H.R. 2825, the Department of Homeland Security Authorization Act Section-by-Section

Sec. 1. Short Title.

This act may be cited as the "Department of Homeland Security Authorization Act" or the "DHS Authorization Act".

Sec. 2. References.

DIVISION A—HOMELAND SECURITY

TITLE I—DEPARTMENT OF HOMELAND SECURITY HEADQUARTERS

Sec. 1001. Short title.

This section establishes the short title for the bill as the "Department of Homeland Security Authorization Act of 2017".

Subtitle A—Headquarters Operations

Sec. 1101. Homeland security enterprise defined.

This section amends the Homeland Security Act of 2002 to include a definition of "homeland security enterprise"

Sec. 1102. Functions and components of Headquarters of Department of Homeland Security.

This section 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. 1103. Repeal of Director of Shared Services and Office of Counternarcotics Enforcement of Department of Homeland Security.

This section abolishes the Director of Shared Services position as well as the now defunct Office of Counternarcotics Enforcement.

Sec. 1104. Responsibilities and functions of Chief Privacy Officer.

This section amends the Homeland Security Act of 2002 by authorizing the Chief Privacy Officer and requiring that official to report directly to the Secretary. Section 1104 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. 1105. Responsibilities of Chief Financial Officer.

This section amends the Homeland Security Act of 2002 by including additional responsibilities for the Chief Financial Officer (CFO). Specifically, Section 1105 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. 1106. Chief Information Officer.

This section 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 FY 2019.

Sec. 1107. Quadrennial Homeland Security review.

This section 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. 1108. Office of Strategy, Policy, and Plans.

This section states that the Office of Strategy, Policy, and Plans shall include the following components: 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 the 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. This section further specifies 12 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. This section 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. 1109. Office of External Affairs

This section authorizes the creation of an Office of External Affairs composed of the Offices of Legislative Affairs, Public Affairs, and Partnership and Engagement. The Office shall be headed by a Principal Assistant Secretary for External Affairs. 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 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 Government Coordination, and the Special Assistant to the Secretary authorized by section 102(f) of the Homeland Security Act of 2002. The Office of State and Local Government Coordination and Special Assistant to the Secretary are abolished.

Sec. 1110. Chief Procurement Officer.

This section 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 1109 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 1109 includes a clerical amendment to include the CPO in the Homeland Security Act's table of contents.

Sec. 1111. Chief Security Officer.

This section amends the Homeland Security Act of 2002 by authorizing the Chief Security Officer and requiring that official to report directly to the USM. Section 1110 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. 1112. Office of Inspector General.

This section 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 1111 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. 1113. Office for Civil Rights and Civil Liberties.

This section 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. 1114. Department of Homeland Security Rotation Program.

This section 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 1113 requires the Secretary to establish the "Intelligence Rotational Assignment Program" to be administered 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 1113 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 1113 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. 1115. Future Years Homeland Security Program.

This section 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 1114 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. 1116. Field efficiencies plan.

This section 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. 1117. Submission to Congress of information regarding reprogramming or transfer of Department of Homeland Security resources to respond to operational surges.

This section 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. 1118. Report to Congress on cost savings and efficiency.

This section 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. 1119. Research and development and CBRNE organizational review.

This section 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 1118 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 three 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. 1120. 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 and Other Matters

Sec. 1131. Chief Human Capital Officer responsibilities.

This section amends the Homeland Security Act of 2002 to improve morale, employee engagement, and communications within the Department of Homeland Security workforce 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 workforce 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. 1132. Employee engagement steering committee and action plan.

This section 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 five years after the date of enactment of this section.

Sec. 1133. Annual employee award program.

This section 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. 1134. Independent investigation and implementation plan.

This section 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. 1135. Timely guidance to DHS personnel regarding Executive Orders.

This section 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. 1136. Secretary's responsibilities regarding election infrastructure.

This section 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. 1201. Definitions.

Section 1201 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. 1211. Acquisition authorities for Under Secretary for Management of the Department of Homeland Security.

This section 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.

This section 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. 1212. Acquisition authorities for Chief Financial Officer of the Department of Homeland Security.

This section 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. 1213. Acquisition authorities for Chief Information Officer of the Department of Homeland Security.

This section 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 1213 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. 1214. Acquisition authorities for Program Accountability and Risk Management.

This section 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.

This section 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.

This section 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.

This section 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. 1215. Acquisition innovation.

This section 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.

This section 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 1215 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. 1221. Acquisition Review Board.

This section 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.

This section includes provisions to strengthen accountability and uniformity within the DHS acquisition review process. Section 1221 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.

This section authorizes the ARB to conduct systematic reviews of acquisitions and consider trade-offs 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 1221 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. 1222. Requirements to reduce duplication in acquisition programs.

This section 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. 1223. Department leadership council.

This section 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. 1224. Government Accountability Office review of Board and of requirements to reduce duplication in acquisition programs.

This section requires the Government Accountability Office to conduct a review of the Acquisition Review Board established in Section 1221.

Sec. 1225. Excluded party list system waivers.

This section 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. 1226. Inspector General oversight of suspension and debarment.

This section 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. 1231. Congressional notification for major acquisition programs.

This section 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% 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% or a likely delay is greater than 12 months from what is in the APB, then the USM must notify Congress.

Sec. 1232. Multiyear Acquisition Strategy.

This section 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 1232 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.

This section 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 workforce accountability that identifies the acquisition workforce 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 workforce personnel to retain highly qualified personnel, among other things.

This section 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. 1233. Acquisition reports.

This section 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 cancelled, 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.

This section 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. 1301. 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."

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. 1302. 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 Department 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. 1303. 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.

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. 1304. 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 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. 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. Additional systems in progress include, Secure Flight, Aviation Worker, Border Crossing Information, and several U.S. Citizenship and Immigration Services datasets.

The Department initially planned to incorporate at least 20 data sets by the end of 2016 but has refocused on building full mission capability within the Cerberus system. 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 two 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 information 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. 1305. 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 workforce 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.

This section requires the Secretary to submit a report to Congress no later than two 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. 1306. 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." However, most experts and officials agree, "there is no more than anecdotal evidence that terrorist groups have used virtual currencies to support themselves." 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.

Sec. 1307. 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.

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 four 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. 1308. 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 responsibilities 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. 1309. 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.

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 one 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 five years regarding individuals who have had security clearances denied, suspended, or revoked. Within one year of enactment, the Secretary must develop a plan for creating greater uniformity across the Department in the security adjudication process and ensure that such information is protected.

Subtitle B—Stakeholder Information Sharing

Sec. 1311. 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. 1312. 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. 1313. 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. 1314. 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. 1315. 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 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 usually 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 1315 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 factsheet, 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. Lastly, section 1315 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. 1316. 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 1316 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 Federal 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. 1317. 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 five 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. 1318. 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 1318 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. 1401. 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% 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. 1402. 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. 1403. 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. 1404. 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. 1405. 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. 1406. Evaluation of Coast Guard Deployable Specialized Forces.

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. 1407. Cost benefit analysis of co-locating DHS assets.

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. 1408. Repeal of interagency operational centers for port security and secure systems of transportation.

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. 1409. Maritime security capabilities assessments.

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% 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 (P.L. 114-328) to identify the number of assets and personnel required to increase the Department's interdiction rate of known illicit activity in the Transit Zone.

Sec. 1410. Conforming and clerical amendments.

This section makes minor conforming and technical edits.

TITLE V—TRANSPORTATION SECURITY ADMINISTRATION

Subtitle A—Administration

Sec. 1501. 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. 1502. 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 five-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 five-year term did not transfer along with it. This section reinstates that five-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. 1503. 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. 1504. 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. 1505. 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.

Lastly, 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 examined 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. 1506. 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. 1507. 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. 1511. 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. 1512. 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. 1513. 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 delayed. The committee directs TSA to prioritize deployment of this technology across the nation's airports no later than December 2018.

Sec. 1514. 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. 1515. 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. 1516. 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, one 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. 1517. 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 publically 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 one 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. 1518. 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. 1519. 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. 1520. 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. 1521. 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. 1522. 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. 1523. 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. 1524. 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. 1525. 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. 1526. 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. 1527. Security screening personnel grievance procedures 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 one 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. 1528. 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. 1529. 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 FY 2018 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 travelling 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. 1531. 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. 1532. 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 six 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. 1533. 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. 1541. 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 database 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 database. 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 database 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 database.

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 jurisdictional 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. 1542. 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. 1543. 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. 1544. 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. 1551. 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. 1552. 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. 1561. 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. 1571. Definitions.

This section defines terms used in the bill.

Sec. 1572. 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. 1573. 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. 1574. 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. 1575. 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. 1576. TSA counterterrorism asset deployment.

This section requires, except during times of urgent need, the Administrator to provide a two-week notification to any affected stakeholder before terminating any TSA resource that was provided for six 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 measures 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. 1577. 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. 1578. 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. 1579. 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. 1580. 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. 1581. 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. 1582. 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. 1583. 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 inspectors 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. 1584. 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. 1585. 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. 1586. 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. 1587. Recurrent vetting for surface transportation credential-holders.

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. 1588. 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.

Subtitle H—Security Enhancements in Public Areas of Transportation Facilities

Sec. 1591. 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. 1592. 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. 1593. 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. 1594. Review of regulations.

This section requires that not later than one 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. 1595. 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. 1601. 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. 1602. 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. 1603. Grants to directly eligible tribes.

This section codifies the period of performance for grant awards to directly eligible tribes at 36 months.

Sec. 1604. 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. 1605. 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. 1606. 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. 1607. 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 Initiative or the State Homeland Security Grant Program. The Administrator is required to implement a uniform process for reviewing such applications against the following criteria:

1) current or past use of proposed equipment or systems by Federal agencies or the Armed Forces;
2) the absence of a national voluntary consensus standard for such equipment or systems;
3) the existence of an international consensus standard for such equipment or systems, and whether such equipment or systems meets such standard;
4) the nature of the capability gap identified by the applicant and how such equipment or systems will address such gap;
5) 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
6) any other factor determined appropriate by the Administrator.

This section also requires the Inspector General to report to Congress, no later than three 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. 1608. 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. 1609. 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. 1610. 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 database 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 database 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. 1611. 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. 1612. 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. 1613. 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% 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 Jersy 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. 1614. 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% increase over the current appropriated level and $152 million above the President's Fiscal Year 2018 budget request.

Sec. 1615. 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 overclassified. 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. 1616. 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. 1617. 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. 1618. 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. 1619. 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.

Subtitle B—Communications

Sec. 1631. 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. 1632. 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. 1633. 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 five 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. 1634. National Emergency Communications Plan.

This section requires the Office of Emergency Communications to update the National Emergency Communications Plan at least once every five years and consider the impact of emerging technologies on the attainment of interoperable communications as part of that update.

Sec. 1635. Technical edit.

This section makes technical corrections to the Emergency Communications Title of the Homeland Security Act of 2002.

Sec. 1636. 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. 1637. 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. 1641. 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 workforce has standards, policies, and metrics for occupational safety and health; and providing medical liaisons to the Department's components.

Sec. 1642. Medical Countermeasures Program.

This section authorizes the Department of Homeland Security's medical countermeasures program to protect the DHS workforce, 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 Governmental 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.

TITLE VII—OTHER MATTERS

Sec. 1701. 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. 1702. 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.

Sec. 1703. 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. 1704. 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. 1705. 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.

Sec. 1706. Savings clause.

This section adds a saves clause that nothing in this act shall be construed as providing the Department of Homeland Security or any of its components, agencies, or programs with real property authority, including with respect to leases, construction or other acquisitions and disposals.

DIVISION B—U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

Sec. 2001. Short title.

This act may be cited as the U.S. Immigration and Customs Enforcement Act.

Sec. 2002. Establishment of U.S. Immigration and Customs Enforcement.

This section amends Section 442 of the Homeland Security Act of 2002 (6 U.S.C. 252) to formally authorize U.S. Immigration and Customs Enforcement (ICE) within the Department of Homeland Security (DHS). It includes an authorization of:

- A Director of ICE
- General Enforcement Powers
- A Deputy Commissioner of ICE
- Homeland Security Investigations
- Office of Enforcement and Removal Operations
- Office of the Principal Legal Counsel
- The Office of Professional Responsibility

DIVISION C—UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES

Sec. 3001. Short title.

This act may be cited as the U.S. Citizenship and Immigration Services Authorization Act

Sec. 3002. Establishment of United States Citizenship and Immigration Services.

This section amends Section 451 of the Homeland Security Act of 2002 to formally reauthorize U.S. Citizenship and Immigration Services (USCIS) within the Department of Homeland Security (DHS). It includes an authorization of:

- A Director of USCIS
- A Deputy Director of USCIS
- Chief Counsel
- Chief of Policy and Strategy
- Office of Citizenship
- Fraud Detection and National Security Directorate
- Immigration Record and Identity Services Directorate
- Service Center Operations Directorate

DIVISION D—UNITED STATES SECRET SERVICE

Sec. 4001. Short title.

This act may be cited as the "Secret Service Reauthorization Act of 2017."

Sec. 4002. Presidential appointment of Director of the Secret Service.

This section requires the Director of the U.S. Secret Service to be Senate confirmed.

Sec. 4003. Restricted building or grounds.

This section clarifies that it is a federal crime to knowingly cause, with the intent to impede or disrupt the orderly conduct of Government business or official functions, any object to enter restricted buildings or grounds, including the White House and the Vice President's residence.

Sec. 4004. Threats against former vice presidents.

This section amends current law to permit the Secret Service to investigate threats against former Vice Presidents.

Sec. 4005. Increased training.

This section directs the Secret Service to increase the number of hours spent training, and directs it to provide joint training between Uniformed Division officers and Special Agents.

Sec. 4006. Training facilities.

This section authorizes the construction of facilities at the Rowley Training Center necessary to improve the training of officers of the Uniformed Division and Special Agents.

Sec. 4007. Evaluation of vulnerabilities and threats.

This section requires the Secret Service to devise and implement procedures for evaluating threats to the White House and its protectees, including threats from drones and explosives, and to report to Congress its findings.

Sec. 4008. Evaluation of use of technology.

This section requires the Secret Service to evaluate its technology at the White House, including ways that technology can be used to improve safety at the White House.

Sec. 4009. Evaluation of use of additional weaponry.

This section requires the Secret Service to evaluate the use of additional weaponry, including non-lethal weapons.

Sec. 4010. Security costs for secondary residences.

This section amends the Presidential Protection Assistance Act of 1976 by enabling the Secret Service to make necessary security upgrades to secondary residences by eliminating the $200,000 cumulative cap previously imposed on spending to secure a protectee's secondary residences, and requires notification to the Committees on Appropriations of any security enhancements made to secondary residences in lieu of a bicameral resolution.

Sec. 4011. Establishment of Ethics Program Office.

This section creates an Ethics Program Office to provide increased training to employees of the U.S. Secret Service.

Sec. 4012. Secret Service protection at polling places.

This section permits Secret Service agents to protect presidential candidates at polling places.

Sec. 4013. Sense of Congress.

This section contains a Sense of Congress that determinations by the Department of Homeland Security or the Secret Service regarding changes to the White House itself for protection reasons should be given significant deference with the many entities that have a role in approving such changes, including the National Capital Planning Commission and the Commission of Fine Arts.

DIVISION E — Coast Guard

Section 5001. Short Title and Table of Contents.

Short Title – cites the short title as "Coast Guard Authorization Act of 2017".

Title I – Authorizations

Section 5101. Authorization of appropriations.

This section amends section 2702 of title 14, United States Code, to authorize funding levels for the Coast Guard for fiscal years 2018 and 2019.

Section 5102. Authorized levels of military strength and training.

This section amends section 2704 of title 14, United States Code, to authorize the levels of military strength and training for fiscal years 2018 and 2019.

Title II – Coast Guard

Section 5201. Training; public safety personnel.

This section amends Chapter 7 of title 14, United States Code, to add a new section 155 which will authorize the Commandant to allow, on a reimbursable or non-reimbursable basis, non-Coast Guard public safety personnel to participate in training when a member of the Coast Guard is unavailable. Public safety personnel is defined as any federal, state (or political subdivision thereof), territorial, or tribal law enforcement officer, firefighter, or emergency response provider.

Section 5202. Commissioned service retirement.

This section allows the President to reduce the retirement requirement of at least 10 years of active service as a commissioned officer to eight years, for Coast Guard officers who retire in fiscal year 2017 or 2018.

Section 5203. Officer promotion zones.

This section amends section 256(a) of title 14, United States Code, to adjust the number of officers in a promotion zone pool to account for current levels of attrition.

Section 5204. Cross reference.

This section amends section 373(a) of title 14, United States Code, to insert “designated under section 371” after “cadet”.

Section 5205. Repeal.

This section repeals section 482 of title 14, United States Code. The Coast Guard does not use the authority for the issuance of clothing at the time of discharge.

Section 5206. Unmanned aircraft system.

This section requires the Secretary of the Department in which the Coast Guard is operating to establish a land-based unmanned aircraft system program that would be under the control of the Commandant of the Coast Guard. The section limits the type of system the Commandant can acquire during any fiscal year when funds are appropriated for Offshore Patrol Cutter design or construction.

Section 5207. Coast Guard health-care professionals; licensure portability.

This section amends Chapter 5 of title 14, United States Code, to include a new section 104. Section 104 allows a health-care professional to practice in any location of any state, the District of Columbia, or a Commonwealth, territory or possession of the United States, regardless of where the health-care professional or patient are located, as long as the practice is within the scope of the authorized federal duties of such health-care professional. The health-care professionals must have a current license to

practice medicine, osteopathic medicine, dentistry, or another health profession, and be performing authorized duties for the Coast Guard.

Section 5208. Incentive contracts for Coast Guard yard and industrial establishments.

This section amends section 648 of title 14, United States Code, to allow the parties to an order for industrial work to be performed by the Coast Guard Yard or a Coast Guard industrial establishment to enter into an order or a cost-plus-incentive-fee order. If the parties agree to one of the project order options, an agreed-upon amount of any adjustment may be distributed as an incentive to the wage-grade industrial employees who complete the order.

Before entering into such order or cost-plus-incentive-fee order, the parties must agree that the wage-grade employees of the Coast Guard Yard or industrial establishment will take action to improve the delivery schedule or technical performance agreed to in the order.

If the workforce of the Coast Guard Yard or the industrial establishment satisfies the performance target established in a chosen order the adjustment pursuant to the agreement shall be reduced by the agreed upon amount and distributed to the wage-grade industrial employees and the remainder of the adjustment credited to the appropriations for the order.

Section 5209. Maintaining cutters in class.

This section amends section 573(c)(3)(A) of title 14, United States Code, to include "and shall maintain such cutter in class".

Section 5210. Congressional affairs; Director.

This section requires the Commandant to appoint a Director of Congressional Affairs from officers who serve in a grade above captain.

Section 5211. Contracting for major acquisition programs.

This section provides the Commandant of the Coast Guard and the head of an integrated program office with contracting authority for major acquisition programs. Contracting authorities include block buy, incremental funding, combined purchases, and multiyear contracts.

This section also makes conforming amendments to repeal section 223 of P.L. 113-281 (14 United States Code 577 note), section 221(a) of P.L. 113-281 (14 United States Code 573 note), and section 207 of P.L. 114-120 (14 United States Code 87 note).

Section 5212. National Security Cutter.

This section requires the Commandant of the Coast Guard, before certifying an eighth National Security Cutter as Ready for Operation, to provide a notification of a new standard method for tracking operational employment of Coast Guard major cutters that does not include time during which such cutter is a way from its homeport for maintenance or repair, and a report analyzing cost and performance for different approaches to achieving varied levels of operational tempos to the House Committee on Transportation and Infrastructure and the Senate Committee on Commerce, Science, and Transportation.

This section makes conforming amendments to repeal section 221(b) of the Coast Guard and Maritime Transportation Act of 2012 and 204(c)(1) of the Coast Guard Authorization Act of 2015.

Section 5213. Radar refresher training.

This section requires the Coast Guard to prescribe a final rule to eliminate the requirement that a mariner complete an approved refresher or recertification course to maintain a radar observer endorsement.

Section 5214. Repeal.

This section amends section 676a(a) of title 14, United States Code, to repeal paragraph (2) removing the sunset date and reconfigures paragraph (1).

Section 5215. Extension of Authority.

This section extends the authority given to the Commandant of the Coast Guard to designate shortage category positions and use the authorities in section 3304 of title 5, United States Code, to recruit and appoint highly qualified people to the positions. The authority is extended for two years, fiscal years 2018 and 2019.

Section 5216. Authorization of amounts for Fast Response Cutters.

This section authorizes $165 million, within the levels authorized in the bill, for the acquisition of six Fast Response Cutters in addition to the 58 currently included in the acquisition baseline. The six additional cutters shall replace the six 110-foot cutters currently in Patrol Forces Southwest Asia.

Section 5217. Authorization of amounts for ice trials of icebreaker vessels.

This section authorizes $3 million, within the levels authorized in the bill, for ice trials of icebreaker vessels.

Section 5218. Shoreside infrastructure.

This section authorizes authorization of $165 million per year, within the levels authorized in the bill, for un-met shore-side infrastructure needs which are now estimated to cost $1.6 billion.

Section 5219. Aircraft improvements.

This section authorizes authorization of $3.5 million per year, within the levels authorized in the bill, to fund analysis and program development for improvements for Coast Guard MH-65 aircraft.

Section 5220. Acquisition plan for inland waterway and river tenders and Bay-class ice breakers.

This section requires the Commandant of the Coast Guard to submit a plan to replace or extend the life of the Coast Guard fleet of inland waterway and river tenders, and the Bay-class icebreakers to the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science and Transportation of the Senate.

Section 5221. Report on sexual assault victim recovery in the Coast Guard.

This section requires the Commandant of the Coast Guard to submit a report on sexual assault prevention polices of the Service and strategic goals related to sexual assault victim recovery to the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science and Transportation of the Senate.

Title III – Ports and Waterways Safety

Section 5301. Codification of Ports and Waterways Safety Act.

This section creates a new chapter 700, Port Safety, in title 46, United States Code. These provisions were previously included in the Ports and Waterways Safety Act.

Section 5302. Conforming amendments.

This section transfers a section of the Ports and Waterways Safety Act to section 3105 of title 46, United States Code. The section also states that except pursuant to an international treaty, convention, or agreement to which the United States is a party, this section shall not apply to any foreign vessel not destined for, or departing from, a port or place subject to the United States. This allows the foreign vessel innocent passage through the territorial sea of the United States or transit through U.S. navigable waters that form a part of an international strait.

Section 5303. Transitional and savings provisions.

This section defines "source provision" and "Title 46 provision". It also outlines that the transferred title 46 provisions are deemed to have been enacted on the date of enactment of the source provision it replaces. References to the source provisions are deemed to refer to the corresponding title 46 provision; any regulation referencing or implementing a source provision are deemed to refer to or implement the corresponding title 46 provision; and any action taken or offense committed under a source provision is deemed to have been taken or committed under the corresponding title 46 provision.

Section 5304. Rule of construction.

This section explains that this title, including any amendments, is intended to move provisions from the Ports and Waterways Safety Act to title 46. It should not be construed as altering: the effect of provisions of the Ports and Waterways Safety Act, or any authorities or requirements in such Act; a department or agency interpretation with respect to such Act; or any judicial interpretation with respect to such Act.

Section 5305. Advisory Committee: Repeal.

This section repeals section 18 of the Coast Guard Authorization Act of 1991.

Section 5306. Regattas and Marine Parades.

This section moves provisions relating to regattas and marine parades into chapter 700 of title 46.

Section 5307. Regulation of vessels in territorial waters of the United States.

This section moves provisions relating to the regulation of vessels in territorial waters of the United States, regulation of anchorage and movement of vessels during national emergency, and seizure and forfeiture of vessel, fine, and imprisonment into chapter 700 of title 46.

Title IV – Maritime Transportation Safety

Section 5401. Clarification of logbook entries.

This section amends section 11304 of title 46, United States Code, to strike "an official logbook, which" and inserts "a logbook". It also amends subsection (b) to include a new paragraph (3) which requires the logbook to include each illness of, and injury to, a seaman of the vessel, the nature of the illness or injury, and the medical treatment provided for the injury or illness.

Section 5402. Technical Corrections: licenses, certifications of registry, and merchant mariner documents.

This section clarifies terminology by amending the following sections of title 46, United States Code: 7106(b) to strike "merchant mariner's document" and insert "license"; section 7107(b) to strike "merchant mariner's document" to insert "certificate of registry"; section 7507(b)(1) to strike "licenses and certificates of registry" and insert "merchant mariner's documents"; and section 7507(b)(2) to strike "merchant mariner's document" to insert "license or certificate or registry."

Section 5403. Numbering for undocumented barges.

This section amends section 12301(b) of title 46 United States Code, to strike "shall" and insert "may", thus making the authority discretionary.

Section 5404. Drawbridge deviation exemption.

This section amends the Act of August 18, 1894 (33 U.S.C. 499) to create an exemption for a change in schedule that governs the opening of a drawbridge that will be in effect for less than six months to not be subject to the rule making requirements of section 533 of title 5, United States Code. Instead, alternative requirements are created to require the Coast Guard to notify each six months or less schedule change through a notice to local mariners, broadcasts, or another method of notice the Secretary considers appropriate. It also requires the owner of the drawbridge to provide notice of such schedule changes to the general public through a newspaper of general circulation, the public office with jurisdiction over the roadway that abuts the approach to the bridge, and the law enforcement organization with authority over the roadway.

Section 5405. Deadline for compliance with alternate safety compliance programs.

This section amends section 4503(d)(1) of title 46, United States Code, to allow the Secretary, in cooperation with the commercial fishing industry, to prescribe an alternate safety compliance program that shall apply in lieu of requirements under section 4502(b). The alternate safety compliance program would apply to any category of fishing vessels, fish processing vessels, or fish tender vessels that are at least 50 feet in overall length, built before July 1, 2013, and 25 years of age or older.

New paragraph (2) requires the alternate safety compliance program to apply to a vessel after the later of January 1, 2020, or the end of the three year period beginning on the date on which the Secretary prescribes the program. In the case of a vessel that undergoes a major conversion completed after July

1, 2013, or the date the Secretary establishes standards for the alternate safety compliance program, upon the completion of the conversion.

A conforming amendment is made to 4502(b) of title 46, United States Code, by inserting "and subject to section 4503(d)," after "In addition to the requirements of subsection (a) of this section,".

Section 5406. Authorization for marine debris program.

This section authorizes funding for Coast Guard marine debris functions at $2 million and limits administrative costs to 10 percent.

Section 5407. Alternative distress signals.

This section requires the Secretary of the department in which the Coast Guard is operating, not later than one year after the date of enactment of this Act, to issue a rule that establishes a performance standard for distress signals. Not later than 180 days after issuing such rule, the Secretary is required to update the Code of Federal Regulations to authorize the use of distress signals.

Section 5408. Atlantic Coast Port Access Route Study recommendations.

This section requires, not later than 30 days after the date of enactment of this Act, the Commandant of the Coast Guard to notify the House Committee on Transportation and Infrastructure and the Senate Committee on Commerce, Science, and Transportation of action taken to carry out the recommendation contained in the final report *Atlantic Coast Port Access Route Study* published March 14, 2016.

Section 5409. Documentation of recreational vessels.

This section would allow Coast Guard personnel performing non-recreational vessel documentation functions to perform recreational vessel documentation functions in any fiscal year where there is a backlog of applications for recreational vessel documentation, when operating expenses funds may not be used for expenses incurred for recreational vessel documentation, and when fees collected from owners of yachts and credited to such use are insufficient to pay the expenses of recreational vessel documentation.

Section 5410. Certificates of documentation for recreational vessels.

This section amends section 12114 of title 46, United States Code, to make the provision allowing recreational endorsements for a vessel to be effective for five years. The section would have the endorsement terminate after a 30 day period if the owner does not notify the Coast Guard of changes in information required for the endorsement within the 30 day window. The section does not limit the authority of a state or local authority to take action to address abandoned and derelict vessels. The section also authorizes the collection of a fee for issuance of recreational vessel certificates of documentation.

Section 5411. Backup Global Positioning System.

This section requires the Secretary of the Department in which the Coast Guard is operating, in consultation with the Secretary of Transportation, to provide for the establishment, sustainment, and operation of a reliable land-based enhanced LORAN, or eLORAN, positioning, navigation, and timing system. The system would provide a compliment to, or backup for, the Global Positioning System. It

would ensure the availability of uncorrupted and non-degraded positioning, navigation, and timing signals for military and civilian users in the event the global system signals are corrupted, degraded, unreliable, or otherwise unavailable.

Section 5412. Waters deemed not navigable waters of the United States for certain purposes.

This section provides regulatory relief for the mule-powered vessel *Volunteer* (Hull Number CCA4108) on the Illinois and Michigan Canal.

Section 5413. Uninspected passenger vessels in St. Louis County, Minnesota.

This section provides regulatory relief for certain passenger vessels on Crane Lake in St. Louis County, Minnesota.

Section 5414.Engine cut-off switch requirements.

This section requires the Coast Guard to issue regulations requiring the installation of engine cut-off switches, in compliance with the American Boat and Yacht Standard A-33, on recreational vessels less than 26 feet in overall length. The section also allows the Coast Guard, through the National Boating Safety Advisory Council, to initiate a boating safety education program on the use and benefit of cut-off switches for recreational vessels.

Section 5415. Analysis of commercial fishing vessel classification requirements.

This section requires the Coast Guard to analyze the implementation of section 4503 of title 46, United States Code, to determine the average costs on vessel owners to comply with section 4503 and the impact the requirements of section 4503 are having on commercial fishing safety.

Title V – Miscellaneous

Section 5501. Repeal.

This section repeals subsection (h) of section 888 of the Homeland Security Act of 2002.

Section 5502. Reimbursements for non-federal construction costs of certain private aids-to-navigation.

This section would allow the Commandant, subject to appropriations, to reimburse a non-federal entity for costs incurred by the entity to construct and establish an aid to navigation authorized in title I of P.L. 110-114 that facilitates safe and efficient marine transportation on a federally authorized navigation channel. The section provides specific conditions under which the Commandant can reimburse an entity, it limits reimbursements for a single project at $5,000,000, and the authority expires four years after the date of enactment of the bill.

Section 5503. Corrections to provisions enacted by Coast Guard Authorization Acts.

This section amends section 604(b) of the Howard Coble Coast Guard and Maritime Authorization Act of 2014 to insert “and fishery endorsement” after “endorsement”.

Section 5504. Ship Shoal Lighthouse transfer; Repeal.

This section puts a sunset date of January 1, 2021, in section 27 of the Coast Guard Authorization Act of 1991.

Section 5505. Coast Guard maritime domain awareness.

This section requires the Coast Guard to enter into an arrangement with the National Academy of Sciences, under which the Academy will prepare an assessment on existing and emerging unmanned technologies that can be used by the Coast Guard in the maritime domain for a number of Coast Guard purposes. The Academy must also analyze how the use of new and emerging maritime domain awareness technologies can assist the Coast Guard to carry out its missions at lower costs, expand the scope and range of the Service's maritime domain awareness, and use its personnel and assets more efficiently, and identify adjustments in any Coast Guard policies, procedures, and protocols to incorporate these technologies.

Section 5506. Towing safety management system fees.

The Commandant of the Coast Guard is required to review and compare the costs of inspections performed by the Service and by a third party. If the Commandant determines there is a difference in the fee costs, the Commandant is required to revise the fee structure to conform to the requirements under section 9701 of title 31, United States Code, that the costs of the fees accurately reflect the costs of administering the inspections.

Section 5507. Oil spill disbursements auditing and report.

This section modifies an existing Oil Spill Liability Trust Fund audit requirement being conducted by the Government Accountability Office and moves the requirement to the Coast Guard to be reported through an existing report. It further requires the Coast Guard to submit information on disbursements from the Fund for removal costs and damages totaling more than $500,000 to Congress.

Section 5508. Land exchange, Ayakulik Island, Alaska.

This section authorizes a land exchange between the owner of the Ayakulik Island and the Secretary of the Interior. The Secretary of the Interior would receive Ayakulik Island, a bird rookery, for the transfer of a tract of submerged lands in Womens Bay, Alaska. It is roughly a one-to-one acre land exchange. The Coast Guard will be given the opportunity to apply operational restrictions on the tract of submerged lands to ensure they can effectively continue Service operations in Womens Bay.

Section 5509. Vessel response plans in the Arctic report.

This section requires the Coast Guard to submit to the Transportation and Infrastructure Committee of the House of Representatives and the Committee on Commerce, Science, and Transportation in the Senate a report on the assets available for a response and the location of the equipment, among other items in the Captain of the Port zone including the Arctic.

Section 5510. Assessment of public comments on additional anchorages on the Hudson River.

This section requires the Commandant of the Coast Guard to assess the public comments it received regarding the establishment of additional anchorages on the Hudson River between Yonkers, New York and Kingston, New York. The Service is required to issue a report to the House Transportation and Infrastructure Committee and the Senate Commerce, Science, and Transportation Committee regarding concerns raised by public comments and how the Service responded to such concerns. The Coast Guard cannot establish new anchorages until 180 days after submission of the report.

Section 5511. Public safety answering points and maritime search and rescue coordination.

This section requires the Secretary of the department in which the Coast Guard is operating to review Coast Guard policy and procedures for public safety answering points and search and rescue coordination with State and local law enforcement entities. The review should look to minimize the possibility that 911 calls being improperly routed and assure the Service can effectively carry out its maritime search and rescue mission. The Commandant of the Coast Guard is required to formulate a national maritime public safety answering points policy and submit a report to Congress.

Section 5512. Documentation of "America's Finest".

This section allows the Coast Guard to issue a certificate of documentation with a coastwise and a fishery endorsement for the fishing vessel *America's Finest* (United States official number 1276760).

DIVISION F—FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

Sec. 6001. Short title.

This act may be cited as the "FEMA Reauthorization Act of 2017."

Sec. 6002. Reauthorization of Federal Emergency Management Agency.

This section reauthorizes FEMA through FY2020, consistent with current funding levels. For FY2018 - $1.05 billion; for FY2019 - $1.07 billion; and for FY2020 - $1.08 billion.

Sec. 6003. Comprehensive study of disaster costs and losses.

This section directs the National Advisory Council to undertake a comprehensive study of the trends related to disaster assistance, costs and losses and provide recommendations to reduce the costs related to these events.

Sec. 6004. National Domestic Preparedness Consortium.

This section reauthorizes the Center for Domestic Preparedness through FY2020, consistent with current funding levels. For FY2018 - $63.9 million; for FY2019 - $65 million; and for FY2020 - $66 million. Reauthorizes the National Domestic Preparedness Consortium through FY2020, consistent with current funding levels. For FY2018 - $101 million; for FY2019 - $102.6 million; for FY2020 - $104.2 million.

Sec. 6005. Rural Domestic Preparedness Consortium.

This section states that the FEMA Administrator is responsible for the Nation's efforts to reduce the loss of life and property from an earthquake, tsunami or combined event.

Sec. 6006. National preparation and response efforts relating to earthquakes and tsunamis.

This section clarifies what constitutes a federal action for purposes of consultation.

Sec. 6007. Authorities.

This section makes technical corrections to the national emergency management provisions of the law by making needed updates and corrections to unintentional errors.

Sec. 6008. 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.

Sec. 6009. 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. 6010. 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 five 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. 6011. 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. 6012. 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. 6013. 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. 6014. 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.

Sec. 6015. 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. 6016. 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 identify 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. 6017. 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 workforce 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 workforce plan for 2008-2012 did not include performance metrics or identify potential workforce gaps, overlaps, or inconsistencies. Additionally, the National Academy for Public Administration recommended that FEMA develop a 5-year strategic workforce 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 workforce.

Sec. 6018. 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 assumed 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.

Sec. 6019. Technical amendments to National Emergency Management.

This section makes technical changes to the national emergency management provisions of the law by making needed updates and corrections to unintentional errors.