local authorities. Yet nearly all survey respondents and roundtable participants who took part in this effort, as well as a number of other experts, agreed that DHS could improve or increase the use of intelligence, threat assessments, and similar information, into policy and planning. Similarly, experts were critical of the Department's use of information unique to DHS components in the development of their intelligence products. These points were further described in the Committee's Department of Homeland Security Intelligence Enterprise report released in December 2016.[2]

This section requires the Department to take a long-term analytical view utilizing Departmental information to identify emerging and persistent threats to the United States Homeland. This assessment must be based on analysis of information gathered by DHS components linked to DHS mission areas. Though there are examples of similar assessments produced by other Federal departments and agencies, none rely on unique DHS data, and it is not clear that these assessments are incorporated into how the Department plans and considers policy.

By relying on information provided by on-the-ground professionals, including State and local law enforcement and the National Network of Fusion Centers, this threat assessment will be a unique contribution to the Intelligence Community, policymakers, and local law enforcement. Furthermore, by requiring the Department to consider specific threats to cyber, transportation, and border security, in addition to terror threats, this section ensures that DHS focuses on its core mission areas. This assessment will inform the Department's budgeting and planning by clarifying the nature and scale of the threats DHS is intended to counter.

The assessment must be completed within 180 days of enactment and must be shared with Congress as a classified report with appropriate unclassified summaries and annexes.

Sec. 304. Department of Homeland Security data framework.

This section authorizes the Department of Homeland Security (DHS) Data Framework. The Data Framework is an ongoing initiative at the Department to connect many of data sets collected by

[2] House Homeland Security Committee Majority Staff Report, "Reviewing the Department of Homeland Security's Intelligence Enterprise", December 2016.

DHS component agencies to improve vetting capability for law enforcement, through a system called Neptune, and intelligence purposes, through the Cerberus system.

The development of the Data Framework has been challenging because each dataset held by DHS component agencies is subject to privacy and legal protections. Additionally, the scope of the project is complicated given the number of DHS component agencies and offices, the variety of DHS missions, and the existence of hundreds of different systems and datasets.

For use in the Cerberus system, which is the Department's current priority, there are 13 datasets fully or partially included in the framework.[3] The four sets fully connected to the Framework are the Electronic System for Travel Authorization (ESTA), the Advanced passenger Information System (APIS), I–94 records for foreign visitors, and the Passenger Name Record (PNR) system.[4] Additional systems in progress include, Secure Flight, Aviation Worker, Border Crossing Information, and several U.S. Citizenship and Immigration Services datasets.[5]

The Department initially planned to incorporate at least 20 data sets by the end of 2016[6] but has refocused on building full mission capability within the Cerberus system.[7] Given the program delays, privacy considerations, and the potential security value provided by the initiative, the Committee believes authorizing the Data Framework is important. The provision includes a deadline of 2 years after enactment for the Department to ensure the Data Framework includes all appropriate information linked to critical missions.

This section provides the first authorization for the program, mandates safeguards and training as part of the process by which appropriate Departmental personnel are able to access the system and includes important privacy and insider threat safeguards. The Secretary must ensure information in the Framework is protected and auditable by requiring mechanisms for identifying insider threats, security risks, and safeguarding privacy. The section also includes a requirement that DHS personnel make information available in a machine-readable, standard format, to the greatest extent practicable, to improve the search functionality of the framework.

The Committee believes that the Data Framework has the potential to greatly enhance the Department's ability to conduct security vetting and improve vetting against classified holdings. The section includes requirements for Congress to receive regular status updates and notification when the Data Framework is fully operational.

As the Department continues to develop and mature the Data Framework, it will be crucial for Department personnel to receive training in how to fully utilize the Framework and safeguard the information. The Committee directs the Secretary to ensure all applicable DHS components are sharing relevant and appropriate in-

---

[3] Department of Homeland Security briefing slides shared with the Committee on Homeland Security, June 9, 2017.

[4] Ibid.

[5] Ibid.

[6] House Homeland Security Committee Majority Staff Report, "Reviewing the Department of Homeland Security's Intelligence Enterprise, December 2016, pg. 37.

[7] Department of Homeland Security briefing slides shared with the Committee on Homeland Security, June 9, 2017.

formation in the Data Framework. Additionally, the Secretary shall review existing capability within the Department for data science to ensure that data sets in the Framework are being utilized to their fullest potential as allowed under the law. If the Department needs additional data science resources, the Secretary shall notify the Committee and make recommendations as necessary.

Sec. 305. Establishment of Insider Threat Program.

This section authorizes the 'Department of Homeland Security Insider Threat and Mitigation Act,' establishes an internal DHS Steering Committee to manage and coordinate DHS activities related to insider threat issues and mandates employee education and training programs.

The Committee believes that an insider threat program is necessary to standardize Department-wide efforts. The Committee is concerned that progress across the Department's component agencies has been uneven and requires more centralized coordination to ensure that all offices within the Department reach a baseline standard of effectiveness.

The Committee strongly believes that while insiders with malicious intent have caused the most serious damage to national security, most insider incidents occur by unwitting employees who are not properly trained. The purpose of the Insider Threat Program is not only to identify and prevent insiders from damaging the United States, but also to spot individuals who may demonstrate tendencies of an insider threat, and intervene through contact with an investigator to mitigate the activity through education and increased awareness.

This section also creates a Steering Committee within the Department to coordinate insider threat efforts across the Department, and review insider threat cases and issues related to the Department's critical assets. The Steering Committee shall be chaired by the Under Secretary for Intelligence and Analysis and the Chief Security Officer shall serve as the Vice-Chair. The Steering Committee's membership includes relevant stakeholders from across the Department and its component organizations that hold pertinent information to insider threats.

The Committee believes that a designated Steering Committee, chaired by senior officials, with a mandate to develop, execute and manage the daily operations of the Department's Insider Threat Program, will ensure that a comprehensive strategy is developed and a thorough assessment of the Department's critical assets is conducted. The Committee also believes that the Steering Committee should be responsible for issuing guidance and training related to insider threats Department-wide to ensure that all employees and contractors achieve a consistent-level of understanding and awareness about the program.

Additional responsibilities for the Steering Committee include leveraging best practices and technology from across the Federal Government, industry, and the research community to implement insider threat solutions that are validated and cost-effective; developing a timeline for deploying workplace monitoring technologies, awareness campaigns, and insider threat training; and developing metrics that indicate the effectiveness of the program.

In addition to the Department's networks, information and technology, the Committee believes that the Department's critical assets include its work force and physical assets. It is important that the Department consider all its assets when conducting its risk assessment so that it can prioritize and allocate resources accordingly.

As part of leveraging best practices and technology, the Committee notes that according to a survey of Federal IT managers, more than 40 percent of Federal agencies don't track data assets on their networks, and therefore they cannot be sure when and how specific documents are shared or otherwise exfiltrated.[8]

This section requires the Secretary to submit a report to Congress no later than 2 years after the date of enactment that describes how the Department and its components have implemented the insider threat strategy, the status of the Department's risk assessment of critical assets, training that has been provided to Department employees, and information on the effectiveness of the program. The Committee believes that the required report in this subsection will assist the Department in articulating its insider threat strategy, how it intends to increase awareness of the problem and train employees on how to identify and report signs of an insider threat, and collect data that will help it evaluate the effectiveness of the program as a whole. Finally, this section provides for definitions used in this section including: 'critical assets,' 'insider,' and 'insider threat.'

Sec. 306. Threat assessment on terrorist use of virtual currency.

This section requires the Under Secretary for Intelligence and Analysis to assess the threat posed by the use of virtual currencies to support designated Foreign Terrorist Organizations (FTOs), and disseminate the assessment to State, local, and tribal law enforcement officials via the national network of fusion centers.

As they have been come increasingly well-known and utilized more widely, some experts have suggested that virtual currencies could be used to support criminal or terrorist activity, as a means of avoiding more formal (and regulated) financial systems. In 2015 the Department of the Treasury warned that VCs "have attracted the attention of various criminal groups, and may be vulnerable to abuse by terrorist financiers."[9] However, most experts and officials agree, "there is no more than anecdotal evidence that terrorist groups have used virtual currencies to support themselves."[10] Still, the Committee is concerned that terrorists could eventually embrace virtual currencies as a means of making or moving funds. Toward that end, this section requires the Department to proactively study the threat this might pose in doing so, and provide potential solutions.

---

[8] Aaron Boyd, "Survey: Insider threats target nearly half of agencies", C4ISR Networks, September 14, 2015, available at: *http://www.c4isrnet.com/story/military-tech/it/2015/09/14/us-government-insider-threats-survey/72254846/*.

[9] "National Terrorist Financing Risk Assessment 2015," United States Department of the Treasury. *https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National Terrorist Financing Risk Assessment - 06-12-2015.pdf*.

[10] Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss, "TERRORIST USE OF VIRTUAL CURRENCIES Containing The Potential Threat," the Center for a New American Security, April 2017. *https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-TerroristFinancing-Final.pdf*.

Sec. 307. Department of Homeland Security counterterrorism advisory board.

In September 2015, the Committee on Homeland Security's Task Force on Combating Terrorist and Foreign Fighter Travel issued a report with 32 findings and more than 50 recommendations for enhancing U.S. security. Among other conclusions, the Task Force found that Congress should authorize the DHS Counterterrorism Advisory Board (CTAB)—an internal body charged with advising the Secretary of Homeland Security on counterterrorism issues—and ensure it is aligned with the current threat environment.[11]

Established at the behest of the Secretary of Homeland Security in 2010, the CTAB brings together top DHS officials to share information and coordinate counterterrorism activities. The CTAB has improved the Department's ability to respond to terrorism threats and harmonize counterterrorism programs and activities across DHS components.

Given that the CTAB has never been authorized in law, there is a risk that the board will be dismantled and that the internal DHS gains achieved, with respect to counterterrorism coordination, will be lost. The Task Force concluded that authorization in law and updates to the charter would keep the CTAB on a strong footing so it can be utilized by future DHS Secretaries and component leaders.

This section inserts a new section 210G into the Homeland Security Act of 2002 entitled 'Departmental Coordination on Counterterrorism,' establishing a board of senior representatives of departmental operational components and headquarters elements to coordinate and integrate departmental intelligence, activities, and policy related to the counterterrorism mission and functions of the Department. It requires the board to update its charter, as appropriate, every 4 years and to align it with the threat environment. This section further delineates the membership of the board and requires that Secretary to appoint a Coordinator for Counterterrorism who will serve as chair of the board. It requires the board to convene on a regular basis to discuss intelligence and coordinate ongoing threat mitigation efforts and departmental activities and to make recommendations to the Secretary. Finally, this subsection directs the board to advise the Secretary on the issuance of terrorism alerts.

Sec. 308. Border and gang threat assessment.

Acts of gang-related violence connected to transnational gangs, including specifically MS–13, have increased across the country in the last several years. Encompassed in this disturbing trend is an increase in violence committed by individuals who have entered the country after being subjected to vetting through various border security screening programs.

The Committee believes that a review of border security screening programs to identify and remedy any vulnerabilities is vital to address this situation. This section directs the Secretary to conduct this necessary review. It provides the Secretary with additional re-

[11] Committee on Homeland Security Task Force on Combatting Terrorist and Foreign Fighter Travel, "Final report of the Task Force on Combating Terrorist and Foreign Fighter Travel," September 2015, pg. 31.

sponsibilities that require the Department of Homeland Security (DHS or the Department) to conduct a threat assessment of these border security screening programs and to ensure that the borders of the United States are secure from the threats posed by human smuggling organizations and transnational gangs. Once this threat assessment has been completed, this section requires the Secretary to make a determination if any changes are necessary to these border security screening programs to address any security vulnerabilities that have been identified.

Sec. 309. Security clearance management and administration.

The Department of Homeland Security has over 230,000 employees. Across the DHS Enterprise, there are approximately 124,000 clearances with 86,000 at the Secret level, 25,000 at the Top Secret Level, and 13,000 TS//SCI.[12]

The proliferation of original and derivative classified material and the exponential growth in the number of individuals with security clearances present significant costs and homeland security and national security challenges that warrant timely action. In addition to the high costs incurred by the Federal Government to investigate the large number of individuals for positions requiring security clearances, over-designations have undoubtedly resulted in the Federal Government recruiting, hiring, and paying individuals at rates that are higher than necessary and not hiring individuals who otherwise have the required knowledge and skills.

This bill seeks to make specific reforms at the Department with respect to security clearance and position designations practices. The reforms at DHS are targeted at the designations of positions and the investigations, adjudications, denials, suspensions, revocations, and appeals processes for security clearances.

Within 1 year of enactment, the Secretary is required to review all sensitivity level designations of national security positions within the Department. If the Secretary determines that a change in the sensitivity level of a position is warranted, the access to the classified information will be adjusted to an appropriate level and a periodic reinvestigation will be completed as necessary.

The Secretary is required to report to the House Committee on Homeland Security and the Senate Committee on Homeland Security and Government Affairs after completion of each review to include the number of positions, by classification and component and office, as well as the determination of whether the position requires access to classified information, no longer requires access to classified information, or requires a different level of access. As an added measure of accountability, this section also requires the Inspector General to conduct audits on Departmental compliance.

This section also requires the Secretary to report to the House Committee on Homeland Security, House Committee on Oversight and Government Reform, and the Senate Committee on Homeland Security and Government Affairs on an annual basis for 5 years regarding individuals who have had security clearances denied, suspended, or revoked. Within 1 year of enactment, the Secretary must develop a plan for creating greater uniformity across the De-

[12] Department of Homeland Security Office of Congressional Affairs email to Committee staff, November 13, 2013.

partment in the security adjudication process and ensure that such information is protected.

SUBTITLE B-STAKEHOLDER INFORMATION SHARING

Sec. 311. Department of Homeland Security Fusion Center Partnership Initiative.

This section amends 210A of the Homeland Security Act to update existing statutory requirements related to Department of Homeland Security responsibilities and support for fusion centers.

As the National Network of Fusion Centers continues to mature into a national asset, this section adds several new responsibilities for the Secretary to reflect the current role of fusion centers in detecting and preventing a terrorist attack. These new responsibilities include "coordinating with the heads of other Federal departments" to provide operational and intelligence support, supporting "the maturation and sustainment" of fusion centers, reducing inefficiencies of Federal resources provided to fusion centers, ensuring that support to fusion centers is included as a priority in homeland security grant guidance, coordinating nationwide suspicious activity reports, ensuring that fusion centers are the focal points for sharing information, and disseminating best practices for appropriate State and local staffing at fusion centers. Additionally, this section addresses concerns the Members heard from stakeholders that fusion centers do not have access to certain Federal information and information systems by requiring the Secretary to become an information sharing advocate on behalf of fusion centers.

Section 210A(c) is amended to require the Under Secretary for Intelligence and Analysis to ensure fusion centers have access to DHS information sharing systems and to deploy appropriate DHS personnel to fusion centers. Such personnel may include intelligence officers, intelligence analysts, and other liaison personnel from DHS component agencies. Furthermore, the Under Secretary shall negotiate memoranda of understanding between DHS and appropriate State or local government agencies regarding how information shall be exchanged and protected between DHS and fusion centers. This subsection also requires DHS to coordinate with other Federal agencies regarding appropriate personnel that should be detailed to fusion centers. Finally, this subsection requires the Secretary to make available the criteria used by the Department for deploying personnel to fusion centers.

Subsection 210A(d), which relates to the responsibilities of Departmental personnel assigned to fusion centers, is amended by inserting a new subparagraph (5) to require such personnel ensure that they are incorporating relevant information from within the Department, including the components, in their analysis. The Committee believes the Department needs to work with fusion center to enhance Department intelligence information data by including State and local generated data. The Office of Intelligence and Analysis is one of the only members of the Intelligence Community that can directly work with State and local stakeholders.

Subsection 210A(e) is amended to require the Secretary to prioritize the deployment of resources, including Departmental personnel, from DHS components with border and maritime security responsibilities.

Subsection 210A(j) is amended to add a definition for the "National Network of Fusion Centers."

Subsection 210A(k) is deleted. This subsection contained the expired authorization of appropriations. This section is being removed because the funding for Departmental support to fusion centers comes largely from the Office of Intelligence and Analysis, which is funded through the National Intelligence Program, a classified appropriation. Other funds are available to State and local governments for fusion centers through homeland security grant programs.

Additionally, to hold the Department accountable, this section requires the Under Secretary of Intelligence and Analysis to report to Congress annually on how the Department is improving support to fusion centers and meeting the requirements in Section 210A of the Homeland Security Act. The reporting requirement sunsets in 2024.

Sec. 312. Fusion center personnel needs assessment.

This section requires the Comptroller General of the United States, within 120 days of enactment, to conduct an assessment of Departmental personnel detailed to fusion centers across the Nation and whether deploying additional Departmental personnel will enhance homeland security information sharing between Federal, State, and local departments and agencies. The assessment will examine the numbers of department personnel deployed to each fusion centers, information on the roles and responsibilities of personnel deployed to fusion centers, a review of additional Federal resources provides to fusion centers, analysis of the optimal number of such personnel at fusion centers, information and analysis on fusion centers near the land and maritime borders of the United States, and information and analysis on fusion centers near large and medium hub airports.

There are 79 centers across the country and they have established the National Network of Fusion Centers to enhance information sharing and coordination between the individual centers. In testimony before the Committee, as well as through numerous briefings and site visits, fusion center personnel have noted that increasing access to information and expertise from other parts of the Department, such as Customs and Border Protection, Immigration and Customs Enforcement, and the Transportation Security Administration would improve the National Network's ability to detect and prevent potential terrorist attacks and other emergencies.

Sec. 313. Program for State and local analyst clearances.

The Committee has heard repeatedly from witnesses and stakeholders about the need for some State and local analysts and officials to have higher security clearance levels, particularly Top Secret and Sensitive Compartmented Information (TS/SCI) clearances. The witnesses and stakeholders noted that in order to continue breaking down stovepipes and increasing information sharing between Federal, State, and local law enforcement officials, State and local analysts should have Top Secret clearances in order to understand the entire threat picture and communicate with Federal personnel about the threat and terrorism investigations.

This section provides a sense of Congress that any program established by the Under Secretary of Intelligence and Analysis to provide eligible State and local analysts located in fusion center with Top Secret clearances must be consistent with the need to know requirements pursuant to Executive Order 13526. Additionally, this section requires the Under Secretary to submit a one-time report to Congress on the effectiveness of granting higher clearance levels to State and local officials to improve information sharing and situational awareness, the costs for issuing and administering clearances and the associated training programs, and the operational security of such program.

Sec. 314. Information technology assessment.

This section requires the Under Secretary of Intelligence and Analysis, in collaboration with the Chief Information Officer and representatives from the National Network of Fusion Centers, to conduct an assessment of information system used to share homeland security information between the Department and fusion centers. The assessment shall include an evaluation of the accessibility and ease of use, a review of how departmental information systems connect with existing systems in the fusion centers, and an evaluation of participation levels of departmental components and offices using information systems to share information with fusion centers. The Committee has heard that despite numerous updates to Department's information systems specifically for State and local partners, there are still issue with usability and components' connectivity to such information systems. This section addresses these concerns.

Sec. 315. Department of Homeland Security classified facility inventory and dissemination.

This section requires the Secretary, to the extent practicable, to maintain and update an inventory of all facilities certified by the Department to house classified infrastructure or systems above the SECRET level. This section also requires the Secretary to share the inventory, as appropriate, with Departmental and other governmental personnel.

Greater transparency in the locations of all facilities certified by DHS to store classified infrastructure or systems above the Secret level[13] will ensure DHS is tracking the specific locations of all the Department's secure facilities and making this information available to departmental and State and local personnel, as appropriate. It will also ensure that DHS does not unnecessarily invest in new facilities in areas already covered by a pre-existing facility and thus reduce the chances for wasteful spending.

The significance of DHS personnel gaining access to SCIFs in the field was highlighted in a joint Intelligence Community, DHS, and Department of Justice OIG report, published in March 2017, which reviewed the domestic sharing of counterterrorism information. The report found that while counterterrorism information is usu-

[13] These facilities are commonly known as Sensitive Compartmented Information Facilities ("SCIFs"). A SCIF is an accredited area, room, or group of rooms, buildings, or installation where sensitive compartmented information may be used, stored, discussed, and/or processed. [Note: This definition is taken from a recent IC, DHS, DOJ joint OIG report entitled, "Review of Domestic Sharing of Counterterrorism Information."]

ally classified at the Top Secret level, DHS personnel lack sufficient access to SCIFs in the field. The report assesses that the effectiveness of DHS's Office of Intelligence and Analysis "as an IC member in particular, is hampered by its limited access to classified systems and facilities." Section 315 ensures that the physical locations of all DHS-certified facilities at the Top Secret level will be known to DHS personnel, including field personnel, as appropriate, and arrangements can be made for access.

In regards to State, local, tribal, and territorial (SLTT) partners, according to a DHS fact sheet, as of February 2017, SLTT personnel applying for a DHS sponsored Top Security clearance must provide documentation that clearly articulates the facility where Top Secret information will be accessed. However, the Committee has found that the locations of these facilities or not readily available to SLTT partners, which can pose unnecessary barriers in the security clearance nomination process. The requirement that the locations of these facilities to be made available to SLTT personnel, as appropriate, will assist in eliminating unnecessary impediments that could prevent or delay these stakeholders from applying for Top Secret security clearances. Last, section 315 also intends to assist SLTT personnel with active Top Secret clearances seeking to locate the nearest DHS-certified facility in which they can access systems and information above the Secret level.

Sec. 316. Terror inmate information sharing.

This section directs the Secretary, in coordination with the Attorney General and other appropriate Federal officials, to provide fusion centers and other law enforcement entities, as appropriate, with release information related to individuals incarcerated for terror-related offenses as defined under Title 18 U.S.C. Section 2332b. This information is to be provided by the Secretary for Homeland Security purposes. The Secretary must also conduct periodic assessments on the overall threat posed by known or suspected terrorists currently incarcerated in Federal correctional facilities, including the risk of such populations engaging in terrorist activities upon release. In carrying out these authorities the Secretary is required to receive input from the Officer for Civil Rights and Civil Liberties, the Officer for Privacy, and the Chief Intelligence Officer of the Department of Homeland Security (DHS or the Department). Section 316 does not require or give the Department the right or responsibility to establish a list or registry of individuals convicted of terrorism.

The Committee believes the new responsibilities added to the Secretary under this section will help mitigate the risk posed by individuals in Federal prison for crimes of terrorism who will be released. This situation must be addressed with consistent, proactive information sharing among Federal agencies, including the Department, the Bureau of Prisons, and State and local partners.

This section directs the Secretary to engage in a consistent, proactive information sharing process by coordinating with appropriate Federal officials and reaching out to State, local, and regional fusion centers and other law enforcement entities with release information related to individuals incarcerated for terror-related offenses. Additionally, the periodic assessment requirement will ensure that the Secretary communicates with appropriate Fed-

eral officials as well as State, local, and regional fusion centers on the overall threat from individuals who are known terrorists currently incarcerated in Federal prison, including the risk of recidivism of these populations upon release.

The Department is best suited to provide this information to State, local, and regional fusion centers due to existing relationships and systems that have been developed between the Department and these entities. Requiring the collection and dissemination of this information does not impose any new requirements on the Bureau of Prisons, as it routinely shares this same information with other Federal partners. The Committee believes that a Memorandum of Understanding between the Secretary and the Attorney General is the appropriate vehicle to facilitate passing this inmate release information to the Department from the Bureau of Prisons.

Sec. 317. Annual report on Office for State and Local Law Enforcement.

This section amends Section 2006(b) of the Homeland Security Act to require the Office for State and Local Law Enforcement (OSLLE) to provide an annual report on their activities for next 5 years. This report must include details of the efforts of the office to coordinate with and improve information sharing between the DHS component agencies, and State, local, and tribal law enforcement; a review of efforts made to improve information sharing through the DHS Homeland Security Information Network (HSIN); the status of performance metrics OSLLE uses; feedback they receive from State, local, and tribal partners; and a description of other ongoing efforts to meet their statutory mandates.

As the Department's primary liaison between DHS and State and local law enforcement agencies, it is critical OSLLE maintains a robust relationship with these key stakeholders. The production of an annual report detailing OSLLE's activities will encourage this office to continually identify gaps and areas for improvement in the Department's information sharing efforts with State and locals, and coordinate with relevant DHS component agencies to close these gaps. The requirement that OSLLE provides performance metrics and details on the feedback the office receives from State and locals will provide much needed assistance to the Committee in its oversight of this office.

Sec. 318. Annual catalog on Department of Homeland Security training, publications, programs, and services for State, local, and tribal law enforcement agencies.

This section amends section 2006(b)(4) of the Homeland Security Act to require the Office of State and Local Law Enforcement (OSLLE) to produce and disseminate an annual catalog that summarizes opportunities for training, publications, programs, and services available to non-Federal law enforcement agencies from the Department, and disseminate it to State and local law enforcement entities within 30 days of production. In furtherance of its role as the Department's liaison to State and local law enforcement it is incumbent on the OSLLE to proactively identify ways in which the Department can support these important stakeholders. This section promotes these efforts by requiring the OSLLE to continue

to produce this resource and ensuring that the services described in the catalog are relevant and useful to State and locals.

This section also requires DHS to share the catalog through the Homeland Security Information Network (HSIN) and share a copy with the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate. This catalog is a product OSLLE currently produces. This section will require them to continue to do so. By requiring the OSLLE to share this catalog on HSIN, section 318 encourages OSLLE to utilize this important information sharing platform that many State and local law enforcement partners rely upon to receive information from the Department. It also ensures this catalog reaches as many of these stakeholders as possible.

Furthermore, this section adds a new requirement for OSLLE to coordinate with other DHS components and Federal agencies to develop and share information on other Federal resources available to enhance fusion center access to information and resources.

TITLE IV-MARITIME SECURITY

Sec. 401. Strategic plan to enhance the security of the international supply chain.

This section requires DHS Secretary submit a strategic plan to Congress every 3 years to address threats to the international supply chain.

Specifically, this section requires an updated strategy, and a subsequent updated strategic plan to be submitted to Congress every 3 years. This ensures that the strategy to secure the highly complex international supply chain, which is responsible for 30 percent of the U.S. economy, is adapting to the present threat environment.

Congress has not received a Strategic Plan to Enhance the Security of the International Supply Chain since the initial passage of the Safe Port of 2006. The Committee believes that as threats to our supply chain and ports evolve, so must our whole of government approach to security.

Sec. 402. Container Security Initiative.

This section is a clerical change to existing Container Security Initiative (CSI) language that removes the requirement for an outdated report.

CSI is a valuable security program that detects and resolves threats before it reaches our shores and the Committee strongly supports it.

Sec. 403. Cyber at ports.

This section amends the Maritime Transportation Security Act (MTSA) and formally gives the United States Coast Guard (USCG) responsibility for cybersecurity at ports. While USCG does not currently have operational authority of cybersecurity at ports, it is responsible for ensuring that cybersecurity is part of the USCG approved facility security plan for ports. With the language proposed in this section, this will be formally codified in MSTA.

Additionally, this section requires the Coast Guard to share information related to cybersecurity risks and incidents among port partners through the National Maritime Advisory Committee.

The Committee believes that our ports and the automated systems that control them are vulnerable to cyber-attacks, which could be devastating to the transit of international commerce. While USCG inspects and approves what are known as "facility security plans" at ports twice a year, these plans are not currently required to have a cybersecurity strategy. The Committee believes that requiring facility operators to have a cyber security plan, and providing them with a mechanism to share best practices and receive current intelligence, is critical to maintaining the uninterrupted flow of maritime commerce and the security of our ports.

Sec. 404. Facility inspection intervals.

Under the Maritime Transportation Security Act (MTSA), USCG is currently required to verify and inspect the implementation of a port's facility security plan twice a year: once announced, and once unannounced. This section amends MTSA to require inspections at every facility at least once a year, but allows USCG to complete additional inspections in a risk-based manner, given a limited number of resources.

This section ensures that both the low-risk grain terminal and the high-risk LNG terminal are inspected at least once a year, but allows USCG to prioritize the highest risk and conduct only one inspection of the grain terminal, and three inspections of the LNG terminal if deemed necessary. The Committee believes that by giving USCG the flexibility to conduct port inspections in a risk-based manner it will increase the security of our most vulnerable ports. For example, currently, both a grain terminal and a Liquid Natural Gas (LNG) terminal are required to be inspected by the USCG twice a year.

Sec. 405. Updates of maritime operations coordination plan.

This section directs the DHS Secretary to update the Maritime Operations Coordination Plan (MOC-P) to decrease duplicative operations between the USCG and CBP AMO. The last MOC-P was signed in 2011 and many of its provisions were never actualized by DHS. Updating the MOC-P is also a DHS OIG recommendation in a recent report on USCG and CBP AMO duplicative operations.

The Committee is concerned with the continued lack of DHS interagency cooperation and a duplication of efforts, particularly in the maritime domain. Updating the MOC-P will allow the Department to take a renewed look at how to best allocate maritime resources.

Sec. 406. Evaluation of Coast Guard Deployable Specialized Forces.

This section directs the DHS Secretary to update the Maritime Operations Coordination Plan (MOC-P) to decrease duplicative operations between the USCG and CBP AMO. The last MOC-P was signed in 2011 and many of its provisions were never actualized by DHS. Updating the MOC-P is also a DHS OIG recommendation in a recent report on USCG and CBP AMO duplicative operations.

The Committee is concerned with the continued lack of DHS interagency cooperation and a duplication of efforts, particularly in the maritime domain. Updating the MOC-P will allow the Department to take a renewed look at how to best allocate maritime resources.

Sec. 407. Cost benefit analysis of co-locating DHS assets.

This section requires the Comptroller General to submit to Congress a report that describes and assesses the State of the Coast Guard's homeland security related Deployable Specialized Forces (DSF). This report will address the cost, capability and operations completed as part of the program. This report will also provide recommendations for future coordination of the DSF.

The Committee believes the DSF provides the Coast Guard with a necessary counter-terrorism, anti-terrorism and counter-narcotic capability. However, the Committee is concerned that some of the high-cost capabilities of the DSF have not provided tangible operational results to date. The Coast Guard made many changes following the Stem to Stern Review of the Deployable Specialized Forces and this section will provide additional insight for the future direction of the DSF program.

Sec. 408. Repeal of interagency operational centers for port security and secure systems of transportation.

This section requires DHS to examine locations where both CBP AMO and the USCG have maritime or aviation assets deployed and to determine the potential for cost savings through co-location. The Committee strongly believes that where operationally feasible, DHS should maximize limited resources and increase operational efficiencies.

Sec. 409. Maritime security capabilities assessments.

This section repeals the mandate for brick and mortar interagency operations centers, giving the Department the flexibility to proceed with virtual situational awareness tool or to leverage existing, proven, interagency coordination mechanisms such as the Regional Coordinating Mechanisms (RECOMs), or the newly enacted Border Security Joint Task Forces to accomplish the same goal.

This section also repeals an obsolete section in U.S. Code (46 U.S.C. 70116) that was updated by the Safe Port Act of 2006 and never repealed.

Sec. 410. Conforming and clerical amendments.

This Section requires the Secretary of the Department of Homeland Security to submit a report to the congressional homeland security committees that details how many maritime assets and personnel the Department would need to increase the interdiction rate of illicit activity in the Transit Zone.

The Committee is concerned that, with the current force laydown and current resource constraints, the Coast Guard is only able to interdict 30 percent of known illicit drug loads moving through the Transit Zone. This reporting requirement will provide a valuable addition to metrics already required by the 2017 National Defense Authorization Act (Pub. L. 114–328) to identify the number of as-

sets and personnel required to increase the Department's interdiction rate of known illicit activity in the Transit Zone.

TITLE V-TRANSPORTATION SECURITY ADMINISTRATION

SUBTITLE A-ADMINISTRATION

Sec. 501. Amendments to the Homeland Security Act of 2002 and title 5, United States Code.

This section amends the Homeland Security Act of 2002 to re-establish the official position and title of the Administrator of the Transportation Security Administration (TSA). It also amends Title 5 of the United States Code to add the Administrator as an officer of the Department of Homeland Security (DHS) and ensure that the Administrator's level and pay rate are appropriate for an Assistant Secretary.

When TSA was transferred to DHS from the Department of Transportation via the Homeland Security Act of 2002, the Administrator's position, title, and level did not transfer along with it. This section addresses these gaps by reinstating the Administrator as an Assistant Secretary within DHS.

Sec. 502. Amendments to title 49, United States Code.

This section amends Title 49 of the United States Code to reflect current policy by ensuring that the TSA Administrator, DHS, and the DHS Secretary are included in the appropriate places in Federal statute. This clarifies that TSA is a component of DHS and ensures that the Administrator has the appropriate title and the 5-year term originally intended by Congress. This section also establishes and updates offices and positions within TSA to ensure that it can successfully carry out its mission. This includes the Deputy Administrator; the Office of Public Affairs; the Office of Civil Rights, Liberties, Ombudsman, and Traveler Engagement; the Office of Legislative Affairs; the Office of Finance and Administration; the Office of the Chief of Operations; the Office of the Chief of Mission Support; the Office of the Chief Counsel; and the corresponding heads of such offices.

When TSA was transferred to DHS from the Department of Transportation via the Homeland Security Act of 2002, the Administrator's original 5-year term did not transfer along with it. This section reinStates that 5-year term to ensure consistent leadership at TSA, as originally intended by Congress. Additionally, the transfer of TSA and the absence of any authorization legislation since has left many outdated titles, roles, and responsibilities. This section addresses those issues by updating Federal statute to conform to current policy and practice.

Sec. 503. Amendments to the Aviation and Transportation Security Act.

This section amends the Aviation and Transportation Security Act (ATSA) to ensure that Federal statute accurately reflects current policy and appropriate roles of TSA.

ATSA, which created TSA in 2001 after the 9/11 terrorist attacks, contains outdated titles and responsibilities. This section

modernizes ATSA by updating the titles and responsibilities appropriate for TSA's current mission.

Sec. 504. Information required to be submitted to Congress under the strategic 5-year technology investment plan of the Transportation Security Administration.

This section amends the Homeland Security Act of 2002 to require TSA to annually report to Congress information about technological acquisitions completed in the preceding and current fiscal year. The section also directs the Administrator of TSA to submit to Congress notice of any increase or decrease in the dollar amount allocated to the procurement of a technology or increase in the number of units of a technology. Additionally, this section requires the Administrator to submit to Congress a report on technology in use after its operational lifecycle or its useful life projection, as specified by either the manufacturer or TSA's own 5-year technology investment plan. Finally, TSA is required to notify airports and airlines of any changes to the 5-year technology investment plan.

Congress previously enacted legislation to require a 5-year technology investment plan for TSA, in order to provide greater transparency for policymakers and stakeholders into the direction TSA intends to go in technology procurement. Unfortunately, TSA issued disparate strategic guidance among different documents, thus continued to cause confusion among industry stakeholders. This legislation will ensure that TSA's 5-year plan is updated more consistently and that Congress and stakeholders are informed of any changes in procurement costs.

Sec. 505. Maintenance of security-related technology.

This section amends the Homeland Security Act of 2002 by requiring the Administrator to develop and implement a preventative maintenance validation process for security-related technology deployed to airports within 180 days of enactment. This process must provide guidance to Administration personnel at airports on how to conduct and document preventative maintenance actions, as well as mechanisms for the Administrator to verify compliance with the newly implemented procedures.

Additionally, this section specifies that when preventative maintenance is carried out by a contractor additional reporting and verification processes must be put into place. The contractors must provide the appropriate Administration personnel with monthly preventative maintenance reports that include information on what specific actions were carried out by the contractor, notification to appropriate Administration personnel when maintenance action is completed, and an independent process to verify the contractor's claims.

Last, this section requires the Administrator to impose penalties for noncompliance when preventative and/or corrective maintenance does meet contractual requirements or manufacturer specifications.

The Department of Homeland Security Office of the Inspector General recently issued a report entitled "The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program" (DHS OIG–15–86) which ex-

amined the TSA's airport screening equipment maintenance program and determined that adequate policies and procedures had not been implemented. This has resulted in equipment not being maintained to the specifications required by the manufacturer. Additionally, TSA did not have adequate policies to oversee if the routine preventative maintenance was accomplished resulting in equipment not being ready for operational use. This could shorten the operational life of some equipment and incur unnecessary costs to replace it. Additionally, the equipment, if not properly maintained, has the potential to be less effective at detecting dangerous items, which could jeopardize passenger and airline safety.

Sec. 506. Transportation Security Administration efficiency.

This section requires the Administrator to conduct a comprehensive, agency-wide efficiency review to identify and effectuate spending reductions and savings by streamlining and restructuring TSA. In the review, the Administrator shall consider the elimination of unnecessarily duplicative programs; the elimination of unnecessary rules, regulations, directives, or procedures; and the reduction of overall operating expenses, including costs associated with the number of personnel. The Administrator must also report to Congress on the results and potential savings of the review.

Since its creation in 2001 after the 9/11 terrorist attacks, TSA has struggled to accomplish its mission in an efficient manner. Low employee morale, leadership turnover and bureaucracy, prolonged airport wait times, and failed internal investigations are just a few of the challenges that TSA continues to face. This section seeks to address these issues by forcing an internal accounting of the agency with an emphasis on efficiency, organization, and savings in order to improve TSA's ability to focus on its important transportation security mission.

Sec. 507. Transportation senior executive service accountability.

This section requires the DHS Secretary, acting through the TSA Administrator, to develop a strategic plan to reduce the number of Senior Executive Service (SES) positions at TSA by 20 percent by June 30, 2019. The Administrator must submit a copy of the plan to Congress.

Currently TSA has over 160 SES positions-more than any other DHS component-with the average salary of over $160,000, which is above the General Schedule (GS)–15 level. Given the high salaries and other benefits granted to SES employees—as well as the large number of such positions at TSA—this section seeks to restore accountability and savings of taxpayer dollars.

SUBTITLE B-PASSENGER SECURITY AND SCREENING

Sec. 511. Department of Homeland Security trusted traveler program collaboration.

This section directs the Secretary of Homeland Security to continue its review of all trusted traveler vetting programs to make recommendations on possible efficiencies that could be gained by integrating requirements and operations and increasing information and data sharing across programs.

The Department of Homeland Security offers several trusted traveler programs that passengers can enroll in thereby allowing the government to vet them to ensure they are not a threat in exchange for expediting screening. However, because these trusted traveler vetting programs are administered by different components within the Department interoperability issues have arisen such as those between TSA PreCheck and CBP Global Entry. The Department should work to ensure that these programs can interface and seek to gain efficiencies by exploring opportunities to harmonize requirements and operations and increase information and data sharing.

Sec. 512. PreCheck Biometric pilot project.

This section requires the Administrator of TSA to conduct a pilot project to test secure, automated and biometric-based systems at airports to verify the identity of individuals who are members of TSA PreCheck or another Department of Homeland Security trusted traveler program. The biometric-based systems must be designed to improve security while reducing the need for security screening personnel to perform identity and travel document verification; reduce average wait times; reduce Administration operating expenses; be integrated with DHS watch listing and trusted traveler programs; and be integrated with other technologies to further facilitate risk-based passenger screening at checkpoints, to the extent practicable.

The Committee believes that the significant advancements in biometric identity verification technology by both the public and private sectors present an opportunity for TSA to improve security while reducing the need for personnel to perform identity and travel document verification. Through the TSA PreCheck program, the Administration maintains the fingerprint records of individuals enrolled in the program and therefore such technology can be piloted in PreCheck passenger screening lanes using existing datasets.

Sec. 513. Identity and travel document verification.

This section requires the Administrator of TSA, no later than December 31, 2018, subject to the availability of appropriations, to implement a secure, automated system at all airports, for verifying travel and identity documents of passengers who are not members of a Department of Homeland Security (DHS) trusted traveler programs. Such system shall assess the need for security screening personnel to perform identity and travel document verification for such passengers, thereby assessing the overall number of such screening personnel; reduce the average wait time of passengers; reduce the overall operating expenses of the Administration; be integrated with the Administration's watch list matching programs and other technologies to further facilitate risk-based passenger screening.

The 9/11 Commission report noted that fraud in identification documents and boarding passes was a critical weakness in the system that needed to be prevented. To this end, in 2014 the Transportation Security Administration (TSA) awarded a contract for credential authentication technology. This technology has been tested and piloted multiple times to ensure its effectiveness. However, the deployment of this technology has been repeatedly de-

layed. The committee directs TSA to prioritize deployment of this technology across the Nation's airports no later than December 2018.

Sec. 514. Computed tomography pilot project.

This section directs TSA to conduct a pilot program to test the use of technology using computed tomography to screen baggage at passenger checkpoints.

The committee believes that TSA should pilot computed tomography technology, which has long been used to screen passenger baggage, at the checkpoint to determine if such technology could improve detection of threat items by security screening personnel in carry-on baggage.

Sec. 515. Explosives detection canine teams for aviation.

The section requires the Administrator to ensure at least 300 explosive detection canine teams dedicated to passenger screening are deployed at airports by December, 31, 2018.

In a briefing to the committee, the Transportation Security Administration (TSA) indicated that 300 passenger screening canine teams would be the optimal number to achieve the desired level of security and efficiencies by using canines to detect screening anomalies. Further, TSA indicated that training and deploying 300 canine teams by December 31, 2018, is a reasonable and achievable goal. Therefore, the committee expects that TSA will meet this goal or otherwise notify the committee in advance as to why it will not be possible to deploy 300 passenger screening canine teams by the aforementioned deadline.

Sec. 516. Standard operating procedures at airport checkpoints.

This section requires the Administrator of TSA to ensure that standard operating procedures at airport checkpoints for passengers and carry-on baggage are carried out in a uniform manner among similarly situated airports, to the extent practicable. This section also requires the Administrator to report to Congress, not later than 270 days after enactment of this Act, on how standard operating procedures were made uniform. Further, 1 year after enactment of this Act, the Inspector General of the Department of Homeland Security shall conduct periodic audits of adherence to standard operating procedures at large, medium and small airports in diverse geographical areas.

An overabundance of standard operating procedures (SOPs) for security screening personnel at airport security checkpoints was burdensome to screeners and has the potential to reduce screening effectiveness. Recognizing that different protocols are necessary for airports of differing sizes and locations, the committee directs TSA to continue to streamline SOPs at checkpoints, to the greatest extent possible.

Sec. 517. Traveler redress improvement.

This section requires the Administrator of the Transportation Security Administration (TSA) to ensure availability of the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) to adjudicate inquiries for individuals who are U.S. citizens or lawful permanent residents; have filed an inquiry with

DHS TRIP after receiving enhanced screening at an airport passenger security checkpoint more than three times in any 60-day period; and believe they have wrongly been identified as a threat to aviation security. It also requires the Administrator to provide a report to the House Committee on Homeland Security and the Senate Committee on Commerce, Science and Transportation on the implementation of the process described above not later than 180 days after enactment of this Act.

This section also requires the Administrator of TSA to review and update the Privacy Impact Assessment for the Secure Flight programs to ensure that the Assessment accurately reflects the operation of such programs. It requires the Assessment to be published on a publicly available website and submitted to the House Committee on Homeland Security and the Senate Committee on Commerce, Science and Transportation.

Additionally, this section requires the Assistant Administrator of TSA's Office of Intelligence and Analysis to coordinate a comprehensive review of the Transportation Security Administration's intelligence-based screening rules 60 days after the enactment of this Act and every 120 days thereafter in conjunction with TSA's Office of Civil Rights and Liberties, Office of the Ombudsman, Office of Traveler Engagement, Office of Chief Counsel, Privacy Office, the Federal Air Marshal Service, and DHS's Office of Civil Rights and Liberties, Office of General Counsel, Privacy Office and Traveler Redress Inquiry Program. It also requires that all of these entities be notified not later than 48 hours after changing, updating, implementing or suspending an intelligence-based screening rule.

This section also requires that the TSA Administrator ensures that intelligence-based screening rules are incorporated in the risk analysis conducted during the Federal Air Marshal mission scheduling process. Not later than 180 days after enactment of this Act the Administrator is required to submit a report to the House Committee on Homeland Security and the Senate Committee on Commerce, Science and Transportation on the implantation of the new scheduling process.

This section also requires that the Government Accountability Office conduct a study on the effectiveness of intelligence-based screening rules on mitigating potential threats to aviation security not later than 1 year after enactment of this Act. The study will also examine the coordination between TSA, DHS and other relevant partners relating to changing, updating, implementing or suspending intelligence-based screening rules.

TSA employs intelligence-based screening rules to flag individuals for enhanced screening at security checkpoints-on both domestic flights and flights coming into the United States from abroad. This program was conceived by TSA's Office of Intelligence Analysis as a way to identify individuals who may not be formally watchlisted, but may present a risk to aviation security.

The Committee has significant concerns with TSA's intelligence-base screening rules program as it circumvents the formal watchlisting process. Moreover, while there is a redress process to adjudicate cases of individuals who are placed on the "No Fly List," there is currently no redress process for an individual who feels

that they have been repeatedly selected for enhanced screening due to an error.

Sec. 518. Screening in areas other than passenger terminals.

This section authorizes the Administrator of TSA to provide screening services to commercial charter air carriers in areas other than primary passenger terminals upon the request of such a carrier. Such a carrier requesting such services shall direct the request to the Federal Security Director of the airport where such services are requested. The Federal Security Director of such airport may provide screening services if they are available. The Administrator shall enter into an agreement with a commercial charter air carrier for compensation for all reasonable costs, including overtime, of such screening services.

The committee believes that the Administrator should have the authority to provide security screening services to a commercial charter air carrier in areas other than primary passenger terminals, as long as the commercial charter air carrier has entered into an agreement with TSA to provide reimbursement for such services, and the Federal Security Director has security screening personnel and other resources available.

Sec. 519. Federal Air Marshal Service agreements.

This section directs the Administrator to develop a standard working document that shall be the basis of all negotiations and agreements between the FAMS and foreign governments and partners regarding Federal Air Marshal coverage of flights to and from the United States. This section also requires such agreements to be written and signed by the Secretary of Homeland Security or the Secretary's designee. Following the signing of such agreements, the relevant congressional committees must be notified within 30 days.

The committee believes that the Federal Air Marshal Service (FAMS) should develop a written document outlining the basis of all negotiations and agreements for FAMS coverage between the U.S. and foreign governments or partners. Further, the committee is concerned that the Federal Air Marshal Service does not maintain written agreements between the United States and foreign governments or partners outlining the terms and conditions of agreements pertaining to the coverage of flights by Federal Air Marshals. In the past, the Administration has refused to provide the committee with information and documentation regarding FAMS agreements hindering the committee's oversight efforts, making it necessary for the Administration to transmit all new agreements to Congress.

Sec. 520. Federal Air Marshal mission scheduling automation.

This section directs the Administrator of TSA to seek to acquire automated software for the scheduling of FAMS missions based on current risk modeling.

Currently, the Federal Air Marshal Service relies on manual methods to schedule missions. Given the existence of off-the-shelf and customizable scheduling software, the committee directs FAMS to pursue automated scheduling software to achieve increased efficiencies and security effectiveness.

Sec. 521. Canine detection research and development.

This section requires the Department of Homeland Security (DHS) to conduct an audit of all canine training programs within DHS and convene a working group of representatives from all such programs to make recommendations on possible efficiencies that could be gained by integrating training standards and facilities.

This section also requires the Administrator of the TSA to develop a staffing allocation model for canines to determine the optimal number of passenger screening canines at airports in the United States.

Finally, this section requires the Secretary of DHS to submit to the House Committee on Homeland Security and the Senate Committee on Commerce, Science and Transportation a report on the recommendations made in the aforementioned working group not later than 180 days after enactment of this Act.

Canines are an invaluable passenger screening tool in that they both reduce checkpoint wait times and increase security effectiveness. Demand for additional canine teams remains high, but TSA is not currently training enough canines to meet the ongoing need. TSA should explore expanding kennel space at the existing training facility at Lackland Air Force Base or opening a second training facility. Further, the committee requests a briefing by TSA on outreach and coordination efforts with private explosive detection canine production and training companies.

Sec. 522. International Civil Aviation Organization.

This section directs the U.S. Ambassador or Charge d'Affaires to the United States Mission to the International Civil Aviation Organization to pursue improvements to airport security, including introducing a resolution to raise minimum standards for airport security if practicable. This section also directs the Ambassador or Charge d'Affaires to report to the relevant congressional Committees no later than 180 days after the enactment of this Act on the aforementioned efforts.

The committee believes that the minimum security standards for airport security set forth by the Chicago Convention established by the International Civil Aviation Organization are not robust enough in the current threat environment where we have repeatedly seen terrorist organizations planning attacks targeting aviation. Therefore, the committee believes the United States should take a leadership role at the ICAO in building consensus among member States to raise these standards.

Sec. 523. Passenger security fee.

This section prohibits the Secretary of Homeland Security from incorporating an increase in the passenger security fees under section 44940 of title 49 U.S. code in the annual budget proposal to Congress unless an increase to the fee has been authorized by Congress prior to the submission of the President's Budget Proposal.

For a number of years, both Republican and Democratic Administrations have proposed increases in the passenger security fee as an offset in the annual budget proposal, despite no such fee increase having been authorized by Congress. The committee believes this practice should not continue absent an authorization of an increase in the passenger security fee by Congress.

Sec. 524. Last point of departure airport certification.

This section amends Subparagraph (B) of section 44907(a)(2) of title 49, United States Code, by inserting ", including the screening and vetting of airport workers" before the semicolon at the end.

In light of evolving threats to aviation security by individuals with access to sensitive areas of the airport and aircrafts, the Committee believes that TSA should collect data about how airport workers are vetted at airports that serve as last points of departure to the United States.

Sec. 525. Security standards at foreign airports.

This section amends section 44907 of title 49, United States Code, in subsections (a) through (d) by striking "Secretary of Transportation" each place it appears and inserting "Secretary of Homeland Security". This section also amends section 44907 of title 49, United States Code, in subsection (e), in the matter preceding paragraph (1) by striking "and 40106(b) of this title, the Secretary of Transportation, with the approval of the Secretary of State and without notice or hearing, shall" and inserting "40106(b), and 41307 of this title, at the request of the Secretary of Homeland Security and with the approval of the Secretary of State and without notice of a hearing, the Secretary of Transportation shall". Finally this section also amends subsection (e) by striking "when the Secretary of Transportation decides" and inserting "when the Secretary of Homeland Security decides".

When responsibility for aviation security was transferred from the Department of Transportation to the Department of Homeland Security, Section 44907 of title 49, United States Code, was not updated to reflect this change. This section makes it clear that it is the Secretary of Homeland Security that is ultimately responsible for taking actions to ensure that foreign airports and air carriers are in compliance with internationally recognized security standards and has the authority to suspend flights from last point of departure airports due to security related concerns.

Sec. 526. Security incident response at airports and surface transportation hubs.

This section amends the Gerardo Hernandez Airport Security Act of 2015 (Public Law 114–50; 49 U.S.C. 44903 note) in section 3 subsection (b), in the matter preceding paragraph (1), by striking "may" in each place it occurs and inserting "shall"; by redesignating subsection (c) as subsection (d); and by inserting after subsection (b) a new subsection which requires the Administrator of the TSA to review the active shooter response guidelines specified for Department of Homeland Security personnel and make a recommendation to the Secretary of DHS to modify such guidelines for personnel who are certified Federal law enforcement officials and for personnel who are uniformed but unarmed security officials. This section also amends section 7 of the aforementioned Act by in subsection (b), in the matter preceding paragraph (1), by striking "may" in each place it appears and inserting "shall" and by redesignating subsections (c) and (d) as subsections (d) and (e) and inserting after subsection (b) a subsection which requires the Administrator of TSA to review the active shooter response guidelines specified for Department of Homeland Security personnel and make a

recommendation to the Secretary of DHS to modify such guidelines for personnel who are certified Federal law enforcement officials and for personnel who are uniformed but unarmed security officials.

On January 6, 2017, an active shooter opened fire in the baggage claim area of Fort Lauderdale-Hollywood International Airport causing a mass evacuation of the airport. A perceived active shooter situation at John F. Kennedy International Airport on August 14, 2016, similarly caused a mass evacuation and subsequent delay. In the wake of these incidents, it is clear that our Nation's airports are not all adequately prepared to coordinate mass evacuations therefore the committee deems it necessary to require airports to prepare for these situations.

Further, following these incidents there were reports of uniformed TSA personnel adding to the chaos and panic by running and pushing passengers as they exited the terminals. It is the committee's understanding that the Department of Homeland Security trains all personnel to "run, hide, fight" in the event of an active shooter situation. However, it does not seem appropriate for all personnel to receive this training given that there are certified Federal law enforcement officers that work for the Department. The committee believes that despite the fact that transportation security officers are not law enforcement officials, the Secretary should consider revising active shooter guidance for these individuals who serve important safety and security functions.

Sec. 527. Airport security screening opt-out program.

This section requires the Administrator of TSA to make best efforts to enter into a contract with a private screening company to provide screening services at an airport not later than 180 days after the date of approval of an application submitted by the operator of such airport. This section also amends the aforementioned section of the U.S. Code in subparagraph (A) of paragraph (4), as so redesignated, in the matter preceding clause (i), by striking "not later than 60 days following the date of the denial" and inserting "immediately upon issuing the denial".

Furthermore, this section strikes subsection (h) of the aforementioned section of the U.S. Code and inserts a new subsection (h) which allows the Administrator of TSA to nominate to the head of the contracting activity an individual representing the airport operator that applied and has been approved to have security screening services carried out by a qualified private screening company. This section also adds a new subsection (i) which encourages the operator of an airport at which screening services are provided to recommend to the Administrator of the TSA innovative screening approaches and technologies. Upon receipt of such recommendations, the Administrator shall review and, if appropriate, test, conduct a pilot project, and, if appropriate, deploy such approaches and technologies.

The committee believes that when an airport chooses to participate in the Screening Partnership Program (SPP) that they should participate in the contract evaluation and award process. Additionally, the period of time between when the SPP application is submitted, approved and the contract decision made is unduly lengthy

and should be truncated to the greatest extent possible without sacrificing the integrity of the procurement process.

Sec. 528. Personnel management system review.

This section requires the Administrator of TSA to convene a working group consisting of representatives of the Administration and representatives of the labor organization representing security screening personnel to discuss reforms to the Administration's personnel management system, including appeals to the Merit Systems Protection Board, not later than 30 days after enactment of this Act. This section also requires the working group to transmit to the House Homeland Security Committee and the Senate Committee on Commerce, Science and Transportation a report containing recommendations to reform the Administration's personnel management system, not later than 1 year after enactment of this Act.

The committee acknowledges that Transportation Security Officers (TSOs) believe they have legitimate grievances that they cannot address through the existing grievance resolution process. The committee believes that TSA could improve and streamline the grievance resolution process in a way that would gain efficiencies at headquarters and improve the morale of frontline workers. Therefore, the committee believes that TSA should establish a working group in conjunction with the American Federation of Government Employees (AFGE) which represents security screening officers and issue a report with recommendations to improve the grievance resolution process. The committee does not expect TSA to implement the recommendations in this report absent further congressional action.

Sec. 529. Innovation task force.

This section allows the Administrator of TSA to establish a task force to collaborate with air carriers, airport operators, and other aviation security stakeholders to foster the pursuit of innovations in aviation security prior to the acquisition process. The task force is authorized to conduct activities designed to identify and develop an innovative technology or capability with the potential of enhancing aviation security. This section also authorizes the composition of such a task force and notes that the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply.

The Committee supports the work done by TSA's Innovation Task Force (ITF), which was originally established by former Administrator Neffenger in the Spring of 2016. The Committee encourages the ITF to continue its collaboration with aviation and surface transportation security stakeholders in an effort to develop, test and deploy innovative new technology in areas at and outside the security screening checkpoint, such as employee screening checkpoints and the public areas of airports. The ITF's initial focus on automated screening lane technology shows promises at enhancing passenger facilitation and security operations, more recent lines of effort in technologies such as computed tomography and biometric identification are welcome developments.

Sec. 530. Airport law enforcement reimbursement.

This section directs the Administrator of TSA to submit to the House Committee on Homeland Security and the Senate Committee on Commerce, Science and Transportation, a report on TSA's law enforcement officer reimbursement program, not later than 120 days after the date of enactment of the Act. This report shall include information related to the current structure of the program and law enforcement activities covered by the program, an assessment of threats at airports, the annual costs to airport authorities for providing law enforcement for covered activities related to the security checkpoint, and proposed methodology for funding allocations.

In the Administration's Fiscal Year budget proposal to Congress, the Administration proposed the elimination of the airport law enforcement reimbursement program. The committee recognizes that budgets across the Department of Homeland Security and the whole of government are constrained. However, airports and airlines remain a high-profile target for terrorists and other criminals conducting illicit activity that has the potential to put the public in danger. While the Transportation Security Administration provides security screening services at the checkpoint, these individuals who provide such services are not sworn law enforcement and do not have the authority, equipment or training to make arrests or interdict criminal or terrorist activity. Therefore, a robust law enforcement presence at airports is critical to ensuring the safety of the traveling public. The committee supports TSA reimbursement of local law enforcement for these purposes, and given the changing threat environment believes TSA should reexamine the threat and provide the committee with recommendations to reform the program to ensure that resources are being directed where the need is most acute.

SUBTITLE C-TRANSPORTATION SECURITY SCREENING PERSONNEL TRAINING AND ACCOUNTABILITY

Sec. 531. Transportation security training programs.

This section authorizes the TSA training program for new security screening personnel at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. This section also requires the Administrator of TSA to establish recurrent training for security screening personnel that addresses updates to screening procedures and technologies not later than 180 days after enactment of this Act. Finally, this section requires the Government Accountability Office to issue a report on the findings of a study on the effectiveness of the security screening personnel initial training program at FLETC.

In January 2015, former TSA Administrator Peter Neffenger established the TSA Academy at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia, in order to establish a centralized, consistent and coordinated approach to training new security screening personnel. In addition to the training program for new security screening personnel, TSA also developed new training for Transportation Security Executive Service level executives and other employees at various levels throughout the agency.

The committee is encouraged by these developments, but would like to see independent validation by the Government Accountability Office that the training at the Academy is leading to improved performance and effectiveness and is a valuable use of taxpayer dollars.

Sec. 532. Alternate new security screening personnel training program cost and feasibility study.

This section requires the Administrator of TSA to conduct a cost and feasibility study of developing a training program within 50 miles of a security screening personnel's duty station that will provide such personnel with an equal level of training as is administered at FLETC.

While the establishment of a unified training center for transportation security officers (TSOs) in Glynco, Georgia, at the Federal Law Enforcement Training Center (FLETC) has reportedly increased the morale and strengthened the mission of TSA, it also has unintended consequences. The academy requires new TSOs to spend 6 weeks in Glynco, possibly dissuading highly qualified and motivated individuals from applying to TSA due to family and other obligations, such as lack of childcare or enrollment in school. TSA should examine the impact of these unintended consequences on its recruiting efforts and ability to onboard part-time personnel when necessary, and conduct a cost and feasibility assessment of training to the same curriculum and standards at FLETC that would be accessible to individuals who are unable to travel for an extended period of time.

Sec. 533. Prohibition of advance notice of covert testing to security screeners.

This section requires the Administrator of the Transportation Security Administration (TSA) to ensure, to the greatest extent practicable, that information concerning a covert test of a transportation security system to be conducted by a covert testing office, the Inspector General of the Department of Homeland Security or the Government Accountability Office is not provided to any individual involved in such test prior to its completion. This section also outlines a number of exceptions to the prohibition of advanced notification described above.

The committee directs the Administrator of TSA, to the greatest extent practicable, to ensure that the least number of people possible are notified of covert testing done at airport security screening checkpoints. The committee recognizes that a limited number of individuals need to be notified prior to testing to ensure the safety of personnel conducting testing, and that it may be necessary for such personnel to disclose their identity to avoid panic that could lead to a public safety or security incident. However, disclosure of covert testing should be limited to avoid compromising the integrity of testing results and trends.

SUBTITLE D-AIRPORT ACCESS CONTROLS AND PERIMETER SECURITY

Sec. 541. Reformation of certain programs of the Transportation Security Administration.

Subsection (a) provides definitions for the following terms in correspondence with the act. The term "Administration" means the Transportation Security Administration (TSA). The term "Administrator" means the Administrator of the Transportation Security Administration. The terms "air carrier" and "foreign air carrier" have the meaning given such terms in section 40102 of title 49, United States Code. The terms "secured area," "Security Identification Display Area," and "sterile area" have the meaning given such terms in section 1540.5 of title 49, Code of Federal Regulations. "Appropriate congressional Committees" refers to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate. The final term, "Intelligence Community," refers to the meaning given such a term in section 3(4) of the National Security Act of 1974 (50 U.S.C. 3003 (4)).

Subsection (b) amends the Homeland Security Act of 2002 by directing the Administrator in consultation with the Aviation Security Advisory Committee to submit to the appropriate congressional committees and the Comptroller General of the United States, a cost and feasibility study of a statistically significant number of airports. The study should concern the cost and feasibility of all employee entry and exit points that lead to secure areas of airports being comprised of a secure door with a card and pin entry or biometric technology, surveillance video that is stored for at least 30 days, and advanced screening technology. The advanced screening technology ought to include one of the following: a magnetometer, explosive detection canines, explosives trace detection, advanced imaging technology, or x-ray bag screening technology.

The report will include information from airports that already have such technology implemented, screening 100 percent of employees that enter and exit the secure area. The report shall include costs associated with establishing employee entry and exit operational technology and a cost comparison of the requirements based on whether the requirements were implemented by the Administration or the airports. Once the report is complete, the Comptroller General shall review the study for its reliability and efficiency and will report to the appropriate congressional committees. The Committee believes a reliable cost and feasibility study to be a necessary source of data for stakeholders, TSA, and Congress to make future decisions on aviation worker screening at airports. Through significant oversight in the 114th and 115th Congresses, the Committee has found that there remains a lack of effective access controls at airports across the United States, despite increased and pronounced concerns of insider threats to aviation security from individuals with secure access to sterile and otherwise sensitive areas of airports. While stakeholders and TSA have articulated a desire to create an expectation of screening without implementing full employee screening, the Committee has not been provided sufficient data or evidence on the security effectiveness of

different forms and levels of screening. With a litany of access controls breaches in recent years and investigations uncovering extensive criminal networks within the aviation system, the Committee believes more data is necessary as a means of identifying potential future improvements to screening.

Subsection (c) focuses on the security awareness of credentialed airport populations regarding insider threats to aviation security and best practices related to airport access control. The Committee believes that aviation workers with trusted access to sensitive areas of airports should be given security awareness related to the need to mitigate insider threats to aviation and best practices related to access controls.

Within 180 days of the enactment of this Act, the Administrator shall consult various air carriers, foreign air carriers, airport operators, vendors, and airport concessionaries to assess credentialing standards, policies, and practices to ensure that insider threats to aviation security are adequately addressed. The report must be submitted to appropriate congressional committees no later than 30 days after the assessment has been completed. Within 60 days of the enactment of this Act, the Administrator must require social security numbers of individuals applying for SIDA, sterile, and air operations area access. This currently exists as a security vulnerability in the aviation sector, as individuals are not statutorily required to provide social security numbers for vetting purposes, sometimes leaving gaps in necessary vetting capabilities. The Committee believes requiring this data submission along with applications for secure access credentials will enhance the overall integrity of security vetting among credentialed aviation workers.

Subsection (d) requires the Administrator, working with airport operators, to identify advanced technologies that will secure employee access to secure and sterile areas of the airport. The act will also ensure that all credentialed aviation worker populations are constantly vetted through the Federal Bureau of Investigation's Rap Back Service. Within 180 days after the enactment of this Act, the Administrator shall identify means to leverage resources of the Department of Homeland Security and the intelligence community to educate Administration personnel on insider threats. The Administrator shall ensure that the Playbook operations—Administration-led employee physical inspection efforts-are focused on providing the greatest level of security effectiveness. The Committee recognizes that advanced biometric security technologies can provide enhanced legitimacy to access controls at airports. Similarly, the Committee believes that the FBI's Rap Back Service can achieve significant improvements in the visibility the Administration and airports have into potential disqualifying offenses committed by credentialed aviation workers. Ensuring that credentialed populations are enrolled will not only lower the background check costs for airports stakeholders, but will also provide much faster insight into potential insider threats. The agency's Playbook operations sometimes focus on conducting physical inspections of credentialed aviation workers as a means of mitigating potential security risks. The Committee believes that the Administration should work to make these operations more strategic, targeted, and effective in order to achieve the desired expectation of screening. Historically, the Committee has been concerned that

Playbook operations targeting aviation workers has focused too broadly on screening a high number of employees, rather than being strategic in screening areas of vulnerability. While the Committee is encouraged by recent efforts to achieve this goal, this provision will ensure that such inspection efforts achieve maximum security effectiveness.

This provision also works to ensure that the Administrator shall increase covert testing of Playbook employee screening and measure existing security operations. The Administrator shall also provide to appropriate stakeholders the results of the testing, and recommendations on how to improve security screening operations. The Administrator, under this Act shall submit to the appropriate congressional committees an annual transparency report on the frequency, methodology, strategy, and effectiveness of employee screenings at airports. The Committee believes that both Congress and the appropriate stakeholders should have visibility into the effectiveness and results of employee screening operations at airports, in order to obtain an accurate assessment of insider threat mitigation efforts.

The provision also ensures that within 180 days of its enactment, the Administrator, along with the Aviation Security Advisory Committee, shall compile a national data base of airport employees who have had their badges revoked for failure to comply with security requirements. The Administrator will determine the proper reporting mechanisms for airports, air carriers, and foreign air carriers to submit the data of employees with revoked data, as well as access to such a data base. The Administrator will reestablish employees who were wrongly added to the list. Currently, there exists a startling lack of coordination and communication within the aviation security community related to aviation workers who have had their secure credentials revoked. The Committee believes that as the arbiter of security threat assessments for aviation workers, TSA should take steps to establish a national data base of aviation workers who have had their credentials revoked for failure to comply with security requirements. This will enhance TSA's ability to provide accurate security threat assessments to airport stakeholders for individuals applying for access to sensitive areas of airports. The Committee also believes in the need for a redress process for employees who have been wrongly added to such data base.

Subsection (e) requires the Department of Homeland Security, as the lead interagency pertaining to insider threat investigations and mitigation efforts at airports, shall make every effort to coordinate with other relevant Government entities when involved in such investigations.

Subsection (f) authorizes the Secretary of the Department of Homeland Security to utilize Homeland Security Investigations personnel and any other DHS personnel to form airport task forces to investigate and mitigate insider threats to aviation security in coordination with Federal, State, local, tribal, and territorial law enforcement partners. While the Department of Homeland Security serves as the interagency lead on insider threat investigation and mitigation efforts at airports, DHS and its components should make every effort to coordinate with other relevant Federal, State, and local entities. Moreover, this section should not be read to construe a change or modification in existing, well-established jurisdic-

tional boundaries between Federal, State, and local entities. The Committee believes that the Department's Homeland Security Investigations airport task forces are a valuable counterterrorism and insider threat mitigation tool. These task forces have served as interagency coordinators for countless investigations and should remain the primary Federal effort in investigation and mitigating insider threats to aviation security.

Subsection (g) implements a 90 day policy in which the Administrator shall submit to the appropriate congressional committees a plan to conduct recurring reviews of the security controls for Administration information technology systems at airports. This provision is based on recent findings by the Department of Homeland Security's Inspector General that TSA's information technology security is in need of more stringent oversight and accountability.

Sec. 542. Airport perimeter and access control security.

Subsection (a) requires the Administrator of the Transportation Security Administration (TSA) to provide an update to the Transportation Sector Security Risk Assessment (TSSRA) no later than 120 days after the Act's enactment with an aviation sector update. No more than 180 days after the enactment of the Act, the Administrator must also provide an update with the latest and most up-to-date intelligence information pertaining to the Risk Assessment of Airport Security in addition to determining a timeframe for when further updates to the Risk Assessment of Airport Security will occur. No more than 90 days after the Act's enactment, a system-wide assessment of airport access control points and airport perimeter security must also occur.

The security risk assessment shall include those updates reflected in the findings of both the TSSRA and Joint Vulnerability Assessment (JVA) including changes to the risk environment pertaining to airport access control points and airport perimeters. The assessment shall also utilize security data for analysis of system-wide trends related to airport access control points and airport perimeter security so as to better inform risk management decision. Finally, the assessment shall take into consideration the geographic and current best practices utilized by airports to help mitigate potential vulnerabilities. The results of the risk assessments shall be reported by the TSA Administrator to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation of the Senate, relevant agencies and departments, and airport operators. The Committee believes that airport access controls and perimeter security remain a point of vulnerability in the ever changing threat landscape facing aviation security. Despite this, the Committee remains concerned that there is a lack of clear assessment and consistency in perimeter security across the country, and feels there is a need for TSA to take a fresh look at perimeter security.

Subsection (b) requires that no more than 180 days after the Act's enactment, the TSA Administrator must provide an update to the 2012 National Strategy for Airport Perimeter and Access Control Security, also referred to as the National Strategy. This updated National Strategy shall include all information from the Risk Assessment of Airport Security as well as information pertaining to

airport security-related activities, the status of TSA efforts to address the goals and objectives outlined in subsection (a) of the Act, finalized outcome-based performance measures and performance levels for each relevant and goal and objective listed under subparagraphs (A) and (B) of the Act, as well as input from airport operators.

Finally, the TSA Administrator must implement a process for determining when additional updates to the strategy will be needed not more than 90 days after the update in subsection (a) of the Act is completed.

Sec. 543. Exit lane security.

This section authorizes $77,000,000 for each of fiscal years 2018 and 2019 for the purposes of carrying out subsection (n)(1) of section 44903 of title 49, United States Code. This provision concerns funding for staffing of airport exit lanes by Transportation Security Officers. The Committee believes that TSA has a statutory responsibility to continue staffing exit lanes, where the Administration currently provides staffing. However, the Committee understands the importance of finding efficiencies and prioritizing Transportation Security Officers for essential security functions, such as passenger screening, and recognizes that many airports have successfully implemented technology solutions for exit lane security. The Committee also believes that other efficiency and staffing reviews required by this legislation will provide relevant data for exit lane staffing in the future.

Sec. 544. Reimbursement for deployment of armed law enforcement personnel at airports.

This section authorizes $45,000,000 for each of fiscal years 2018 and 2019 to carry out subsection (h) of section 44901 of title 49, United States Code. This provision authorizes funding for TSA's Airport Law Enforcement Reimbursement Program, in order to support security efforts carried out by State and local law enforcement at airports pursuant to 49 U.S.C. 44903(c) and 49 C.F.R. part 1542. The Committee recognizes the value of TSA's funding for airport law enforcement as an important counterterrorism tool serving to protect the airport environment, including passenger screening checkpoints. Additionally, given the heightened nature of threats to soft target areas of transportation systems, such as the prescreening public areas of airports, the Committee believes that a robust law enforcement presence in such areas is important to deterring, preventing, and responding to attacks. As amended, section 529 of this legislation also requires a report on the current structure of this program, as well as information relating to threats requiring law enforcement officer response at airports, the scope of current law enforcement activities covered under this program, the annual costs to airport authorities for providing law enforcement for such covered activities, and a proposed methodology for funding allocations. The Committee believes this will provide important data on how this program can maximize efficiency and security effectiveness.

SUBTITLE E-AIR CARGO SECURITY

Sec. 551. Air cargo advance screening program.

This section directs the Secretary, through the Commissioner of CBP and in coordination with the Administrator of TSA, to implement the long-piloted Air Cargo Advance Screening program, ensuring DHS access to relevant security data and enhanced ability to protect against threats to cargo. The Committee recognizes the desire of both industry stakeholders and the Department to fully implement this program and issue a final rule on air cargo advance screening for the purposes of receiving data and inspecting high-risk cargo. The Committee believes that the Department needs to take actionable steps to implement the program, which is broadly supported by industry, taking into account the lessons learned from the pilot, as well as industry stakeholder perspectives on how the program should be implemented and carried out.

Sec. 552. Explosives detection canine teams for air cargo security.

This section directs TSA to issue standards to be used to certify third-party canines for use in the air cargo sector, in order to expand the number of canines being used for cargo screening and enhance security in an operationally efficient manner. The Committee believes third-party, non-Federal explosives trace detection canines are a valuable tool in screening air cargo and that TSA should issue standards to be used to certify such canines in a timely manner. The Committee recognizes that TSA and industry partners have been working collaboratively on developing processes and standards for the use of third-party, non-Federal explosives detection canines to screening of air cargo and desires to see such collaboration continue.

SUBTITLE F-INFORMATION SHARING AND CYBERSECURITY

Sec. 561. Information sharing and cybersecurity.

This section requires the Administrator to direct Federal Security Directors at airports to meet at least quarterly with relevant stakeholders to discuss incident management protocols and to inform stakeholders of relevant security matters within a timely manner. The section also requires the creation of an information sharing improvement plan to enhance the overall quality of information sharing by TSA. Additionally, this section requires TSA to establish a mechanism through which to share aviation security best practices and develop a cybersecurity risk assessment model to evaluate cyber risks to aviation security. Additionally, the section directs TSA to seek enhanced sector participation in cybersecurity mitigation efforts and directs the Secretary, upon request, to conduct a cybersecurity vulnerability assessment for airports and air carriers. As amended, the provision also ensures clarity that requirements under this section pertain exclusively to aviation security. Additionally, the amended provision requires a cybersecurity vulnerability assessment of the data transmitted and held for the Department's trusted traveler and security credentialed populations, such as TSA PreCheck and the TWIC program.

Through its oversight, the Committee has come to appreciate the vital role that relationships among airport operators, aviation

stakeholders, and local TSA personnel play in the overall effectiveness of aviation security operations and coordination. The Committee believes TSA and its Federal Security Directors should take all necessary steps to regularly engage with stakeholders on the ground and maintain productive working relationship. Additionally, TSA should remain a clearinghouse of aviation security best practices and establish effective strategies, policies, and procedures for information sharing. Further, the Committee believes that the cybersecurity landscape continues to shift and that the aviation community remains a point of vulnerability. Because of this, the Committee believes that the Secretary, in consultation with relevant partners, should develop an aviation security risk assessment model to identify risks to cybersecurity in the aviation environment. The Committee believes that cybersecurity mitigation efforts should be voluntary on the part of industry stakeholders and that risk assessments should only be conducted upon request from the stakeholder.

The Committee also believes that the Department must work to ensure that potential vulnerabilities in the security of personally identifiable information held in its various trusted traveler or vetting programs are identified and mitigation strategies implemented. The Committee notes that the President's budget request for Fiscal Year 2018 estimates a growth in PreCheck participation. The Committee believes that ensuring the American flying public that their most sensitive data, including their biometrics, is secure will foster more confidence within the population that TSA needs to attract to the PreCheck program.

SUBTITLE G-SURFACE TRANSPORTATION SECURITY

Sec. 571. Definitions.

This section defines terms used in this Subtitle.

Sec. 572. Surface transportation security assessment and implementation of risk-based strategy.

This section requires the Administrator of the Transportation Security Administration to conduct a vulnerability and risk assessment for surface transportation using current threat intelligence. This section further requires the Administrator to develop and implement a multi-modal, risk-based strategic plan to mitigate threats identified in the risk assessment, and coordinate with other stakeholders in the implementation of the plan. This section further requires the Administrator to report to Congress on the security assessment and the implementation of the risk-based plan, and to provide regular updates for both.

The Committee believes that surface transportation modes are of particular concern given the ongoing rise in terrorist attacks overseas against surface transportation hubs and other soft targets of transportation modes. The porous nature of surface transportation makes the sector difficult to secure, and the Committee feels there needs to be an updated security assessment and risk-based strategy for securing surface transportation modes.

Sec. 573. Risk-based budgeting and resource allocation.

This section requires that the TSA budget submissions clearly indicate which resources will be used for surface transportation security and which will be dedicated to aviation. This section further requires TSA to notify Congress if agency resources, including staff, were used for purposes not related to transportation security. In prior years, the Committee has been concerned that TSA has failed to clearly and coherently articulate surface transportation budget priorities, deployments, and allocations. In response to this, the Committee believes this provision will ensure that TSA and DHS provide more useful information to Congress related to surface transportation security efforts.

Sec. 574. Surface transportation security management and interagency coordination review.

This section requires a GAO review of TSA's surface transportation program management structure, including the allocation of staff to different modes of transportation, and how the programs are developed, managed and implemented. As part of the above review, GAO will examine how TSA can improve coordination between other Federal, State, local, or industry stakeholders to reduce redundancy and regulatory burden. Given the overlapping nature of many surface transportation security entities, the Committee believes a GAO review to be both prudent and necessary in assessing the overall State of interagency coordination in protecting the Nation's vital surface transportation systems.

Sec. 575. Transparency.

This section requires TSA to regularly update a public website on the status of surface transportation rulemakings. This section further requires the Department of Homeland Security Inspector General (DHS IG) to review the required regulations to see if they are still necessary or relevant. The Committee has become concerned by stakeholder perspectives that rulemaking processes are often opaque and lack input from relevant stakeholders. Additionally, in some instances, previously required but unimplemented regulations may no longer be practicable or relevant to the current threat landscape. This provision will provide for greater transparency in the rulemaking process and give needed information on the relevancy or need of regulatory requirements.

Sec. 576. TSA counterterrorism asset deployment.

This section requires, except during times of urgent need, the Administrator to provide a 2-week notification to any affected stakeholder before terminating any TSA resource that was provided for 6 months or more. Additionally, the provision requires the development of performance measures and objectives for TSA's Visual Intermodal Prevention and Response (VIPR) teams, as well as risk-based deployment metrics. As amended, this provision authorizes up to 30 VIPR teams for the Administrator to use in support of counterterrorism efforts at surface and aviation transportation hubs, while requiring congressional notification if the number of teams drops below 30. Moreover, the amended provision requires a report to Congress, after the development of the performance meas-

ures and objectives, on the identified number of teams needed by the Administrator.

The Committee recognizes that TSA VIPR teams serve as a TSA counterterrorism tool in deterring and responding to terrorist attacks. However, the Committee also has longstanding concerns as to the lack of proven security effectiveness of VIPR teams, and believes it necessary for TSA to develop performance measures and objectives in order to assess the value of the teams and ensure that VIPR teams are deployed in a risk-based manner that maximizes security effectiveness. Due to the heightened threat landscape facing soft terror targets at transportation hubs, the Committee believes that it is critical that limited resources are directed effectively, while maintaining flexibility for the Secretary and the Administrator to deploy the resources of the Federal Air Marshal Service to respond to changing threats, and potential increased aviation mission needs.

Sec. 577. Surface transportation security advisory committee.

This section requires the Administrator to establish a Surface Transportation Security Advisory Committee to provide stakeholders and the public the opportunity to coordinate with the agency and comment on policy and pending regulations.

The Committee has seen a significant positive impact in establishing the Aviation Security Advisory Committee for TSA to receive valuable input from stakeholders across the aviation sector. In establishing a similar entity for the surface environment, the Committee hopes to create critical lines of communication on security-related issues among surface transportation modes and the Administrator. The Committee recognizes that the surface transportation sector is multi-modal and different from the aviation sector but like the aviation sector, has government and sector coordinating councils to foster collaboration. The Committee also believes that the advisory committee established by this provision can serve a valuable role in raising awareness within TSA of surface transportation security issues, challenges, and can be a critical help to the Administrator in determining policies and strategies aimed at protecting surface transportation systems. The Committee in no way intends to direct policymaking authority away from the Administrator or other relevant government entities for the surface transportation sector, but desires to implement a model similar to that of the Aviation Security Advisory Committee.

Sec. 578. Review of the explosives detection canine team program.

This section requires the DHS IG to conduct a review of the National Explosives Detection Canine Team Program to determine examine how TSA is administering the program and how they are using the canine teams to mitigate risks.

Explosives detection canines play a critical role in protecting transportation assets from security threats. The Committee believes that the National Explosives Detection Canine Team Program requires prudent review in order to maximize the security effectiveness of and proliferate the overall use of explosives detection canines within transportation security modes.

Sec. 579. Expansion of national explosives detection canine team program.

This section allows for the immediate expansion of 70 additional canine teams upon passage of the legislation. It directs TSA to consider the DHS Inspector General's recommendations before adding any further additional teams. The Committee believes that this program requires additional resources in order to expand the use of explosives detection canines across transportation sectors and modes. Further, the evolving and stark threat landscape requires emphasis on proven, effective security resources and counterterrorism assets like explosives detection canines. The Committee believes that TSA should expand this program by 70 additional teams, while taking the recommendations of the DHS Inspector General related to this program into account before adding further additional teams.

Sec. 580. Explosive detection technology.

This section requires the Secretary to research and develop next generation technologies to detect explosives in transportation systems and transportation facilities. The Committee has seen worrying changes in the overall threat landscape and believes that the Secretary of Homeland Security should concentrate on advancing and prioritizing the next generation of explosives detection for transportation systems.

Sec. 581. Study on security standards and best practices for United States and foreign passenger transportation systems.

This section requires the GAO of the United States to conduct a study of how TSA identifies international security best practices and disseminates that information to stakeholders. The Committee believes that TSA plays an important role in identifying and sharing international best practices related to transportation security but that improvements can be made in both policies and procedures. This provision will ensure that such improvements are identified by the required GAO study and provide TSA and Congress with recommendations for enhancing security.

Sec. 582. Amtrak security upgrades.

This section allows Amtrak to use security grant funding to improve passenger manifest systems to ensure that passengers can be identified. The Committee recognizes the important role that surface stakeholder data can play in preparing for and responding to potential threats, and believes that additional flexibility in how Amtrak uses its allotted grant funding can assist in protecting rail passengers and the passenger rail system from security threats.

Sec. 583. Study on surface transportation inspectors.

This section requires GAO to submit a report to Congress that reviews the effectiveness of surface transportation security inspectors, including hiring practices and training standards. The report will also determine the extent to which the Transportation Security Administration has used a risk-based, strategic approach to determine the appropriate number of surface transportation security in-

spectors and if the Transportation Security Administration's surface transportation inspection policies are risk-based.

Through its oversight activities, the Committee has determined a need to review TSA's Surface Transportation Inspectors program, due to a lack of clarity on the distinct roles, skills, and mission of surface inspectors. While the program makes up a small part of TSA's larger efforts to secure surface and aviation transportation system, the Committee would like additional information related to the overall security contribution, effectiveness, and performance measures of surface inspectors.

Sec. 584. Security awareness program.

This section requires the Administrator of the Transportation Security Administration to establish a program to enhance the security of surface transportation by training the surface transportation operators and frontline employees. As amended, this program is clarified as not serving in fulfillment of other statutorily required regulatory responsibilities.

Due to the reality of the challenges in protecting surface transportation from threats to security, the Committee recognizes a need for TSA to develop a security awareness program for use by frontline surface transportation employees and surface mode operators to better recognize, understand, and respond to security threats.

Sec. 585. Voluntary use of credentialing.

This section authorizes the voluntary use of TWIC for security at transportation facilities other than ports. The Committee recognizes the security and efficiency value of permitting individuals requiring background investigations to satisfy such requirements by voluntarily obtaining a TWIC card. Such requirements would be due to a need for a hazardous material endorsement on a commercial driver's license or because their employment is regulated by the Transportation Security Administration, Coast Guard, or Department of Transportation or as required by the Homeland Security Act of 2002.

Sec. 586. Background records checks for issuance of hazmat licenses.

This section ensures that individuals who have undergone a security threat assessment for a TWIC do not have to pay a duplicative assessment to be run for a hazardous materials endorsement. The Committee recognizes a need to clarify sometimes conflicting and duplicative background investigation requirements for drivers seeking to obtain credentials regulated by the Department of Homeland Security or the Transportation Security Administration. The Committee believes this provision increases efficiency and eliminates unnecessary burden on certain stakeholders and drivers requiring security credentials without compromising security requirements or standards.

Sec. 587. Recurrent vetting for surface transportation credentialholders.

This section amends Section 70105 of title 46, United States Code, to require the Secretary of the Department of Homeland Security to develop and implement a plan to utilize the FBI's Rap

Back Service in order to establish recurrent vetting capabilities for individuals holding valid transportation security cards. The Committee recognizes the value of the FBI's Rap Back program for the purposes of providing perpetual vetting capabilities for certain credentialed populations requiring an FBI criminal history records check. The Committee believes that enabling TWIC card holders to be enrolled in this program will both enhance security and eliminate the need for biannual investigation requirements.

Sec. 588. Pipeline security study.

This section requires the Comptroller General of the United States within 180 days of enactment to conduct a study to determine the respective roles of the Department of Homeland Security and the Department of Transportation in pipeline security. Additionally, not later than 90 days after the submission of the aforementioned report, the Secretary shall submit any recommendations for changes to the Annex to the Memorandum of Understanding executed on August 9, 2006, between the Department of Homeland Security and the Department of Transportation or improvements to pipeline security. The Committee recognizes pipelines as a critical transportation system. Pipelines serve as a vital security concern and the Committee believes a security study conducted by the GAO to be necessary to clarify roles and responsibilities.

Sec. 589. Repeal of limitation relating to motor carrier security-sensitive material tracking technology.

This section repeals a requirement for Congress to grant additional approval for TSA to implement requirements on motor carrier sensitive security tracking technologies. The Committee believes that the statutory requirement for Congress to grant additional approval of an otherwise standard rulemaking authority for motor carrier security-sensitive material tracking technology to be duplicative and unnecessary. Therefore, the Committee seeks to update the existing code by repealing this requirement. However, the Committee in no way intends for this provision to be interpreted as direction by Congress for the Secretary to engage in a rulemaking on this matter. Additionally, the Committee expects that, as in all rulemaking efforts, any regulatory process on this matter includes sufficient input from stakeholder and industry perspectives prior to any finalization or implementation of a regulation.

SUBTITLE H-SECURITY ENHANCEMENTS IN PUBLIC AREAS OF TRANSPORTATION FACILITIES

Sec. 591. Working group.

This section allows the Secretary of Homeland Security to establish a working group to promote collaborative engagement between the Department and public and private sector stakeholders to develop recommendations for enhancing public area security at transportation facilities. If such a working group is established, the Secretary shall report on the organization, participation, activities, findings, and non-binding recommendations for the immediately preceding 12-month period. The Federal Advisory Committee Act does not apply to this working group or any subsidiary thereof. The

Committee believes that recent efforts by the Department and TSA to promote security collaboration and awareness in response to increased threats to public areas of airports and other transportation hubs are an important part of responding to changing threats. The Committee hopes that this provision will ensure the continued efforts to prepare for and respond to threats targeting public areas of transportation facilities.

Sec. 592. Technical assistance; Vulnerability assessment tools.

This section directs the Secretary of Homeland Security to inform stakeholders of the availability of Departmental technical assistance, including vulnerability assessments, to help enhance public area security at transportation facilities and provide assistance upon request, subject to appropriations. Moreover, this section directs the Secretary to publish and disseminate best practices for protecting and enhancing the resiliency of public areas of transportation facilities. The Committee believes the Department of Homeland Security plays an important role in raising the overall State of security readiness and awareness at transportation hubs across the country. Additionally, the Department should be working to raise the level of resiliency of transportation systems.

Sec. 593. Operations centers.

This section requires the Administrator, within 120 days of enactment, to make available to stakeholders a framework for establishing an operations center within a transportation facility to promote interagency response and coordination.

Sec. 594. Review of regulations.

This section requires that not later than 1 year after enactment, the Administrator of TSA shall submit a report to Congress reviewing regulations, directives, policies, and procedures issued by the Administrator regarding the transportation of a firearm and ammunition by an aircraft passenger, and, as appropriate, plans to modify any such regulation, directive, policy, or procedure based on such review. In preparing the report, the Administrator shall consult with stakeholders through the Aviation Security Advisory Committee. The Committee believes that TSA should endeavor on such a review, in order to ensure consistency, clarity, and efficiency.

Sec. 595. Definition.

This section defines the term "public and private sector stakeholders" as the meaning given such term in section 114(u)(1)(C) of title 49, United States Code, which the Committee believes fully encompasses the intent of the overall provision.

TITLE VI-EMERGENCY PREPAREDNESS, RESPONSE, AND COMMUNICATIONS

SUBTITLE A-GRANTS, TRAINING, EXERCISES, AND COORDINATION

Sec. 601. Urban Area Security Initiative.

This section amends section 2003 of the Homeland Security Act of 2002 by requiring States to provide a detailed accounting of items, services, or activities purchased utilizing funds retained from the Urban Area Security Initiative to relevant high-risk urban areas within 90 days of retention. The intent of this language is to ensure transparency and the avoidance of unnecessary duplication of effort between States and eligible high-risk urban areas. This section also requires Urban Area Security Initiative awardees to submit a Threat and Hazard Identification and Risk Assessment to the Administrator, consistent with current practice.

This section codifies the period of performance for funding awarded under the Urban Area Security Initiative at 36 months. The Committee shared the concern of grant recipients that the previous period of performance, 24 months, did not provide a sufficient amount of time for grantees to complete projects, particularly at the subgrantee level. The Committee supports FEMA's decision to revert to a 36-month period of performance for grant programs in this Title and encourages the continued enforcement of that deadline.

In addition, this section authorizes the appropriation of $800 million for each of the fiscal years from 2018 through 2022 for the Urban Area Security Initiative, which is $195 million above the current appropriated level and $350 million above the President's Fiscal Year 2018 budget request.

Sec. 602. State Homeland Security Grant Program.

This section amends section 2004 of the Homeland Security Act of 2002 by requiring States participating in the State Homeland Security Grant Program to submit a Threat and Hazard Identification and Risk Assessment to the Administrator, consistent with current practice. States are required to include input on their assessments from local and tribal governments, including first responders. First responders are defined in this section as representatives from local governmental and nongovernmental fire, law enforcement, emergency management, and emergency medical personnel. This section also codifies the period of performance for the State Homeland Security Grant Program at 36 months. Finally, this section authorizes $600 million each Fiscal Year 2018 through 2022 for the State Homeland Security Grant Program, which is $133 million above the current appropriated level and $250 million above the President's Fiscal Year 2018 budget request. The Committee has held numerous hearings, briefings, and meetings with stakeholders in the first responder community regarding the consistent need for homeland security investments provided through this program.

Sec. 603. Grants to directly eligible tribes.

This section codifies the period of performance for grant awards to directly eligible tribes at 36 months.

Sec. 604. Law enforcement terrorism prevention.

This section seeks to ensure that the 25 percent set aside for law enforcement terrorism prevention activities required under the State Homeland Security Grant Program and Urban Area Security Initiative is met by requiring the Assistant Secretary for State and Local Law Enforcement to work with the FEMA Administrator to certify and report annually to Congress that the grants are appropriately focused on law enforcement terrorism prevention activities. This section also requires the Assistant Secretary for State and Local Law Enforcement to coordinate with State, local, and tribal law enforcement partners on Department policies and programs that may impact such partners.

Sec. 605. Prioritization.

This section clarifies the population data that must be considered as part of the risk formula, including international tourists and military personnel living outside military installations.

This section further requires the Administrator and Government Accountability Office to each review the risk formula and methodology used to determine awards for the Urban Area Security Initiative and the State Homeland Security Grant Program. Additionally, the Administrator is required to report the results of this review within 90 days of enactment of this Act to 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.

A number of stakeholders have expressed concern with the transparency of the risk formula utilized by FEMA to make grant awards. FEMA should, to the extent practicable, share as much data as possible with grant recipients to ensure confidence in the grant aware process.

Sec. 606. Allowable uses.

This section authorizes State Homeland Security Grant Program and Urban Area Security Initiative funds to be used to (1) enhance medical preparedness, and (2) enhance cybersecurity. This section consolidates two allowable use bills, both of which passed the House earlier this year.

The section also requires communications expenditures to align with the Statewide Communication Interoperability Plan and be coordinated with the Statewide Interoperability Coordinator or Statewide interoperability governance body of the State, consistent with current grant guidance.

Sec. 607. Approval of certain equipment.

This section amends subsection (f) of section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609) by adding at the end a review process for applications seeking to purchase equipment or systems that do not meet or exceed applicable national voluntary consensus standards using funds from the Urban Area Security Initia-

tive or the State Homeland Security Grant Program. The Administrator is required to implement a uniform process for reviewing such applications against the following criteria:

- current or past use of proposed equipment or systems by Federal agencies or the Armed Forces;
- the absence of a national voluntary consensus standard for such equipment or systems;
- the existence of an international consensus standard for such equipment or systems, and whether such equipment or systems meets such standard;
- the nature of the capability gap identified by the applicant and how such equipment or systems will address such gap;
- the degree to which such equipment or systems will serve the needs of the applicant better than that which meets or exceeds existing consensus standards; and
- any other factor determined appropriate by the Administrator.

This section also requires the Inspector General to report to Congress, no later than 3 years after enactment of this Act, on the implementation of the review process established under this Act that includes the number of requests to purchase equipment or systems that do not meet or exceed any applicable consensus standard evaluated under such review process; the number of such requests granted and denied; and how long it takes to review such requests. This section is identical to H.R. 687, which passed the House by voice vote on January 31, 2017.

Sec. 608. Memoranda of understanding.

This section requires the Administrator of the Federal Emergency Management Agency (FEMA) to enter into memoranda of understanding with subject matter experts from other Department of Homeland Security (DHS) components and offices to ensure subject matter experts are involved in policy guidance decisions relating to the State Homeland Security Grant Program, Urban Area Security Initiative, Port Security Grant Program, and Transit Security Grant Program.

Sec. 609. Grants metrics.

This section requires FEMA to use information provided by States and high-risk urban areas in their Threat and Hazard Identification and Risk Assessments and State Preparedness Reports to determine the extent to which State Homeland Security Grant Program and Urban Area Security Initiative funds have been used effectively to close capability gaps. FEMA is also required to submit an assessment of the data 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 of the Senate.

Sec. 610. Grant management best practices.

This section requires FEMA to share information on methods to address areas identified for improvement in grant audits conducted by the Department's Office of Inspector General and innovative projects and practices with recipients of State Homeland Security

Grant Program and Urban Area Security Initiative funds as part of yearly grant guidance.

The Committee believes that grant recipients can greatly benefit from sharing information on management best practices, corrective actions, and other innovative practices. They could also benefit from access to information on projects conducted by other jurisdictions. The Committee has received testimony from first responders advocating for the development of a searchable data base of grant projects funded through the State Homeland Security Grant Program and Urban Area Security Initiative through which grantees can reference while developing their own projects. The Committee supports FEMA's efforts to collect more project level data in grant applications, but acknowledges that such a data base may not be within FEMA's capabilities as this time. However, as FEMA gains greater insight into individual projects, there may be merit in the development of a mechanism for grant applicants to learn about successful projects in another jurisdiction.

Sec. 611. Prohibition on consolidation.

This section prohibits the Secretary of Homeland Security from implementing the National Preparedness Grant Program or any successor program to consolidate grant programs unless the Secretary receives prior authorization from Congress.

Sec. 612. Maintenance of grant investments.

This section requires grant applicants to develop a plan for the maintenance of equipment purchased using State Homeland Security Grant Program or Urban Area Security Initiative funds.

Sec. 613. Transit security grant program.

The Committee believes it is important to invest consistent resources to secure passenger surface transportation. Surface transportation modes serve over 28 million riders daily and over 10 billion riders annually. As a result, this mode of transportation continues to remain a terror target. For this reason the Committee authorizes $200 million for the Transit Security Grant Program for each Fiscal Year from 2018 to 2022, which is a 100 percent increase over the current appropriated level and $152 million above the President's Fiscal Year 2018 budget request. This section amends section 1406 of the Implementing Recommendations of the 9/11 Commission Act of 2007 to permit grant recipients to use funding to pay for backfill associated with sending personnel to security training. Further, this section codifies the period of performance for grants awarded under the Transit Security Grant Program at 36 months, with the exception of large-scale capital security projects.

During the 114th Congress, the Committee conducted a field hearing in Jersey City, New Jersey that addressed the critical security challenges facing surface transportation. Members heard at the field hearing that the current period of performance of 36 months is insufficient for transit agencies to complete large scale capital projects to harden their systems. This section addresses this issue by setting the period of performance for large scale capital projects at 55 months. This section is similar to H.R. 549, which passed the House by voice vote on January 31, 2017.

Sec. 614. Port security grant program.

This section codifies the period of performance for the grants awarded under the Port Security Grant Program at 36 months. The Committee recognizes the importance of this program to the security of our Nation's ports and, as such, this section authorizes $200 million from Fiscal Year 2018 through 2022 for the Port Security Grant Program, which a 100 percent increase over the current appropriated level and $152 million above the President's Fiscal Year 2018 budget request.

Sec. 615. National Domestic Preparedness Consortium.

This section reauthorizes the National Domestic Preparedness Consortium, which was originally authorized in the Implementing Recommendations of the 9/11 Commission Act of 2007. Additionally, the section requires the National Domestic Preparedness Consortium to provide training exercises simulating real response environments, such as urban areas, for State, local, and tribal emergency response providers. The section authorizes $63,939,000 for the Center for Domestic Preparedness for fiscal years 2018 and 2019 and the $101 million for the remaining members of the National Domestic Preparedness Consortium for fiscal years 2018 and 2019, amounts equal to the current appropriated levels.

The Committee believes the National Domestic Preparedness Consortium remains an invaluable resource to first responders, and therefore the entire DHS enterprise. More than 2.6 million first responders and emergency managers have received vital training through the consortium.

Sec. 616. Rural Domestic Preparedness Consortium.

This section authorizes the Rural Domestic Preparedness Consortium, which provides training to emergency response providers from rural communities. This section authorizes $5 million out of the amount appropriated for the Continuing Training Grants to be used for the Rural Domestic Preparedness Consortium.

Sec. 617. Emergency support functions.

This section requires the Administrator to periodically update the National Response Framework. Additionally, based on findings from a recent Government Accountability Office (GAO) report, this section requires the President, through the Administrator, to develop and provide to relevant Federal agencies and departments, metrics to ensure readiness to execute responsibilities under the National Response Framework's Emergency Support Functions.

Sec. 618. Review of National Incident Management System.

The Committee believes that as threats to the homeland evolve, we must maintain our ability to efficiently adapt to the threats. This section amends the Homeland Security Act of 2002 by requiring the National Incident Management System to be updated not less than once every 5 years. During this process, FEMA should work with critical partners in the first responder community, including law enforcement, to ensure their input and expertise is appropriately incorporated to meet capabilities in the field.

Sec. 619. Remedial action management program.

The section requires the Administrator to utilize the Remedial Action Management Program, authorized in the Post Katrina Emergency Management Reform Act of 2006, for the purpose of coordinating corrective actions identified as a result of exercises and the response to acts of terrorism and both man-made and natural disasters. The section also requires the FEMA Administrator to electronically share after-action reports and information on lessons learned and best practices from responses to acts of terrorism, natural disasters, and other exercises or emergencies with Congress and relevant Federal, State, local, tribal, and private sector officials. Recent GAO work has identified the need for Federal departments and agencies to coordinate efforts to close capability gaps identified in Federal response after-action reports.

Sec. 620. Cyber preparedness.

This section seeks to ensure information related to cyber risks and threats is shared with fusion centers. This section includes, as a function of the National Cybersecurity and Communications Integration Center (NCCIC), sharing information about cyber best practices, in addition to the sharing of cyber threat indicators and defensive measures currently required by law. The section also authorizes representatives from fusion centers to be assigned to the NCCIC, similar to the assignment of representatives from information sharing and analysis centers (ISACs) permitted under current law. Further this section expresses the sense of Congress that the Department of Homeland Security should, to the greatest extent practicable, work to establish tear lines so actionable intelligence related to cyber threats may be shared with those without clearances. This section is similar to H.R. 584, which passed the House by voice vote on January 31, 2017.

The Committee has heard that, while improving, the flow of Federal cyber threat and risk information to State and local emergency response providers is slow and over–classified. Additionally, for several years now, FEMA has released an annual National Preparedness Report, which highlights the States' 32 core capabilities, as defined by the National Preparedness Goal. Since the first National Preparedness Report was released in 2012, States have ranked their cybersecurity capabilities as one of their lowest.

The current process of sharing information has caused emergency response providers to be reactive rather than proactive in addressing the current cyber threats. To date, there are 79 fusion centers across the Nation with the primary mission to serve as the conduit between the Federal Government and States and localities for the sharing of intelligence and homeland security information. Most fusion centers have developed dissemination channels that can be used to ensure cyber threat and risk information is getting to the appropriate emergency response providers. Additionally, the Committee supports the ability of States and urban areas to use SHSGP and UASI funds for cyber preparedness. This section will ensure that SHSGP and UASI funds remain available for cyber preparedness. The Department should work to establish tear lines to ensure valuable cyber threat information is disseminated to all appropriate stakeholders.

Sec. 621. Major metropolitan area counterterrorism training and exercise grant program.

This section establishes the Major Metropolitan Area Counterterrorism Training and Exercise Grant Program. Specifically, the section authorizes $39 million in annual grants from fiscal years 2018 through 2022 for emergency response providers to enable them to prevent, prepare for, and respond to emerging terrorist attack scenarios, including complex, coordinated terrorist attacks and active shooters, against major metropolitan areas. Eligible applicants for this program include emergency response providers in jurisdictions that are currently receiving, or that previously received, Urban Area Security Initiative funding. Recipients of this program may use the above described funding for identifying capability gaps, developing and updating plans, as well as conducting training and exercises associated with complex, coordinated terrorist attacks. FEMA should ensure that funding authorized under this section is not utilized for purely administrative purposes. Additionally, FEMA is required to collect, analyze, and disseminate information for first responders on lessons learned and best practices from activities conducted using these grant funds. This section is similar to H.R. 2188, which passed the Committee earlier this year.

Sec. 622. Center for Domestic Preparedness.

This section requires FEMA to develop an implementation plan and submit to Congress information on efforts to implement recommendations from the Management Review of the Chemical, Ordinance, Biological, and Radiological Training Facility at the Center for Domestic Preparedness. Additionally, the Government Accountability Office is required to review and report to Congress on FEMA's progress implementing the recommendations.

Last year, the Committee learned that the Center for Domestic Preparedness was unknowingly using ricin holotoxin, rather than an inactive form of ricin, in first responder training at the Chemical, Ordinance, Biological, and Radiological Training Facility. FEMA conducted a review of the training facility and issued management recommendations to prevent another incident like this from happening.

Sec. 623. Operation Stonegarden.

This section establishes Operation Stonegarden, a Department of Homeland Security grant program for law enforcement agencies to help improve border security. The section authorizes Operation Stonegarden at $110,000,000 for each Fiscal Year from 2018 to 2022.

Sec. 624. Non-Profit Security Grant Program.

This section establishes the Non-Profit Security Grant Program within the Department of Homeland Security, which awards grants to eligible non-profit organizations for hardening activities including physical security enhancements and inspection systems to protect against terrorist attacks. The section authorizes the Non-Profit Security Grant Program at $50,000,000 for each Fiscal Year from 2018 through 2022.

The Committee authorizes the Non-Profit Security Grant Program for the first time, recognizing the impact of this program on

the security of non-profit organizations at risk of terrorist attacks, many of which have seen an increase in threats this year. In authorizing the program, the Committee intends the Federal Emergency Management Agency to maintain the current program guidelines, risk-based scoring, and review process.

In recognition of this increase in threats, the Committee expands eligibility to non-profit organizations located outside of Urban Area Security Initiative (UASI) jurisdictions. The section divides the funding authorization between the two types of eligible applicants with $35 million authorized for organizations in UASI jurisdictions and $15 million for organizations outside UASI jurisdictions. This program has traditionally been funded as a carve out of funding appropriated for UASI. In expanding eligibility, the Committee does not intend for organizations outside of UASI jurisdictions to be funded from the UASI account.

Sec. 625. FEMA Senior Law Enforcement Advisor.

This section codifies the position, qualifications, and responsibilities of the Senior Law Enforcement Advisor to the Administrator of FEMA. The Senior Law Enforcement Advisor is responsible for coordinating with State, local, and tribal law enforcement officials to help prevent, protect, and respond to natural disasters, terrorist attacks, or other manmade disasters.

Law enforcement stakeholders have discussed the value of the Senior Law Enforcement Advisor in their efforts to communicate effectively with FEMA. This section codifies that provision to ensure their voices are heard in the development of policies and programs.

Sec. 626. Study of the use of grant funds for cybersecurity.

This section requires the Administrator of FEMA, in consultation with relevant Department of Homeland Security components, to report to Congress on how State Homeland Security Grant Program and Urban Area Security Initiative grant funds are used to prepare for and respond to cybersecurity incidents. Every year it has been published, the National Preparedness Report indicates that States rank cybersecurity as the core capability in which they have the least confidence. At the same time, Urban Area Security Initiative and State Homeland Security Grant Program grantees generally do not invest significant portions of their awards in addressing cybersecurity gaps. In light of the evolving cybersecurity threats, it is critical to understand why grantees are not using grant funds to address this pressing national security issue. The Committee urges FEMA to use the findings of its report to better tailor grant guidance to help grantees identify investments that will bolster cybersecurity capabilities.

Sec. 627. Technical expert authorized.

This section codifies the Children's Technical Expert at the Federal Emergency Management Agency. The provision is identical to a provision in H.R. 1372, which passed the House by voice vote on April 25, 2017.

In 2009, FEMA appointed Children's Needs Coordinator and established a Children's Working Group to address the unique needs of children during a disaster. Administrator Fugate eliminated the

position in 2012, but restored it in 2015 pursuant to a recommendation made by the FEMA National Advisory Council (NAC). According to the NAC, significant gaps remain related to integrating children into disaster planning. Former Administrator Fugate acknowledged as much when he testified that incorporating the needs of children into disaster policy and planning is "not something that's in the DNA yet." At present, FEMA has a technical expert that focuses on the needs of children in disasters, but the position is not formally authorized. By formally authorizing the Children's Technical Expert, the Committee is making clear that integrating children in emergency planning, policies, and activities should be a priority at FEMA.

SUBTITLE B-COMMUNICATIONS

Sec. 631. Office of Emergency Communications.

This section restricts the Secretary of Homeland Security's ability to change the location or reporting structure of the Office of Emergency Communications (OEC) without prior authorization from the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs.

First responder organizations, one of OEC's primary constituents, have expressed concern with the Department of Homeland Security's plans to move OEC as part of its reorganization of the National Protection and Programs Directorate (NPPD). The Committee is currently working with the Department and stakeholders on legislation authorizing NPPD and its structure, which will include OEC. Until such time as that legislation is enacted, the Committee expects OEC to remain in its current location.

Sec. 632. Responsibilities of Office of Emergency Communications Director.

This section makes technical corrections to the responsibilities of the Director of the Office of Emergency Communications and codifies additional responsibilities.

Sec. 633. Annual reporting on activities of the Office of Emergency Communications.

This section requires the Director of the Office of Emergency Communications to submit an annual report, for the next 5 years, to the Committee on Homeland Security and the Committee on Energy and Commerce of the House and the Committee on Homeland Security and Governmental Affairs of the Senate on the activities and programs of the Office of Emergency Communications. The reports must include specific information on the Office's efforts to: promote communication among emergency response providers during disasters; conduct nationwide outreach to foster the development of interoperable emergency communications capabilities; and provide interoperable emergency communications technical assistance to State, regional, local, and tribal government officials.

Sec. 634. National Emergency Communications Plan.

This section requires the Office of Emergency Communications to update the National Emergency Communications Plan at least once every 5 years and consider the impact of emerging technologies on

the attainment of interoperable communications as part of that update.

Sec. 635. Technical edit.

This section makes technical corrections to the Emergency Communications Title of the Homeland Security Act of 2002.

Sec. 636. Public Safety Broadband Network.

This section requires the Under Secretary of the Department of Homeland Security's National Protection and Programs Directorate to submit information to the House Committee on Homeland Security, the House Committee on Energy and Commerce, and the Senate Committee on Homeland Security and Governmental Affairs on the Department of Homeland Security's responsibilities related to the development of the nationwide Public Safety Broadband Network. This includes information on efforts by the Department to work with the First Responder Network Authority to identify and address cyber risks that could impact the near or long term availability and operations of the network and recommendations to mitigate such risks.

Sec. 637. Communications training.

Based on the findings of a GAO report, this section requires the Under Secretary for Management, in coordination with appropriate component heads, to develop a mechanism to verify that radio users at the Department of Homeland Security receive relevant radio training.

SUBTITLE C-MEDICAL PREPAREDNESS

Sec. 641. Chief Medical Officer.

This section codifies the current responsibilities of the Department's Chief Medical Officer, including coordinating the Department's policy, strategy, and preparedness for pandemic influenza and emerging infectious diseases; ensuring the Department work force has standards, policies, and metrics for occupational safety and health; and providing medical liaisons to the Department's components.

Sec. 642. Medical Countermeasures Program.

This section authorizes the Department of Homeland Security's medical countermeasures program to protect the DHS work force, working animals, and individuals in the Department's care and custody from the effects of chemical, biological, radiological, and nuclear agents, and to ensure mission continuity. The section also addresses findings from a September 2014 DHS Inspector General review of the medical countermeasures program. Additionally, this section requires the Chief Medical Officer to establish a medical countermeasures working group comprised of representatives from relevant Department components and offices. The working group is responsible for ensuring medical countermeasures standards are maintained and guidance is consistent. Further, the Chief Medical Officer must report to the House Committee on Homeland Security and the Senate Committee on Homeland Security and Govern-

mental Affairs, within 180 days of enactment of this Act, on efforts made to achieve the requirements of this section.

The Committee is concerned with findings from an August 2014 DHS Inspector General review of the Department's medical countermeasure program, DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures (OIG–14–129). As a result, the section addresses the Inspector General recommendations related to medical countermeasure quantity determination; stockpile replenishment; inventory tracking; and cross-component standards for storage, security, dispensing and documentation.

SUBTITLE D-MANAGEMENT

Sec. 651. Mission support.

This section requires the Administrator of FEMA to designate an individual to serve as the chief management official and principal advisor to the FEMA Administrator on matters related to the management of FEMA.

The Committee is supportive of FEMA's efforts to strengthen and improve its management through the Mission Support Bureau and authorizes the designation of a chief management official and principal advisor to the FEMA Administrator on issues related to the five management business lines: human resources, procurement, information technology, real property, and security. The Committee believes the role of a chief management official is essential to the efficient functioning of the agency. The Committee believes FEMA must develop and implement management controls to ensure appropriate oversight of Agency management functions. The Committee continues to remain concerned about previous findings from the DHS Office of Inspector General and the Government Accountability Office. Findings identified trends with program offices responsible for the acquisition of systems that support FEMA's mission which did not follow appropriate acquisition policies. As a result, these million dollar acquisitions were subject to dysfunction, life cycle cost increases, and limited oversight.

The Committee intends for the review of the five management business lines to identify management controls, costs, number of associated systems, associated capability gaps, and areas of duplication both at FEMA headquarters and the ten regional offices. Further, this review must include a strategy that demonstrates how the designated management official captures reliable, interoperable, and measurable data on all management and administrative activities. The strategy should address any problems identified in the review.

Sec. 652. Systems modernization.

This section requires the Administrator of FEMA to report to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House and the Committee on Homeland Security and Governmental Affairs of the Senate on plans to modernize its grants and financial information technology systems within 180 days of enactment of this Act. The report should include lessons learned in the summary of all previous efforts to modernize each of these systems. This report should iden-

tify how each of these modernization efforts are meeting cost schedule expectations and the efforts being made to avoid delays in the acquisition life cycle.

Sec. 653. Strategic human capital plan.

This section reinStates a requirement in the Post Katrina Emergency Management Reform Act of 2006 requiring the Administrator of FEMA to develop and submit to Congress a strategic human capital plan. This plan must include a work force gap analysis, recruitment and retention analysis, performance metrics, and staffing goals.

According to a July 2015 GAO report, FEMA's Workforce Management (GAO–15–437), FEMA's strategic work force plan for 2008–2012 did not include performance metrics or identify potential work force gaps, overlaps, or inconsistencies. Additionally, the National Academy for Public Administration recommended that FEMA develop a 5-year strategic work force plan that addresses retention challenges by implementing goals and objectives for recruiting and retaining employees. In 2016, FEMA ranked 284 out of 355 for best place to work in the Federal Government according to the Partnership for Public Service. To address these shortcomings, the Committee continues the requirement that FEMA develop and implement a strategic human capital plan. The Committee commends FEMA's efforts to address these longstanding challenges by publishing the Human Capital Strategic Plan for Fiscal Years 2016–2020. The Committee will continue to follow FEMA's progress in aggressively address challenges facing their work force.

Sec. 654. Office of Disability Integration and Coordination of Department of Homeland Security.

This section codifies the Office of Disability Integration and Coordination (ODIC) within FEMA to be responsible for coordinating matters relating to individuals with disabilities in before, during, and after natural disasters, terrorist attacks, or other manmade disasters. Additionally, the section requires the Government Accountability Office to study and report to Congress on the funding and staffing needs of the Office of Disability Integration and Coordination.

Hurricane Katrina revealed that adequate measures had not been taken to integrate the needs of vulnerable populations into disaster response planning. Congress responded by, among other things, establishing the position of the Disability Coordinator at FEMA to assess the unique needs of children related to the preparation for, response to, and recovery from all hazards, including major disasters and emergencies.

The Disability Coordinator was tasked with providing guidance and coordination on matters related to individuals with disabilities in emergency planning and relief efforts, providing guidance to ensure disaster response plans, including evacuation routes and transportation options accommodate and are made known to individuals with disabilities, and implementing policies to ensure that the rights and feedback of individuals with disabilities regarding post-evacuation residency and relocation are respected, among other things.. In December 2009, the Disability Coordinator as-

sumed the leadership of a new Office of Disability Integration and Coordination.

The Committee formally authorized the ODIC in recognition of its important work advancing the goal of integrating the needs of those with disabilities into emergency plans and the work that remains to be done.

TITLE VII-OTHER MATTERS

Sec. 701. Decision regarding certain executive memoranda.

This section requires the Secretary of Homeland Security to review existing Department of Homeland Security memoranda to determine whether such memoranda should remain in effect and if so whether any memoranda should be modified.

The Committee believes the Department should work to streamline existing guidelines and supports action by the Secretary to review and organize existing Department memoranda.

Sec. 702. Permanent authorization for Asia-Pacific Economic Cooperation Business Travel Card Program.

This section will permanently authorize the Asia-Pacific Economic Cooperation Business Travel Card Program (APEC) while maintaining the Department of Homeland Security's authority to revoke an individual's card if there is a sufficient security justification.

Nearly 30,000 American business and government card-holders will be able to access fast-track lanes at airports in the 21 APEC countries, which saves a significant amount of time. This program is of no cost to taxpayers, and facilitates travel for verified individuals who have enrolled in a trusted traveler program. The program will sunset on September 30, 2018, and all cards will expire in 2021. This section will permanently authorize the APEC program while maintaining the Department's authority to revoke an individual's card if there is a sufficient security justification.

This section defines the term "public and private sector stakeholders" as the meaning given such term in section 114(u)(1)(C) of title 49, United States Code, which the Committee believes fully encompasses the intent of the overall provision.

Sec. 703. Authorization of appropriations for Office of Inspector General.

This section authorizes the Office of the Inspector General of the Department of Homeland Security at $175,000,000 for each Fiscal Year from 2018 to 2019.

Sec. 704. Canine teams.

This section authorizes the Commissioner of U.S. Customs and Border Protection to request additional canine teams to assist in the drug detection mission at the border. There must be a justified and documented shortage of existing canine teams in order to invoke this section. Canine teams serve a critical function and are one of the most reliable assets for drug detection.

The Committee believes that canines are a valuable resource for CBP to detect drugs, and fully supports the Commissioner's authority to deploy them as necessary.

Sec. 705. Technical amendments to the Homeland Security Act of 2002.

This section makes a number of technical changes to the Homeland Security Act of 2002. The section also strikes section 872 of the Homeland Security Act of 2002, removing the Secretary of Homeland Security's authority to reorganize the Department of Homeland Security without specific congressional authorization.

In keeping with its Article I constitutional powers, the Committee believes that reorganization of the Department should only occur following specific statutory authorization by Congress.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

The changes to existing law made by the bill in compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, were not made available at the time the report was filed.

○