Calendar No. 381

115TH CONGRESS *2d Session*	SENATE	REPORT 115–351

DEPARTMENT OF HOMELAND SECURITY REAUTHORIZATION ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

H.R. 2825

TO AMEND THE HOMELAND SECURITY ACT OF 2002 TO MAKE CERTAIN IMPROVEMENTS IN THE LAWS ADMINISTERED BY THE SECRETARY OF HOMELAND SECURITY, AND FOR OTHER PURPOSES

NOVEMBER 13, 2018.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
89–010 WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN MCCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
JOHN HOEVEN, North Dakota
STEVE DAINES, Montana

CLAIRE MCCASKILL, Missouri
THOMAS R. CARPER, Delaware
HEIDI HEITKAMP, North Dakota
GARY C. PETERS, Michigan
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
DOUG JONES, Alabama

CHRISTOPHER R. HIXON, *Staff Director*
GABRIELLE D'ADAMO SINGER, *Chief Counsel*
MICHAEL J. LUEPTOW, *Chief Counsel for Homeland Security*
MARGARET E. DAUM, *Minority Staff Director*
CHARLES A. MOSKOWITZ, *Minority Senior Legislative Counsel*
SUBHASRI RAMANATHAN, *Minority Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 381

115th Congress
2d Session

SENATE

REPORT
115–351

DEPARTMENT OF HOMELAND SECURITY REAUTHORIZATION ACT

NOVEMBER 13, 2018.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, submitted the following

REPORT

[To accompany H.R. 2825]

[Including cost estimate of the Congressional Budget Office]

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

CONTENTS

		Page
I.	Purpose and Summary	1
II.	Background and Need for the Legislation	2
III.	Legislative History	25
IV.	Section-by-Section Analysis	27
V.	Evaluation of Regulatory Impact	59
VI.	Congressional Budget Office Cost Estimate	59
VII.	Changes in Existing Law Made by the Act, as Reported	63

I. PURPOSE AND SUMMARY

H.R. 2825 authorizes the Department of Homeland Security (DHS or the Department) and makes improvements to multiple Department policies and programs. The Act includes seven titles covering headquarters, acquisition accountability, intelligence and information sharing, emergency preparedness, the Federal Emergency Management Agency, a new Cybersecurity and Infrastructure Security Agency, and other matters.

II. Background and the Need for Legislation

In response to the terrorist attacks against the United States on September 11, 2001, Congress established the Department with the passage of the Homeland Security Act of 2002.[1] The establishment of the Department represented the most significant transformation of the U.S. Government in over a half-century.[2] Prior to its creation, homeland security activities were spread across more than 100 Federal organizations.[3] DHS was created to be America's "single, unified homeland security structure that will improve protection against today's threats and be flexible enough to help meet the unknown threats of the future."[4] Since 2002, DHS has undergone internal reorganizations and consolidations to create efficiencies, enhance mission effectiveness, and reduce duplication of effort across Department components. Today, DHS consists of 14 operational and support components, in addition to the Office of the Secretary.[5]

The Department has five core missions and responsibilities that include: "prevent terrorism and enhanc[e] security; secure and manage our borders; enforce and administer our immigration laws; safeguard and secure cyberspace; and ensure resilience to disasters."[6]

Authorizing legislation is a critical responsibility of Congress to provide direction for the missions, activities, and offices of executive agencies. Therefore, this Committee aims to provide DHS comprehensive guidance in a reauthorization of the Department to clarify its organization, authorities, and responsibilities.

Title I—DHS Headquarters

The Department has not been fully reauthorized since its inception over fifteen years ago. As the threat landscape continues to evolve, the Department adjusted its organization and activities to address emerging threats and protect the U.S. homeland.[7] This evolution of the Department's duties and organization, including the structure and operations of the DHS Headquarters, has never been codified in statute.

Title I of the Homeland Security Act of 2002 established DHS, its mission, and the roles and responsibilities of several offices and officers in the Department that directly support the DHS Secretary in management of the Department and its activities.[8] However, not all components of the DHS Headquarters were initially outlined in the Homeland Security Act of 2002, and the functionality of headquarters components has evolved over the past fifteen years.

---

[1] Pub. L. No. 107–296 (107th Cong.) (2002).

[2] U.S. Department of Homeland Security, DHS, (June 2002), https://www.dhs.gov/sites/default/files/publications/book_0.pdf.

[3] *Id.*

[4] *Id.*

[5] U.S. Department of Homeland Security, *Operational and Support Components*, https://www.dhs.gov/operational-and-support-components.

[6] DHS, *Our Mission*, https://www.dhs.gov/our-mission (last updated May 11, 2016).

[7] *See, e.g., The Department of Homeland Security*, (June 2002), *available at* https://www.dhs.gov/sites/default/files/publications/book_0.pdf. *Compare Department of Homeland Security Original Organization Chart, March 2003, available at* https://www.dhs.gov/xlibrary/assets/dhs-org-chart-2003.pdf, with *Department of Homeland Security Organization Chart, available at* https://www.dhs.gov/sites/default/files/publications/18_0519_DHS_Organizational_Chart.pdf (May 21, 2018).

[8] Pub. L. No. 107–296 (107th Cong.) (2002).

The Department's Headquarters and management have struggled with a variety of issues since initial authorization and establishment. GAO and the DHS OIG have consistently cited challenges with oversight of management, acquisitions and procurement, workforce strategic planning and retention, and stakeholder engagement. For example, since 2003, GAO has consistently placed management functions of the Department on its High Risk List.[9] The initial undertaking of consolidating 22 different agencies and organizations into one cabinet-level department posed great challenges in and of itself. However, as the threat landscape and the DHS mission evolved over the years, so did the management challenges. In 2013, DHS made enough progress in its operational components that GAO refocused its reporting specifically on DHS Headquarters.[10] For DHS to succeed, the institutional framework for the Department's Headquarters, including offices and critical leadership positions, need clearly defined roles and authorities as directed by Congress.

Title I of this Act codifies some of the organizational changes DHS has made to address challenges and enhance oversight and management of critical initiatives. This legislation clarifies responsibilities for key leadership roles within the Headquarters, including the Chief Acquisitions Officer and Chief Human Capital Officer (CHCO), to ensure effective and strategic management of all of the Department's resources. One specific authority granted to chief officers to make management more effective is the ability for Headquarters to directly oversee their operational component counterparts.

Another position codified in the Act but not included in the Homeland Security Act of 2002 is the Chief Procurement Officer, tasked with oversight of procurement contracts and major acquisitions for DHS.[11] DHS has historically struggled with large-scale procurements and acquisition programs.[12] For example, the Secure Border Initiative Network (SBI*net*) technology acquisition process started in November 2005 to enhance security along the entire southwest border.[13] The DHS Office of Inspector General (OIG), the Government Accountability Office (GAO), and hearings held by the Committee have highlighted the failures of SBI*net* due to acquisition management deficits.[14] DHS ended the multi-billion dollar project after numerous schedule delays, cost overruns, and technical problems.[15] Ultimately the program cost the taxpayers $1 bil-

---

[9] Gov't Accountability Office, GAO–17–317, Strengthening Department of Homeland Security Management Functions, https://www.gao.gov/highrisk/strengthening_homeland_security/why_did_study.

[10] *Id.*

[11] Pub. L. No. 107–296 (107th Cong.) (2002).

[12] Gov't Accountability Office, GAO–17–346SP, Earlier Requirements Definition and Clear Documentation of Key Decisions Could Facilitate Ongoing Progress (2017), https://www.gao.gov/products/GAO-17-346SP.

[13] Gov't Accountability Office, GAO–08–131T, Observations on Selected Aspects of SBI*net* Program Implementation (2007), https://www.gao.gov/assets/120/118254.pdf.

[14] Gov't Accountability Office, GAO–10–840T, DHS Needs to Follow Through on Plans to Reassess and Better Manage Key Technology Program (2010), https://www.gao.gov/new.items/d10840t.pdf; *Securing the Border: Fencing, Infrastructure, and Technology Force Multipliers: S. Homeland Sec. & Governmental Affairs Comm.,* 114th Cong. (2015) (Statement of Chairman Ron Johnson); and *Border Security: Moving Beyond the Virtual Fence: S. Homeland Sec. & Governmental Affairs Comm.*, 114th Cong. (2010) (Statement of Chairman Joseph Lieberman).

[15] Gov't Accountability Office, GAO–14–368, Arizona Border Surveillance Technology Plan: Additional Actions Needed to Strengthen Management and Assess Effectiveness (2014), https://www.gao.gov/assets/670/661297.pdf.

lion and only provides security to 53 miles of the 387-mile Arizona-Mexico border.[16] By codifying the Chief Procurement Officer's position, role, and responsibilities, the Act provides needed organizational controls at DHS Headquarters to oversee and implement consistent procurement activities of DHS components.

The Committee remains concerned about the ability of the Department to effectively manage its resources to execute its mission. The Act contains a provision that enhances the Committee's ability to conduct oversight of the Department's budget and increases transparency of how its resources are used to carry out vital homeland security programs and operations. Specifically, the Act requires DHS to submit annual reports to the Homeland Security Committees (as defined in the legislation) that include information regarding the transfer and reprogramming of funds to address unforeseen costs and operational surges through 2023.

The Committee was concerned that the Department was not sufficiently organized to address threats posed by chemical, biological, radiological and nuclear weapons. Building on other Federal entities' efforts to consolidate and streamline their weapons of mass destruction mission functions, Congress required DHS to review its weapons of mass destruction responsibilities and consider how best to restructure these functions.[17] DHS submitted its report in June 2015.[18] GAO subsequently concluded that the Department's proposed reorganization did not include an assessment of the potential problems, costs, and benefits resulting from its consolidation proposal.[19] Congress did not enact legislation to consolidate the Department's chemical, biological, radiological, nuclear, and explosives functions as outlined in the 2015 proposal.[20] In October 2017, acting through authorities provided under section 872 of the Homeland Security Act of 2002, the Department notified Congress of its plans to reorganize and combine its weapons of mass destruction mission functions into a Countering Weapons of Mass Destruction (CWMD) office.[21] This reorganization was effective December 2017.[22]

This Act authorizes the establishment of the CWMD office within DHS and codifies a basic organizational structure in which the Domestic Nuclear Detection Office (DNDO) and portions of the Office

---

[16] *Id.*

[17] Senate explanatory statement accompanying the Consolidated and Further Continuing Appropriations Act, 2013, Pub. L. No. 113-6, 127 Stat. 198 (2013), 159 Cong. Rec. S1547 (daily ed. Mar. 11, 2013). See also H.R. Rep. No. 112-492, at 13-14 (2012).

[18] Gov't Accountability Office, GAO-16-603, DHS's Chemical, Biological, Nuclear and Explosives Program Consolidation Proposal Could Better Consider Benefits and Limitations (2016), https://www.gao.gov/products/GAO-16-603.

[19] Gov't Accountability Office, GAO-16-603, DHS's Chemical, Biological, Nuclear and Explosives Program Consolidation Proposal Could Better Consider Benefits and Limitations (2016), https://www.gao.gov/products/GAO-16-603.

[20] See H.R. 3875, Department of Homeland Security CBRNE Defense Act of 2015, 114th Cong.; *see also Examining the Department of Homeland Security's Efforts to Counter Weapons of Mass Destruction, H. Homeland Sec. Comm., Emergency Preparedness, Response, and Communications Subcomm.*, 115th Cong. (2017), https://homeland.house.gov/hearing/examining-department-homeland-securitys-efforts-counter-weapons-mass-destruction/.

[21] Letter from The Honorable Elaine Duke, Acting Secretary, Dep't of Homeland Sec., to The Honorable Ron Johnson, Chairman, to Homeland Sec. & Governmental Affairs Comm. (Oct. 6, 2017); Letter from The Honorable Elaine Duke, Acting Secretary, Dep't of Homeland Sec., to The Honorable Claire McCaskill, Ranking Member, Homeland Sec. & Governmental Affairs Comm. (Oct. 6, 2017).

[22] Press Release, Dep't of Homeland Sec., *Secretary Nielsen Announces the Establishment of the Countering Weapons of Mass Destruction Office* (Dec. 7, 2017), https://www.dhs.gov/news/2017/12/07/secretary-nielsen-announces-establishment-countering-weapons-mass-destruction-office.

of Health Affairs comprise the new CWMD office. Because questions remain about the new organizational structure,[23] the CWMD office is authorized for a five-year period, after which time, Congress is required to re-authorize the office. If Congress does not re-authorize the office, the entities and functions comprising the office will be structured as they were preceding the enactment of this Act.

Title I also includes authorizing language related to human resources and other matters, which are intended, in part, to support the Department's efforts to enhance strategic workforce planning and improve overall employee effectiveness and morale. The Committee remains concerned that DHS has not taken the steps necessary to develop workforce plans that identify and address critical skills gaps across the Department. DHS remains on GAO's High-Risk List due in part to its inability to fully address human capital management challenges through the identification of the people and resources needed to fill critical mission support positions, specifically information technology and acquisition positions.[24] The authorizing language codifies the role and responsibilities of the Department's CHCO and includes provisions to address human capital management deficiencies. Specifically, the CHCO is charged with executing strategic resource plans that are driven by industry best practices, assessing the resourcing requirements for mission-support functions, and assessing the Department's efforts to recruit and retain employees in rural areas. The CHCO is to make policy recommendations to the Secretary and Congress, as necessary, to enhance the Department's human capital management processes.

The Committee is also concerned that DHS consistently ranks at or near the bottom of the annual Federal Employee Viewpoint Survey (FEVS) administered by the U.S. Office of Personnel Management.[25] Despite year-over-year improvements based on the most recent survey results, the Committee remains concerned about the overall employee morale and effectiveness of management to create a high-performing culture across components of the Department.

However, the Committee also recognizes the Department's efforts to improve historically-low employee morale. For instance, DHS has taken steps to strengthen employee engagement by implementing a GAO recommendation to establish metrics to evaluate the success of the Department's employment engagement action plans.[26] The Department's 2017 FEVS scores are indicative of this progress, as DHS's scores increased across four areas—leadership

---

[23] *Examining the Department of Homeland Security's Efforts to Counter Weapons of Mass Destruction, H. Homeland Sec. Comm., Emergency Preparedness, Response, and Communications Subcomm.*, 115th Cong. (2017), https://homeland.house.gov/hearing/examining-department-homeland-securitys-efforts-counter-weapons-mass-destruction/ (Statement of Chairman Ray Donovan).

[24] *Roundtable-Reauthorizing DHS: Positioning DHS to Address New & Emerging Threats to the Homeland, S. Homeland Sec. & Governmental Affairs Comm.* 5, 115th Cong. (2017), https://www.hsgac.senate.gov/imo/media/doc/Testimony-Scott-2018-02-07.pdf (Statement of George A. Scott, Managing Director, GAO Homeland Security & Justice).

[25] Joe Davidson, *Report ranks best and worst agencies for federal employees*, Wash. Post (Dec. 15, 2016), https://www.washingtonpost.com/news/powerpost/wp/2016/12/15/report-ranks-best-and-worst-agencies-for-federal-employees/?utm_term=.0f79787e3498.

[26] *Roundtable-Reauthorizing DHS: Positioning DHS to Address New & Emerging Threats to the Homeland, S. Homeland Sec. & Governmental Affairs Comm.* 7, 115th Cong. (2017), https://www.hsgac.senate.gov/imo/media/doc/Testimony-Scott-2018-02-07.pdf (Statement of George A. Scott, Managing Director, GAO Homeland Security & Justice).

and knowledge management, results-oriented performance culture, talent management, and job satisfaction.[27]

In testimony before the Committee, George Scott, GAO's Managing Director for Homeland Security and Justice Issues, stated that improving DHS's employee morale is a "significant undertaking that will likely require multiyear efforts" to fully address.[28] To better position DHS to continue improving morale, this Act requires an employee engagement and retention plan to enhance and build upon recent efforts to improve employee morale across the Department and its components.

The ever-present threat of malicious cyber-related attacks on our nation's critical infrastructure and Federal computer networks represents a significant challenge for the Department. As the lead Federal agency responsible for coordinating with public and private sector partners to mitigate these threats, DHS must ensure that it effectively deploys the tools, capabilities and workforce necessary to execute its mission.[29] GAO reported in February 2018 that DHS began the process of identifying its workforce capability gaps, but has yet to comply with a congressional mandate to identify and report Department-wide cybersecurity critical needs.[30] As such, the Committee is concerned that DHS may not have a workforce with the skills to carry out its mission. Moreover, the Committee echoes concerns raised by the Office of Management and Budget that the ability to attract and retain cybersecurity and information technology talent poses significant challenges and risks throughout the Federal Government.[31]

The Committee is also concerned that DHS is not sufficiently adhering to the Federal Information Technology Acquisition Reform Act (FITARA)—a bill aimed at reforming Federal information technology management and its acquisition workforce.[32] For instance, according the most recent Biannual FITARA Scorecard released in November 2017 by the House Committee on Oversight and Government and GAO, DHS's score declined from a B- to C- over the previous reporting period.[33]

As a step toward addressing these issues, this Act includes provisions to incorporate cybersecurity into DHS research and development activities by ensuring that the Department has access to the tools and resources necessary to properly execute its cybersecurity mission. Specifically, this Act requires DHS to submit a report detailing new cybersecurity projects and develop a training program for acquisitions staff involved in acquiring new cybersecurity technologies. The language also authorizes a cybersecurity talent exchange program to strengthen public and private sector collabora-

---

[27] *Id.*; Best Places to Work in the Federal Government, *Agency Report: Department of Homeland Security*, http://bestplacestowork.org/BPTW/rankings/detail/HS00.

[28] *Roundtable-Reauthorizing DHS: Positioning DHS to Address New & Emerging Threats to the Homeland, S. Homeland Sec. & Governmental Affairs Comm.* 4, 115th Cong. (2017), https://www.hsgac.senate.gov/imo/media/doc/Testimony-Scott-2018-02-07.pdf (Statement of George A. Scott, Managing Director, GAO Homeland Security & Justice).

[29] U.S. Government Accountability Office, GAO-18-175, Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements, https://www.gao.gov/assets/690/689880.pdf.

[30] *Id.*

[31] Federal Cybersecurity Workforce Strategy, Memorandum M-16-15, Office of Management and Budget (July 12, 2016).

[32] National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (Dec. 19, 2014), 40 U.S.C. § 11319(b)(1)(B)(ii).

[33] *OGR Biannual FITARA Scorecard*, https://oversight.house.gov/wp-content/uploads/2017/11/FITARA-Scorecard-5.0-.pdf.

tion on cybersecurity, which will support the Department's ability to execute its cybersecurity responsibilities including enhancing infrastructure security.

The Act also addresses an emerging threat related to U.S. election systems. DHS and the Intelligence Community confirmed that a number of states were targeted by Russia during the 2016 Presidential election.[34] While the Committee is pleased that DHS is working with state and local election officials to secure election infrastructure by providing a suite of tools including risk and vulnerability assessments, cyber hygiene scans, and intelligence threat feeds, we remain concerned about future efforts to interfere in U.S. elections and will continue conducting oversight of the Department's efforts.[35] This Act requires the Secretary to prioritize providing assistance, as appropriate, to state and local election officials. DHS must provide a yearly unclassified report to Congress on the Department's responsibilities and activities coordinating the election infrastructure critical infrastructure sector and its priorities for enhancing the sector's security. The report may have a classified annex.

Title I also directs the Department to perform research and development on canine detection. It is a priority for the Committee to enhance national security and transportation screening capabilities, and DHS's canine detection program has proven to be an effective method to do so. The Committee held a hearing in 2016 to examine the capabilities of the program and how canines assist in homeland security.[36] The hearing highlighted the effectiveness of the program and its ability to significantly increase DHS's capacity to detect illicit drugs, screen passengers and cargo, and provide security.[37] This Act advises on areas of research and development to canine detection and encourages coordination between public and private sectors, as well as academia.

Title II—Department of Homeland Security Acquisition Accountability and Efficiency

DHS spends billions of dollars each year on acquisitions of critical programs and systems to accomplish its mission-essential functions, and cost estimates for the Department's existing major acquisitions programs are over $180 billion.[38] The Department's acquisitions include a broad range of goods and services, from air and marine vessels for the U.S. Coast Guard and Customs and Border Protection (CBP) to secure American borders and ports to Continuous Diagnostics and Mitigation (CDM) cybersecurity tools that support

---

[34] Assessing Russian Activities and Intentions in Recent US Elections, Office of Director of National Intelligence (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[35] *Election Security, Hearing before the S. Select Comm. On Intelligence* (Mar. 21, 2018), https://www.dhs.gov/news/2018/03/21/written-testimony-dhs-senate-select-committee-intelligence-hearing-titled-election (DHS Written Testimony); DHS Statement on NBC News Coverage of Election Hacking, Feb. 12, 2018, https://www.dhs.gov/news/2018/02/12/dhs-statement-nbc-news-coverage-election-hacking.

[36] *Dogs of DHS: How Canine Programs Contribute to Homeland Security, S. Homeland Sec. & Governmental Affairs Comm.* (Mar. 3, 2016), https://www.hsgac.senate.gov/hearings/dogs-of-dhs-how-canine-programs-contribute-to-homeland-security.

[37] *Id.*

[38] See U.S. Gov't Accountability Off., *Homeland Security Acquisitions: DHS Has Strengthened Management, but Execution and Affordability Concerns Endure* (March 2016), https://www.gao.gov/assets/680/676240.pdf.

Federal agencies.[39] Component agencies are empowered to establish and execute their own acquisitions processes, while the Department Headquarters is supposed to oversee and provide guidance and frameworks for the components' acquisitions management processes as well as for Department-wide review of major acquisitions programs.[40]

As a result of combining 22 agencies—some legacy and others completely new entities—into one department to create DHS, the Department has faced a series of challenges in acquisitions management. Since 2003, acquisitions has been a primary driver of DHS's inclusion on the GAO "high risk" list, with GAO pointing to staffing, funding, requirements issues, and a lack of oversight and accountability that have resulted in increased costs, extended project timelines and execution failures in contract performance across the Department.[41]

The Department has taken a series of steps to improve its acquisition processes since its formation in attempts to address these challenges. In 2008, DHS created its Acquisition Life Cycle Framework to improve efficiency and consistency in acquisition management, and it established the Office of Program Accountability and Risk Management (PARM) in 2011 to oversee major acquisition programs and workforce, develop program management policies, and collect performance data.[42] DHS's 2013 Acquisition Management Directive 102 (MD 102) provided the framework for all Department policies and processes to manage current and future acquisitions and enterprise services.[43] DHS attempted to strengthen acquisition oversight by empowering Component Acquisition Executives (CAEs) with authority over program managers, and with the CAEs reporting to the Under Secretary for Management (USM), who under departmental policy serves with the Deputy Secretary as the ultimate acquisition decision authority within the Department.[44]

---

[39] *See* Department of Homeland Security, *Budget-in-Brief: Fiscal year 2019* (February 2019), https://www.dhs.gov/publication/fy-2019-budget-brief.

[40] Major acquisitions programs are programs with life cycle cost estimates amounting to greater than $300 million. U.S. Gov't Accountability Off., GAO-16-338SP, Homeland Security Acquisitions: DHS Has Strengthened Management, but Execution and Affordability Concerns Endure (Mar. 2016), https://www.gao.gov/assets/680/676240.pdf.

[41] *See* U.S. Gov't Accountability Off., DHS Management—High Risk Issue, https://www.gao.gov/key_issues/dhs_implementation_and_transformation/issue_summary (last visited Oct. 4, 2018); *DHS Management and Acquisition Reform: Hearing Before the S. Comm. On Homeland Sec. and Gov't Affairs*, 114th Cong. (March 16, 2016) (Statement of John Roth, Inspector General, Dep't of Homeland Sec. 1) https://www.oig.dhs.gov/assets/TM/2016/OIGtm-JR-031616.pdf, hereinafter *"DHS Management and Acquisition Reform Hearing"*; *DHS Management and Acquisition Reform Hearing* (Statement of Rebecca Gambler, Director, Homeland Security and Justice, and Michele Mackin, Director, Acquisition and Sourcing Management; U.S. Gov't Accountability Office, GAO-16-507T, Progress Made, but Work Remains in Strengthening Acquisition and Other Management Functions 16, https://www.gao.gov/assets/680/675827.pdf, hereinafter *"DHS Management and Acquisition Reform Hearing"* (Statement of GAO).

[42] *See* U.S. Gov't Accountability Off., GAO-15-292, Homeland Security Acquisitions: DHS Should Better Define Oversight Roles and Improve Program Reporting to Congress 5 (Mar. 2015), https://www.gao.gov/assets/670/668975.pdf; *DHS Management and Acquisition Reform Hearing* (Statement of GAO).

[43] *See* Dep't of Homeland Sec., Directive 102-1 (Rev 02), *Acquisition Management Directive* (February 2013), https://www.dhs.gov/sites/default/files/publications/102-01_Acquisition_Management_Directive_Rev02.pdf.

[44] *See* U.S. Gov't Accountability Off., GAO-16-338SP, Homeland Security Acquisitions: DHS Has Strengthened Management, but Execution and Affordability Concerns Endure 5 (Mar. 31, 2016), https://www.gao.gov/assets/680/676240.pdf; *DHS Management and Acquisition Reform Hearing* (Statement of GAO); U.S. Gov't Accountability Off., GAO-15-292, Homeland Security Acquisitions: DHS Should Better Define Oversight Roles and Improve Program Reporting to Congress 13 (March 2015), https://www.gao.gov/assets/670/668975.pdf.

Although DHS has taken steps to establish greater rigor and structure for the Department's acquisition activities and improve management, the Committee remains concerned by GAO's findings of inconsistent implementation of the acquisition guidance and processes across the subordinate components and resulting wasteful spending of untold billions of taxpayer dollars.[45] The Committee remains concerned that DHS continues to be beset by longstanding challenges in managing its major acquisition programs, resulting in the wasteful spending of untold billions of taxpayer dollars.

The lack of proper acquisition methodology and oversight across DHS not only has degraded the Department's ability to execute its mission, as evidenced by the SBI*net* failure, but also its basic management functions. For example, the 2017 failure of the $24.2 million Performance and Learning Management System (PALMS) set back efforts to provide Department-wide improvement in efficiency and reliability of performance and learning management processes.[46] The DHS OIG also reported in November 2017 that the Department's inadequate internal policies and competing priorities resulted in DHS failing to follow statutory requirements for using Other Transaction Authority (OTA) and reporting its use to Congress.[47] The persistent challenges DHS has faced in management of its acquisitions have been a major factor contributing to DHS's inclusion on GAO's list of high-risk agencies and programs since the Department's creation.[48]

To facilitate the Department developing a cohesive approach to acquisitions management, the Act requires DHS to provide clear written guidance on the requirements and responsibilities across DHS component agencies for it to successfully manage and hold accountable its procurement and oversight operations. In the face of the substantial issues continuing to challenge acquisition management across the Department, Title II of this Act codifies the roles and responsibilities of the key stakeholders in DHS acquisitions processes, including the Chief Financial Officer, the Chief Information Officer, and the USM of the Department. The USM is codified as the Department's Chief Acquisitions Officer, and therefore is responsible for acquisition oversight and management activities across DHS. To enable congressional oversight of the USM in fulfilling this role, the USM is required to develop and brief Congress on a multi-year acquisition strategy that will provide needed guidance to departmental components and drive strategically-oriented and agile procurement activities across DHS.

---

[45] *See* U.S. Gov't Accountability Office, GAO-15-292, Homeland Security Acquisitions: DHS Should Better Define Oversight Roles and Improve Program Reporting to Congress (Mar. 2015), https://www.gao.gov/assets/670/668975.pdf; U.S. Gov't Accountability Office, GAO-17-346SP, Homeland Security Acquisitions: Earlier Requirements Definition and Clear Documentation of Key Decisions Could Facilitate Ongoing Progress 1 (2017), http://www.gao.gov/assets/690/683977.pdf; *see also* Dana Hedgpath, *Congress Says DHS Oversaw $15 Billion in Failed Contracts*, Wash. Post (Sept. 17, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/09/16/AR2008091603200.html.

[46] *See* Off. of the Inspector Gen., Dep't of Homeland Sec., PALMS Does Not Address Department Needs 8, 11 (June 30, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-91-Jun17.pdf.

[47] *See* Off. of the Inspector Gen., Dep't of Homeland Sec., Department of Homeland Security's Use of Other Transaction Authority 1, 7-8 (November 30, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017-12/OIG-18-24-Nov17.pdf.

[48] *See* U.S. Gov't Accountability Off., GAO-17-317, Hisk-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others (Feb. 2017), https://www.gao.gov/assets/690/682765.pdf.

The Committee recognizes the need for an innovative, streamlined approach to improve acquisitions programs; however, the Department's inability to meet statutory requirements for using innovative mechanisms such as Other Transaction Authority indicate the need for enhanced oversight of these activities.[49] This legislation establishes a wide scope of authorities for DHS to test emerging acquisitions practices but also delineates a reporting mechanism to Congress regarding the departmental use and impacts of innovative acquisitions mechanisms. To further enhance responsible resource management across the Department, Title II of this Act also limits DHS in its use of acquisitions vehicles that can restrict efficient and effective acquisitions management, such as bridge contracts, and prohibits the use of cost-plus contracts for major acquisition programs. DHS may only implement a cost-type contract for a major acquisition program after issuance of a written determination that the program's complexity and difficulty in establishing program requirements necessitate the use of a cost-type contract. DHS is also required to assess and report the root causes of any instances of breaches of major acquisition programs. Ultimately, these measures will help mitigate the risk of cost overruns.

The Department's lack of a coordinated and centralized mechanism for overseeing suspension and debarment activities has contributed to inaccurate reporting and inadequate documentation of suspensions and debarments across DHS components.[50] This legislation contains a provision to ensure that DHS appropriately addresses these weaknesses through the establishment of a suspension and debarment program that integrates information and facilitates centralized oversight and transparency of related activities across all DHS components. The DHS Chief Procurement Officer is also required to establish a process for reviewing performance of contractors and to integrate such considerations of performance into contract award determination processes.

Title III—Intelligence and Information Sharing

Congress created the Department in 2002 in part to improve U.S. intelligence and information sharing to prevent another catastrophic attack like that of September 11th, 2001.[51] Since the Department's creation, threats to the homeland have evolved. New technology provides a broader reach for terrorist propaganda and secure communications that are used to facilitate plots that remain beyond the reach of law enforcement.[52] Congress has periodically

---

[49] *See* Off. of the Inspector Gen., Dep't of Homeland Sec., Department of Homeland Security's Use of Other Transaction Authority 1, 7-8 (Nov. 30, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017-12/OIG-18-24-Nov17.pdf.

[50] DHS OIG, DHS Needs to Strengthen Its Suspension and Debarment Program, (Jan. 25, 2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-01/OIG-18-41-Jan18.pdf.

[51] *See* Subtitle I of Title VIII of the Homeland Security Act of 2002, with the short title "Homeland Security Information Sharing Act," https://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf; *see also*, Gov't Accountability Office, GAO-03-715T, Homeland Security: Information Sharing Responsibilities Challenges, and Key Management Issues (May 8, 2003), *available at* https://www.gao.gov/products/GAO-03-715T.

[52] *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment: Hearing Before S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2015); *see also Threats to the Homeland: Hearing Before S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2015); *see also Fifteen Years After 9/11: Threats to the Homeland: Hearing Before S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2016); *see also Threats to the Homeland: Hearing Before S. Comm. on Homeland Sec. & Governmental Affairs*, 115th Cong. (2017).

reformed the U.S. Intelligence Community;[53] DHS's intelligence and information sharing programs require a similar update.

Congressional and watchdog oversight efforts of DHS since 2002 have identified significant weaknesses and raised questions about the role, value, and effectiveness of DHS intelligence programs.[54] For example, a bipartisan investigation conducted by the Committee's Permanent Subcommittee on Investigations reported in 2012 that Federally-supported state and local fusion centers had not provided useful intelligence to support Federal counterterrorism efforts.[55] A 2015 review of the Department's performance by the Committee's then-Ranking Member, Senator Tom Coburn, questioned the extent to which DHS is focused on its stated mission of terrorism prevention as opposed to response and recovery from terrorist acts.[56] A more recent 2016 House of Representatives Homeland Security Committee Majority review also found that DHS intelligence analysts were not familiar with component data, that data sharing within the DHS intelligence enterprise was personality-driven and limited by incompatible systems and reporting formats, and that many components felt that DHS Intelligence and Analysis (I&A) employees used the Chief Intelligence Officer's authority to dictate unreasonable Department-wide policies.[57]

A 2014 audit by GAO found that I&A products received "mixed reviews" from its customers and that the Intelligence Community was among the customers that did not value I&A products.[58] Specifically, GAO's interviews "with representatives of I&A's five customer groups indicate that customers in two groups—DHS leadership and state and local officials at fusion centers—found I&A's products to be useful, while customers in the other three groups—DHS components, the Intelligence Community, and private critical infrastructure sectors—generally did not."[59] GAO found that the Department's intelligence framework failed to establish strategic intelligence priorities.[60] Instead, DHS allowed components to drive analysis that did not lead to intelligence products that "aligned to support departmental priorities."[61]

The Department has an important role to serve within the United States Intelligence Community. It collects and owns valuable raw intelligence and data about trade, travel, border crossings, immigration, cybersecurity incidents, and financial crimes, which is unique compared to data owned by other intelligence partners.

---

[53] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 (108 Cong.) (2004); *see also* the Protect America Act of 2007, Pub. L. No. 110-55 (110 Cong.) (2007).

[54] S. Permanent Subcommittee on Investigations, Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report (Oct. 3, 2012); U.S. Government Accountability Office, GAO 14-397, DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges (June 2014).

[55] S. Permanent Subcommittee on Investigations, Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Report (Oct. 3, 2012).

[56] Tom Coburn, A Review of the Department of Homeland Security's Missions and Performance, 21 (2015), https://www.hsgac.senate.gov/download/?id=B92B8382-DBCE-403C-A08A-727F89C2BC9B.

[57] House Homeland Security Committee, Reviewing The Department Of Homeland Security's Intelligence Enterprise, House Homeland Security Committee Majority Staff Report (Dec. 2016), https://homeland.house.gov/wp-content/uploads/2016/12/Reviewing-DHS-Intelligence-Enterprise-Report.pdf

[58] Government Accountability Office, GAO 14-397, DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges (June 2014), https://www.gao.gov/assets/670/663794.pdf.

[59] *Id.* at 17.

[60] *Id.* at Highlights.

[61] *Id.*

DHS is the only Intelligence Community partner statutorily charged with sharing information and intelligence with state, local, tribal and territorial governments, and private sector partners.[62] Strengthening the DHS intelligence enterprise and better serving these customers will help the Department carry out its missions.

Title III of the Act directs the Secretary, acting through the Chief Intelligence Officer, to establish an intelligence doctrine for the Department. It requires the Secretary to prioritize the provision of expert staff who are knowledgeable about the intelligence functions of Department component programs to assist the Chief Intelligence Officer. It also codifies the existing Homeland Security Counter Threats Advisory Board to ensure ongoing Department-wide coordination. These provisions will enhance the effectiveness of the entire homeland security enterprise by addressing the long-standing challenges related to the lack of strategic priorities driving DHS component intelligence programs.

Title III authorizes current efforts to integrate component systems into a unified Homeland Security Data Framework that facilitates Department-wide sharing. It also directs the Chief Intelligence Officer to exert greater authority over the intelligence enterprise within the Department by developing and disseminating guidelines for the processing, analysis, production, and dissemination of homeland security and terrorism information within the Department. These requirements will streamline sharing within the DHS intelligence enterprise by standardizing intelligence reporting formats and ensuring component data systems are interoperable.

The Act also consolidates existing fusion center requirements and includes language that authorizes existing training to ensure fusion centers protect the privacy of U.S. persons while also providing meaningful support to Federal national security missions. It strengthens congressional oversight by requiring the Secretary to track the Federal funding provided to such centers.

Title III requires several terrorism-related threat assessments and after-action reports. This Committee heard testimony from frontline responders to terrorism that "the information gap still remains."[63] During the Committee's 2016 hearing examining how the country's first responders prepare for and respond to terrorist incidents, former Boston Police Commissioner Edward Davis recommended that the Federal Government regularly audit "the transfer of information" related to terrorist suspects and activities before attacks.[64] In response to limited information sharing prior to the 2016 Orlando nightclub attack, Chairman Johnson asked for "a thorough, independent review" of the FBI's removal of Omar Mateen from the Terrorist Screening Database.[65] This Act's terrorism reporting requirements will require DHS to provide recommendations to Congress to improve threat and information shar-

---

[62] Department of Homeland Security, *Office of Intelligence and Analysis*, https://www.dhs.gov/office-intelligence-and-analysis; and "Directorate for Information Analysis and Infrastructure Protection; Access to Information" Subtitle A of Title II of the Homeland Security Act of 2002, Pub. L. No. 107-296 (107th Cong.) (2002).

[63] *Frontline Response to Terrorism in America: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2016) (testimony of Mark S. Ghilarducci, Director, California Office of Emergency Services and the Governor's Homeland Security Advisor).

[64] *Id.* (testimony of Edward F. Davis III, Former Commissioner, Boston Police Department).

[65] Press Release, United States Senator Ron Johnson, Chairman Johnson Seeks Independent Review of Why Orlando Terrorist Was Taken Off Terror Watchlist (July 27, 2016), https://www.hsgac.senate.gov/media/majority-media/chairman-johnson-seeks-independent-review-of-why-orlando-terrorist-was-taken-off-terror-watchlist.

ing before events to better prevent terrorism.[66] The Act also requires an explanation of gaps in national security that could be addressed to prevent future acts of terrorism and recommendations for measures to address identified gaps.

This legislation also requires a report on the benefits, costs, and risks of a DHS-sponsored security clearance process for law enforcement partners to improve the Department's ability to transfer sensitive or classified information to first responders to prevent an attack.

Several other requirements of Title III aim to improve the timely sharing of threat information with law enforcement. DHS is required to develop and share a list of its secure facilities with appropriate partners to improve those partners' timely access to classified threat information. A GAO report will assess the effectiveness of, and recommend improvements for, DHS staffing to fusion centers. DHS will also be required to share information with state and local law enforcement through fusion centers about the release of incarcerated terrorists.

This Committee also suggests strengthening the Department's counternarcotics efforts through the use of the National Network of Fusion Centers.[67] As the opioid epidemic continues to pose a serious threat to the health and safety of U.S. citizens, DHS must consider ways to include fusion centers in the information sharing process. A DHS strategy will highlight ways to support law enforcement investigations and suggest best practices for fusion center participation.

Additionally, Title III requires DHS to focus on improving information sharing to counter threats from issues such as: opioid trafficking in the mail, virtual currencies, and border security vulnerabilities. A 2018 report by this Committee's Permanent Subcommittee on Investigations examined opioid trafficking in the international mail system and recommended increased information sharing about this threat.[68] The legislation requires DHS to develop a strategy for such information sharing that incorporates DHS components, the U.S. Postal Service, and other stakeholders. It also requires DHS to brief Congress on a holistic assessment of the threat presented by terrorist use of pharmaceutical-based chemicals. The briefing will include an assessment of the Government's capability to mitigate such an attack and a strategy to address any gaps in those capabilities.

To counter this threat, Title III requires DHS, with other agencies, to consider the threats posed by distributed ledger technologies. This provision was included to counter potential use of virtual currency technologies by foreign actors, terrorists, and

---

[66] Tom Coburn, A Review of the Department of Homeland Security's Missions and Performance 20 & 22 (2015), https://www.hsgac.senate.gov/download/?id=B92B8382-DBCE-403C-A08A-727F89C2BC9B.

[67] Senator Johnson suggested this role for fusion centers during the HSGAC nomination hearing for U/SIA Glawe on July 11, 2017; *see also* "Counternarcotics Officer" Section 878 of Subtitle H of Title VIII of the Homeland Security Act of 2002, Pub. L. No. 107-296 (107th Cong.) (2002).

[68] S. Permanent Subcomm. On Investigations, Staff Report, Combatting the Opioid Crisis: Exploiting Vulnerabilities in International Mail (Jan. 24, 2018), *available at* https://www.hsgac.senate.gov/imo/media/doc/Combatting%20the%20Opioid%20Crisis%20-%20Exploiting%20Vulnerabilities%20in%20International%20Mail1.pdf.

criminal organizations that turn to those tools for the perceived anonymity they offer.[69]

Title IV—Emergency Preparedness, Response, and Communications

The Homeland Security Act of 2002 authorized DHS to administer Federal homeland security grant programs to assist state and local governments and other partners to enhance the homeland security enterprise.[70] These grants focused on assisting state and local governments prepare for and respond to terrorist attacks, secure critical infrastructure, assist nonprofit organizations, and secure high-threat and high-risk urban areas.[71] The Implementing Recommendations of the 9/11 Commission Act of 2007 authorized a number of DHS grants and mandated some of their allocation methodologies.[72]

The Federal Emergency Management Agency's (FEMA) Grants Program Directorate (GPD) administers the eight preparedness (non-disaster) grant programs.[73] These programs "support our grantees develop[ment] and sustain[ment of] capabilities at the state and local, tribal, and territorial levels and in our nation's highest-risk transit systems, ports, and along our borders to prevent, protect against, respond to, recover from, and mitigate terrorism and other high-consequence disasters and emergencies."[74]

All Federal emergency management preparedness non-disaster grants are based on capability targets and capability gaps identified during the Threat and Hazard Identification and Risk Assessment (THIRA) process, and assessed in the Stakeholder Preparedness Review (SPR).[75] THIRA is a three-step common risk assessment process that assists individuals, businesses, faith-based organizations, nonprofit groups, schools and academia, and all levels of government to understand their risks and estimate capability requirements.[76] SPR is a self-assessment of a jurisdiction's current capability levels against the capability targets identified in its THIRA.[77]

The DHS OIG and the GAO have consistently identified issues with the preparedness grants, such as lack of internal oversight and metrics to show that the grants are reducing the Nation's col-

---

[69] Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle & Julia Solomon-Strauss, *Terrorist Use of Virtual Currencies: Containing the Potential Threat*, Center for New American Security (May 2017), *available at* https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-TerroristFinancing-Final.pdf.

[70] Pub. L. No. 107-296 (2002). Grant programs over time included: Nunn-Lugar-Domenici Program, Emergency Management Performance Grant Program, Homeland Security Grant Program, State Homeland Security Grant Program, Urban Area Security Initiative, Operation Stonegarden, Intercity Bus Security Grant Program, Intercity Passenger Rail Security—Amtrak Grant Program, Port Security Grant Program, Tribal Homeland Security Grant Program, and Transit Security Grant Program. *See* Cong. Research Serv., Department of Homeland Security Preparedness Grants: A Summary and Issues at 2 (Oct. 28, 2016), https://fas.org/sgp/crs/homesec/R44669.pdf.

[71] Cong. Research Serv., Department of Homeland Security Preparedness Grants: A Summary and Issues (Oct. 28, 2016), https://fas.org/sgp/crs/homesec/R44669.pdf.

[72] Pub. L. No. 110-53 (110th Cong.) (2007).

[73] FEMA, *Preparedness (Non-Disaster) Grants*, https://www.fema.gov/preparedness-non-disaster-grants (last updated Apr. 9, 2018).

[74] FEMA, *Grants*, https://www.fema.gov/grants (last updated June 14, 2018).

[75] FEMA, *Stakeholder Preparedness Review*, https://www.fema.gov/stakeholder-preparedness-review (last updated May 31, 2018).

[76] FEMA, *Threat and Hazard Identification and Risk Assessment*, http://www.fema.gov/threat-and-hazard-identification-and-risk-assessment (last updated Feb. 7, 2018).

[77] FEMA, *About the Stakeholder Preparedness Review*, http://www.fema.gov/state-preparedness-report#wcm-survey-target-id (last updated Feb. 22, 2018).

lective risk.[78] In a 2016 report to DHS, the DHS OIG determined "that FEMA had not adequately analyzed recurring recommendations to implement changes to improve its oversight of these grants. This occurred because FEMA did not clearly communicate internal roles and responsibilities and did not have policies and procedures to conduct substantive trend analyses of audit recommendations."[79] DHS OIG further determined that "because FEMA regularly waives these questioned costs, the subgrantees have no motivation to comply with basic contracting and acquisition principles, and the problem will continue to fester."[80]

In testimony before the Committee's Subcommittee on Federal Spending Oversight and Emergency Management in 2016, GAO highlighted FEMA's challenges in managing its preparedness grants.[81] For example, GAO noted coordination challenges between FEMA headquarters and regional staff in managing preparedness grants, which create inefficiencies.[82] GAO recommended that FEMA develop a plan with timeframes, goals, metrics, and milestones that target resolving longstanding challenges with its grants management model.[83]

The Urban Area Security Initiative (UASI) and State Homeland Security Grant Program (SHSGP) have been identified as examples of FEMA grant programs that would be better served by stronger performance metrics. A 2012 Committee minority staff report, *Safety at Any Price*, noted that DHS issued guidance-waiving requirements and expanded the allowable uses of certain grant programs to encourage state and local governments to use more than $8.2 billion in previously unspent grants as a stimulus package.[84] The Committee report found that "FEMA cannot demonstrate how UASI dollars (or for that matter, any other homeland security grant dollars) have helped to buy-down risk and enhance the na-

---

[78] *See e.g.* Gov't Accountability Office, GAO-16-38, Strengthening Regional Coordination Could Enhance Preparedness Efforts (2016), https://www.gao.gov/assets/680/674968.pdf; Gov't Accountability Office, GAO-12-526T, Managing Preparedness Grants and Assessing National Capabilities: Continuing Challenges Impede FEMA's Progress, (2012); Dep't of Homeland Security Office of Inspector General, OIG-16-49, Analysis of Recurring Audit Recommendations could Improve FEMA's Oversight of HSGP (2016) https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-49-Mar16.pdf.

[79] Dep't of Homeland Security Office of Inspector General, OIG-17-08, Major Management and Performance Challenges Facing the Department of Homeland Security at 6 (Nov. 2016) https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-08-Nov16.pdf.

[80] *Preparedness, Response, and Rebuilding: Lessons from the 2017 Disasters: Hearing Before the H. Comm. on Homeland Sec.*, 115th Cong. (2018) (statement of John Kelly, Acting Inspector General, Dep't of Homeland Sec. Office of Inspector General).

[81] *FEMA: Assessing Progress, Performance, and Preparedness: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs, Subcomm. On Fed. Spending Oversight & Emergency Mgmt.*, 114th Cong. (2016) (statement of Christopher Currie, Director of Emergency Management, National Preparedness, and Critical Infrastructure Protection, Homeland Security and Justice Team, U.S. Government Accountability Office) [hereinafter "FEMA Preparedness Grant Hearing"].

[82] *FEMA: Assessing Progress, Performance, and Preparedness: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2016) (statement of Christopher Currie, Director of Emergency Management, National Preparedness, and Critical Infrastructure Protection, Homeland Security and Justice Team, U.S. Government Accountability Office).

[83] *FEMA: Assessing Progress, Performance, and Preparedness: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2016) (statement of Christopher Currie, Director of Emergency Management, National Preparedness, and Critical Infrastructure Protection, Homeland Security and Justice Team, U.S. Government Accountability Office).

[84] Minority Staff Report, Sen. Tom Coburn, Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities (Dec. 2012), https://info.publicintelligence.net/SenatorCoburn-UASI.pdf.

tion's ability to prevent, respond to, or recover from manmade attacks or natural disasters." [85]

Additionally, coordination challenges among four FEMA grant programs that share similar goals and fund similar projects contribute to the risk of overlap and duplication among the grant programs.[86] GAO recommended that FEMA take steps, as it develops its new Non-Disaster Grant Management System, to collect project information with sufficient detail to identify potential duplication among its grant programs.[87]

Similarly, a lack of coordination among Federal, state, tribal, and local government agencies that transmit public alerts over the radio, television, and on their wireless devices has created challenges to effectively communicating critical messages to the American public. While FEMA—which administers the Integrated Public Alert and Warning System (IPAWS) [88] at the heart of our national emergency alert infrastructure—provides guidance to state, tribal, and local officials, it does not require them to follow common standards to participate in IPAWS. Without strong coordination, local governments widely differ on when and how to issue alerts, often adopting technology and establishing protocols that suit local needs without consideration of best practices that may help reduce the risk of issuing a false notification that could undermine the public's confidence in the emergency alert system. Coordination is a critical need because alerts pose national implications, as demonstrated by the false missile alert by the state of Hawaii in January 2018.[89]

GAO has also identified areas for improvement with FEMA's management of the THIRA process. In March 2013, GAO found that FEMA faced challenges that may call into question the usefulness of the THIRA process.[90] For example, the National Preparedness Report noted that while many programs exist to build and sustain preparedness capabilities, challenges remain in measuring their progress over time.[91] According to GAO, FEMA officials stated that the THIRA process is intended to develop a set of national capability performance requirements and measures.[92] However, GAO reported in March 2016 that such requirements and measures had not yet been developed.

Title IV of the Act authorizes the Department's existing preparedness grant programs including the UASI, SHSGP, Transit Se-

---

[85] Minority Staff Report, Sen. Tom Coburn, Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities, (Dec. 2012) https://info.publicintelligence.net/SenatorCoburn-UASI.pdf.

[86] *FEMA: Assessing Progress, Performance, and Preparedness: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2016) (statement of Christopher Currie, Director of Emergency Management, National Preparedness, and Critical Infrastructure Protection, Homeland Security and Justice Team, U.S. Government Accountability Office).

[87] *FEMA: Assessing Progress, Performance, and Preparedness: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2016) (statement of Christopher Currie, Director of Emergency Management, National Preparedness, and Critical Infrastructure Protection, Homeland Security and Justice Team, U.S. Government Accountability Office), https://www.gao.gov/assets/680/676484.pdf.

[88] Pub. L. No. 114–143 (114th Cong.) (2016).

[89] Press Release, State of Hawaii, Dep't of Defense, Emergency Management Agency (Jan. 13, 2018), *available at* https://dod.hawaii.gov/hiema/files/2018/01/20180113-NR-HI-EMA-statement-on-missile-launch-false-alarm.pdf.

[90] *AFEMA has Made Progress in Improving Grant Management and Assessing Capabilities, but Challenges Remain: Hearing Before the H. Comm. on Homeland Sec., Subcomm. On Emergency Preparedness, Response, and Communications*, 113th Cong. (2013) (statement of David Maurer, Director of Homeland Security and Justice, U.S. Government Accountability Office), https://www.gao.gov/assets/660/653122.pdf.

[91] *Id.*

[92] *Id.*

curity Grant Program, Port Security Grant Program, Operation Stonegarden, and the Non-Profit Security Grant Program. In conjunction with authorizing the grants, however, the legislation requires the creation of grants metrics to create transparency and accountability within the grant programs. The intent is to require DHS to develop effective metrics to measure the programs' effectiveness where it currently does not.

Section 1410 requires the Administrator of FEMA to develop grant metrics and assess how well specific preparedness grants are closing capability gaps, if at all. These metrics will provide FEMA and Congress with the information needed to make more prudent and targeted investments in those programs moving forward.

Additionally, Title IV's authorization of the UASI and SHSGP narrows the FEMA Administrator's previously broad discretion over what can be funded by the subject programs. This, combined with the newly created performance metrics, will ensure more prudent investment of grant funding.

To address the potential overlap and duplication created by FEMA's multiple preparedness grants and give DHS flexibility to better direct funding to critical needs and capability gaps, Section 1412 of the Act requires DHS to evaluate the merits of consolidating the preparedness grant programs and/or transferring management of the programs to another entity within DHS. The Secretary is prohibited from implementing a grant program consolidation without prior congressional approval.

To address a lack of standardization and coordination within the national emergency notification system network, Title IV requires the IPAWS subcommittee of the FEMA National Advisory Council to make recommendations on the best practices that state and local governments should follow to maintain the integrity of IPAWS. Additionally, it makes the Federal Government primarily responsible for alerting the public in the event of a missile threat.

Title V—Federal Emergency Management Agency

On April 1, 1979, President Jimmy Carter signed the executive order that created FEMA[93] after decades of *ad hoc* disaster legislation and programs.[94] Today, the centerpiece legislation for providing Federal aid for emergency and disaster relief is the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act).[95] The Stafford Act provides an emergency preparedness framework for the protection of life and property from hazards. While it confers responsibility for emergency preparedness jointly to the Federal, state, and local governments, congressional intent for response and recovery was for the Federal Government to step in only when a state has been overwhelmed.[96] The Post-Katrina Emergency Management Reform Act of 2006 (PKEMRA) provided important provisions, including the key principle that after a major disaster or emergency declaration, accelerated Federal assistance

[93] Executive Order 12127, March 31, 1979, https://www.hsdl.org/?view&did=464521.
[94] Ranking Member Tom Coburn, An Imperfect Storm, U.S. Senate Homeland Security & Governmental Affairs Committee, Table A.1, 18, *available at* https://www.hsgac.senate.gov/download/?id=5518F153-BBB6-4AFF-BCDB-F700A58479DD.
[95] Pub. L. No. 100–707 (100th Cong.) (1988).
[96] Id.

could be sent by FEMA even in the absence of a specific request by a state to save lives and prevent suffering.[97]

The 2017 hurricanes and wildfires tested the limits of the nation's disaster response capabilities.[98] In total, the Federal Government responded to 59 Federally-declared disasters and provided support through 16 emergency declarations and 62 fire assistance declarations.[99] The storms and fires affected roughly fifteen percent of the American population.[100] The Federal response to the 2017 major hurricanes—Harvey, Irma, and Maria—tested an already strained FEMA workforce, which maintained surge staffing of the National Response Coordination Center for a record 76 consecutive days.[101]

The unprecedented recovery effort that followed 2017's disasters highlighted the need to incentivize pre-disaster mitigation efforts.[102] Informed by hurricanes Harvey, Irma, and Maria, FEMA's 2018–2022 Strategic Plan focuses on moving assistance efforts toward pre-event investment and giving states and localities the personnel and training that they need to respond to any disaster.[103]

Finally, as evidenced by the false missile alert in Hawaii on January 13, 2018, public alert and warning systems carry significant ramifications if improperly managed or if state emergency management programs do not understand their levels of authority.[104]

To address these issues, Title V of the Act reauthorizes FEMA, including authorizing amounts for management and administration purposes for Fiscal Year (FY) 2018, FY 2019, and FY 2020 and makes a number of reforms. The authorization levels would set the stage to provide FEMA with consistent funding as the agency continues to respond to disasters, help communities recover after a disaster, and mitigate against future disasters.

Title V authorizes the National Domestic Preparedness Consortium (NDPC), a DHS partner providing training to emergency responders throughout the United States and its territories.[105] Originally founded as a Department of Justice program in 1998, the NDPC now partners with DHS to deliver state and local training.[106] To date, two million U.S. emergency responders have attended the 176 courses offered by NDPC. Section 1503 codifies this program and section 1504 addresses the unique training issues of rural communities by authorizing DHS to establish a rural domestic preparedness consortium.

---

[97] 6 USC § 701.

[98] Fed. Emergency Mgmt. Agency, *FEMA Reflects on Historic Year* (Dec. 29, 2017), *available at* https://www.fema.gov/news-release/2017/12/29/fema-reflects-historic-year.

[99] *Id.*

[100] *FEMA: Prioritizing a Culture of Preparedness: Hearing Before the S. Committee on Homeland Sec. & Governmental Affairs,* 115th Cong. (Apr. 11, 2018), http://www.hsgac.senate.gov/download/2018-04-11-long-testimony (statement of the Honorable Brock Long).

[101] Fed. Emergency Mgmt. Agency, *FEMA Reflects on Historic Year* (Dec. 29, 2017), *available at* https://www.fema.gov/news-release/2017/12/29/fema-reflects-historic-year.

[102] *FEMA: Prioritizing a Culture of Preparedness: Hearing Before the S. Committee on Homeland Sec. & Governmental Affairs*, 115th Cong. (Apr. 11, 2018), https://www.hsgac.senate.gov/hearings/fema-prioritizing-a-culture-of-preparedness (statement of the Honorable Brock Long).

[103] Fed. Emergency Mgmt. Agency, *2018–2022 Strategic Plan*, (2018), *available at* https://www.fema.gov/media-library-data/1521736077767-89fc0afeacb7a93bd7b6a1091aaeba2b/strat_plan.pdf pp. 21–22.

[104] Hawaii Emergency Mgmt. Agency, Press Release (Jan. 13, 2018) *available at* https://dod.hawaii.gov/hiema/files/2018/01/20180113-NR-HI-EMA-statement-on-missile-launch-false-alarm.pdf.

[105] The National Domestic Preparedness Consortium, *available at* https://www.ndpc.us/pdf/About_NDPC.pdf.

[106] *Id.*

In 2006, by executive order, the DHS Center for Faith Based and Neighborhood Partnerships (DHS Center) was created with the mission of helping emergency managers effectively engage with faith and community-based groups.[107] In 2010, the DHS Center expanded its focus to include human trafficking by becoming a founding member of the Blue Campaign, the Department's comprehensive, intra-agency approach to fighting human trafficking.[108] Section 1505 of the Act codifies this program.

For FEMA employees, it takes years of training and experience to effectively deploy FEMA's programs to state, local, tribal, territorial governments and their disaster survivors.[109] This Committee recognizes the importance and value of FEMA employees and the ability of FEMA to maintain a career ladder within the agency for retention of skilled response and recovery personnel. Section 1516 of the Act will allow the FEMA Administrator to appoint experienced personnel currently part of a temporary cadre to permanent positions in the agency. These employees will be assigned in the same manner as competitive service employees with competitive status when considered for transfer, reassignment, or promotion to such positions. To qualify for such an appointment, prospective employees must have maintained continuous service with the agency for three years prior.

Developing resilient capacity in communities prior to a disaster has proven to reduce loss of life as well as the economic disruption that occurs following a disaster.[110] By investing more in pre-disaster mitigation funding, there is potential for a greater return on investment of taxpayer dollars by decreasing the overall cost of post-disaster spending over time, while also increasing the nation's overall resiliency and catastrophic readiness.[111] The Committee supports the establishment of the National Public Infrastructure Pre-disaster Mitigation Assistance Program in Section 1519 of the Act, which will commit Federal funding to pre-disaster mitigation efforts. One hundred and eighty days after a major disaster declaration, an estimate would be made for the combined obligations of Stafford Act sections 403, 406, 407, 408, 410, and 416 grant funding;[112] consequently, an additional six percent of that estimate would be transferred from the Disaster Relief Fund (DRF) to this program for use.

As previously noted, administrative costs associated with implementing FEMA's disaster recovery programs rest in large part at

---

[107] Department of Homeland Security, *DHS Center for Faith-Based Neighborhood Partnerships, available at* https://www.dhs.gov/dhs-center-faith-based-neighborhood-partnerships (last accessed April 15, 2018).

[108] *Id*.

[109] U.S. Government Accountability Office, GAO–15–437, Federal Emergency Management Agency: Additional Planning and Data Collection Could Help Improve Workforce Management Efforts (Jul. 2015), *available at* https://www.gao.gov/assets/680/671276.pdf.

[110] *FEMA: Prioritizing a Culture of Preparedness: Hearing Before the S. Committee on Homeland Sec. & Governmental Affairs*, 115th Cong. (Apr. 11, 2018) *available at* https://www.hsgac.senate.gov/hearings/fema-prioritizing-a-culture-of-preparedness (statement of the honorable Brock Long).

[111] National Institute of Building Sciences, *Natural Hazard Mitigation Saves: 2017 Interim Report, available at* https://www.nibs.org/page/mitigationsaves (last accessed Apr. 16, 2018).

[112] Section 403 of the Stafford Act provides for Essential Assistance, Section 406 provides for Repair, Restoration, and Replacement of Damaged Facilities, Section 407 provides for Debris Removal, Section 408 provides for Federal Assistance to Individuals and Households, Section 410 provides for Unemployment Assistance, and Section 416 provides for Crisis Counseling Assistance and Training. Pub. L. No. 100–707 (100th Cong.) (1988).

the state, local, tribal and territorial level.[113] Often these costs can be substantially burdensome for the impacted entity to meet.[114] Section 1515 of the Act will increase allowable funding percentages for administrative costs, which coupled with FEMA's efforts to reduce the complexity of the disaster administrative process, will empower state, local, tribal and territorial authorities to more effectively deliver vital recovery programs to disaster survivors.

Finally, Section 1521 of the Act takes steps toward standardizing and promulgating best practices for public alert and warning systems. Additionally, due to the ramifications inherent to missile alerts and warnings, this section transfers authority to originate such warnings to the Federal Government.

Title VI—Cybersecurity and Infrastructure Security Agency

The Homeland Security Act of 2002 established DHS as responsible for leading and coordinating efforts to protect American critical infrastructure.[115] Previous administrations have worked to further define the Department's role in protecting infrastructure, such as through President George W. Bush's Homeland Security Presidential Directive (HSPD) 7 and its superseding Presidential Policy Directive (PPD) 21, issued by President Obama, which required DHS to develop policies, methodologies, and approaches to ensure the security and resilience of the sixteen critical infrastructure sectors.[116]

The National Protection and Programs Directorate (NPPD) was established within DHS in 2007 to execute functions that protect Federal agencies and critical infrastructure from physical and cyber threats and hazards.[117] NPPD is currently comprised of five divisions: the Federal Protective Service (FPS), the Office of Biometric Identity Management, the Office of Cybersecurity and Communications, the Office of Cyber and Infrastructure Analysis, and the Office of Infrastructure Protection.[118]

The scope and nature of the Department's cybersecurity mission and role within the Federal Government has evolved to correspond to the changing threat environment and growth of the Federal Government's understanding of the cyber domain.[119] This Committee and the Congress worked in the 113th and 114th Congresses to enact significant legislation empowering DHS with authorities and resources to fulfill its cybersecurity mission areas, including enhancing cybersecurity information sharing and Federal information

---

[113] Fed. Emergency Mgmt. Agency, *Memorandum For: All Regional Directors*, Jun. 2, 1993, *available at* https://www.fema.gov/media-library-data/20130726-1717-25045-4279/2_state_management_costs_for_disaster_assistance_programs.txt.

[114] *FEMA: Prioritizing a Culture of Preparedness: Hearing Before the S. Committee on Homeland Sec. & Governmental Affairs*, 115th Cong. (Apr. 11, 2018) *available at* https://www.hsgac.senate.gov/hearings/fema-prioritizing-a-culture-of-preparedness (statement of the honorable Brock Long).

[115] *See Homeland Security Act of 2002*, Pub. L. No. 107–296, Subtitle B (107th Cong.) (2002).

[116] See Homeland Security Presidential Directive (HSPD)–7, *Critical Infrastructure Identification, Prioritization, and Protection* (Dec. 17, 2003); Presidential Policy Directive (PPD)–21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013).

[117] See 6 U.S.C. § 315. *See also* 6 U.S.C. § 452 (authorizing the Secretary of the Department of Homeland Security to allocate or reallocate functions among the officers of the Department, and to establish, consolidate, alter, or discontinue organizational units within the Department).

[118] *See* U.S. Gov't Accountability Off., GAO–16–140T, National Protection and Programs Directorate: Factors to Consider when Reorganizing (Oct. 2015), https://www.gao.gov/assets/680/672944.pdf (last visited Oct. 10, 2018).

[119] *See* Homeland Security Act of 2002, Pub. L. No. 107–296, § 223, 224, and 225 (107th Cong.) (2002).

security management.[120] The Committee also enacted legislation to provide the Department with greater flexibility and resources to strengthen its cybersecurity workforce to carry out its authorities.[121]

However, past oversight of NPPD and NPPD's programs by the Committee and other independent oversight bodies like GAO have revealed challenges that limit the Directorate's ability to execute its critical missions. In September 2017, for example, GAO reported that DHS, and by extension NPPD, needs to ensure proper execution of its assigned responsibilities under the Federal Information Security Modernization Act (FISMA). Recommendations included improving coordination on the development of a plan and schedule to determine whether the security capability model established for evaluating the extent to which Federal agencies information security programs are FISMA compliant is useful and provides consistent and comparable results.[122]

Additionally, the often ineffective and inefficient implementation of NPPD's primary mechanisms for sharing and disseminating information on cyber-related incidents to Federal and non-Federal stakeholders, including private sector entities, has raised questions about the agency's ability to identify cyber-based threats, mitigate vulnerabilities and manage risks.[123] GAO reported in February 2017 that NPPD's National Cybersecurity and Communication and Integration Center (NCCIC) is not fully carrying out its statutorily required functions as mandated by the National Cybersecurity Protection Act and Cybersecurity Act.[124] In its report, GAO identified a number of programmatic impediments inhibiting the NCCIC's performance including those relating to the consolidation of entry points for receiving and logging incident data and maintaining the NCCIC's relationship with Federal and non-Federal customers.[125]

Within NPPD's Office of Infrastructure Protection, the Chemical Facility Anti-Terrorism Standards (CFATS) program has also been the subject of a number of oversight hearings relating to the improper implementation and mismanagement of the program.[126]

---

[120] *See* Congressional Research Service (CRS), *DHS's Cybersecurity Mission—An Overview* (June 2017); CRS, *Cybersecurity Legislation in the 113th and 114th Congress* (March 2017); *Cybersecurity Workforce Assessment Act*, Pub. L. No. 113–246 (113th Cong.) (2014); *Cybersecurity Enhancement Act of 2014*, Pub. L. 113–274 (114th Cong.) (2014); *Border Patrol Agent Pay Reform Act of 2014*, Pub. L. No. 113–277 (114th Cong.) (2014); *National Cybersecurity Protection Act of 2014*, Pub. L. 113–282 (114th Cong.) (2014); and *Federal Information Security Modernization Act of 2014*, Pub. L. 113–283 (114th Cong.) (2014).

[121] *Cybersecurity Act of 2015*, Pub. L. 114–113, Div. N (included the *Cybersecurity Information Sharing Act, National Cybersecurity Protection Advancement Act of 2015, Federal Cybersecurity Enhancement Act of 2015*, and the *Federal Cybersecurity Workforce Assessment Act of 2015*) (115th Cong.) (2015).

[122] *See* U.S. Gov't Accountability Off., GAO–17–549, Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices (Sept. 2017), https://www.gao.gov/products/GAO-17-549.

[123] *See* U.S. Gov't Accountability Off., GAO–16–294, DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System (Jan. 2016), https://www.gao.gov/products/GAO–16–294; U.S. Gov't Accountability Off., GAO–17–163, DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely (Feb. 2017), https://www.gao.gov/products/GAO-17-163.

[124] U.S. Gov't Accountability Off., GAO–17–163, DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely (Feb. 2017), https://www.gao.gov/products/GAO-17-163.

[125] *Id.*

[126] *Department of Homeland Security—Chemical Facility Anti-Terrorism Standards (CFACTS) Program: Hearing before the H. Comm. On Appropriations* (Sept. 20, 2012), *available at* https://appropriations.house.gov/calendar/eventsingle.aspx?EventID=303717; *Evaluating Internal Operation and Implementation of the Chemical Facility Anti-Terrorism Standards program (CFATS)*

Continued

CFATS was first authorized by Congress in 2007 to identify and regulate high-risk chemical facilities to reduce the likelihood of those chemicals being used in a terrorist attack.[127] Prior to reauthorizing the program in 2014, the Committee held a hearing and released a Majority Staff Report that examined the extent to which the CFATS regulatory regime reduced the risk that terrorists could exploit vulnerabilities at chemical facilities.[128] The report found "fundamental problems in the design, implementation and management of CFATS."[129] The report further noted that the CFATS program "focuses on the wrong threats, shifts risk to other parts of the chemical sector and supply chain, and is unable to determine if it is improving security at the facilities it regulates."[130] The 2014 CFATS reauthorization bill included a series of requirements aimed at addressing the issues highlight by the Committee and GAO.[131] The Committee continues to monitor and assess the implementation of the CFATS program, as the next deadline for reauthorization is in December 2018.[132]

FPS is responsible for protecting Federal facilities and their grounds.[133] The Department of Homeland Security Appropriations Act of 2010 transferred FPS, then within the General Services Administration, to NPPD.[134] GAO and the DHS OIG have reported extensively on FPS's longstanding human capital and operational challenges.[135] In January 2016, GAO reported that lack of coordination between GSA and FPS, agencies that share responsibility

---

by the Department of Homeland Security: Hearing before the H. Energy & Commerce Comm. (Feb. 3, 2012), *available at* https://energycommerce.house.gov/hearings/evaluating-internal-operation-and-implementation-chemical-facility-anti/; *Charting a Path Forward for the Chemical Facilities Anti-Terrorism Standards Program: Hearing before the S. Homeland Sec. & Governmental Affairs Comm.* (May 14, 2014), *available at* https://www.hsgac.senate.gov/hearings/charting-a-path-forward-for-the-chemical-facilities-anti-terrorism-standards-program; *Industry Views of the Chemical Facility Anti-Terrorism Standards Program: Hearing before the H. Cybersecurity & Infrastructure Protection Subcomm.* (Feb. 15, 2018), *available at* https://homeland.house.gov/hearing/industry-views-chemical-facility-anti-terrorism-standards-program/.

[127] Dep't of Homeland Sec., *Chemical Facility Anti-Terrorism Standards (CFATS)*, https://www.dhs.gov/chemical-facility-anti-terrorism-standards (last visited Oct. 9, 2018).

[128] *Charting a Path Forward for the Chemical Facilities Anti-Terrorism Standards Program: Hearing before the S. Homeland Sec. & Governmental Affairs Comm.* (May 14, 2014), *available at* https://www.hsgac.senate.gov/hearings/charting-a-path-forward-for-the-chemical-facilities-anti-terrorism-standards-program; Majority Staff Rept., Sen. Tom Coburn, S. Homeland Sec. & Governmental Affairs Comm., *Chemical Insecurity: An Assessment of Efforts to Secure the Nation's Chemical Facilities from Terrorist Threats* (July 2014), *abstract available at* https://www.hsdl.org/?abstract&did=762338 (copy on file with Comm.).

[129] Majority Staff Rept., Sen. Tom Coburn, S. Homeland Sec. & Governmental Affairs Comm., *Chemical Insecurity: An Assessment of Efforts to Secure the Nation's Chemical Facilities from Terrorist Threats* (July 2014), *abstract available at* https://www.hsdl.org/?abstract&did=762338 (copy on file with Comm.).

[130] *Id.*

[131] *See generally Protecting & Securing Chemical Facilities from Terrorist Attacks Act of 2014*, Pub. L. No. 113–254 (113th Cong.) (2014).

[132] *Id.*

[133] Dep't of Homeland Sec., *The Federal Protective Service*, https://www.dhs.gov/topic/federal-protective-service (last visited Oct. 9, 2018).

[134] Pub. L. No. 111–83 (2009); FPS, *Annual Report Fiscal Year 2015*, DHS 5 (2015), *available at* https://www.dhs.gov/sites/default/files/publications/Federal%20Protective%20Service%20Annual%20Report%20508%20Compliant%20FY2015.pdf; DHS, *Creation of the Department of Homeland Security*, https://www.dhs.gov/creation-department-homeland-security (last updated Sept. 24, 2015); DHS, *Secretary Napolitano Announces Transfer of Federal Protective Service to National Protection and Programs Directorate* (Oct. 29, 2009), https://www.dhs.gov/news/2009/10/29/transfer-federal-protective-service-national-protection-and-programs-directorate.

[135] Gov't Accountability Office, GAO–16–384, FPS: Enhancements to Performance Measures and Data Quality Processes Could Improve Human Capital Planning (Mar. 24, 2016), https://www.gao.gov/products/GAO-16-384; Gov't Accountability Office, GAO–16–135, FPS and GSA Should Strengthen Collaboration to Enhance Facility Security (2016), https://www.gao.gov/products/GAO-16-135; Dep't of Homeland Sec. Office of Inspector General, OIG–16–02, The FPS Vehicle Fleet is Not Managed Effectively (Oct. 2015), https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-02-Oct15.pdf.

for protecting facilities that are Federally-owned or leased, "created inefficiencies and security risks." [136]

Department leadership has cited that the current name, the "National Protection and Programs Directorate," obscures the focus of the Directorate and presents challenges for a common understanding among agency employees and stakeholders of NPPD's mission. Further, the fractured organization of NPPD hinders timely information sharing and synchronous action between cybersecurity mission-oriented personnel with physical security personnel in the Directorate.[137]

To clarify and streamline its organizational structure and mission, Title VI of this Act renames NPPD the Cybersecurity and Infrastructure Security Agency (CISA), and repositions it as an operational component agency within the Department. The purpose of this reorganization is to enable DHS to more effectively execute its existing authorities for overseeing the protection of Federal civilian agencies' networks and enhance the security of the nation's critical infrastructure assets. CISA is to be led by a Director and Deputy Director responsible for leading the Department's cybersecurity and infrastructure protection programs and ensuring cross-divisional coordination of efforts within the agency. CISA will consist of three operational divisions—the Cybersecurity Division, Infrastructure Security Division, and Emergency Communications Division—all led by Assistant Directors.

The electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) threat spans multiple critical infrastructure sectors, requiring collaboration between these multiple agencies, including DHS, Department of Energy, Department of Defense, National Oceanic Atmospheric Administration, and others. According to GAO, DHS "has the lead role in coordinating the overall federal effort to promote the security and resiliency of the nation's critical infrastructure . . . ." [138] However, GAO has also found that DHS's coordination is lacking. Specifically, it found that DHS lacks specific roles and responsibilities for addressing EMP risks; DHS has not integrated opportunities to collect risk data to inform risk assessments; DHS and DOE did not take actions to identify critical electrical infrastructure assets; and DHS and DOE, in combination with industry, did not coordinate in recognizing and executing risk management activities to address EMP threats.[139]

This legislation adds language that makes explicit the CISA Director's responsibilities for overseeing DHS's EMP and GMD planning, protection, and preparedness activities. The Act also requires DHS to comply with language passed in the National Defense Authorization Act (NDAA) of 2017, which required DHS to recommend a strategy to Congress to protect and prepare U.S. critical

---

[136] Gov't Accountability Office, GAO–16–135, FPS and GSA Should Strengthen Collaboration to Enhance Facility Security (2016), https://www.gao.gov/products/GAO-16-135.

[137] *Examining DHS's Cybersecurity Mission: Hearing before the H. Comm. on Homeland Sec., Subcomm. on Cybersecurity and Infrastructure Protection* (Oct. 2017), https://www.dhs.gov/news/2017/10/03/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-and (written statement of Jeanette Manfra).

[138] U.S. Gov't Accountability Office, GAO–18–67, Critical Infrastructure Protection: Electricity Suppliers Have Taken Actions to Address Electromagnetic Risks, and Additional Research Is Ongoing (2018), https://www.gao.gov/products/GAO-18-67.

[139] U.S. Gov't Accountability Office, GAO–16–243, Critical Infrastructure Protection: Federal Agencies Have Taken Actions to Address Electromagnetic Risks, but Opportunities Exist to Further Assess Risks and Strengthen Collaboration (2016), https://www.gao.gov/products/GAO-16-243.

infrastructure against EMPs and GMDs.[140] The 2017 NDAA also required DHS to submit a report to Congress on its progress and an estimated completion date for EMP and GMD national planning, research and development, progress on the recommended strategy, and outreach and education.[141] Both the strategy and report were due in June 2017, and as of October 2018, the Committee has yet to receive them. The Department's strategic approach to overseeing protection of critical infrastructure from EMP and GMD threats remains unclear.

To ensure CISA continues to develop and promote cyber information sharing with private sector stakeholders in accordance with the Cybersecurity Act of 2015, the Act requires the director of CISA to publicly report information on the mechanisms and structures used by the agency for stakeholder outreach and engagement.[142] This report should be updated, as appropriate, to reflect changes in the mechanisms used to share cyber information. This report would fulfill congressional mandates to enhance the quality and utilization of the information shared and disseminated by CISA with private sector entities and help resolve stakeholder engagement issues identified by GAO.

This Act also includes provisions that would streamline the agency by relocating incongruent offices. Specifically, two offices currently residing within NPPD, the Office of Biometric Identity Management and FPS, support missions far broader than the streamlined CISA mission set of cybersecurity and critical infrastructure protection. This legislation transfers the Office of Biometric Identity Management to the Management Directorate of the Department to maintain its support and coordination function across DHS component agencies and other Federal agencies. The operations and facility-oriented nature of FPS requires further review to determine its appropriate location within the Department or another executive branch agency. Within 90 days after GAO completes a review of the FPS's organizational placement within, the Act requires DHS to conduct a review and to make a recommendation for the appropriate placement for FPS within DHS or another Federal agency.

Title VII—Other Matters

When DHS was created in 2002, combining 22 existing agencies into a new Department, the original legislation maintained some of the prior congressional committees' jurisdictional responsibilities for overseeing component, offices, or programs within the Department.[143] By the Department's count, it had "congressional engagement" with 79 congressional committees or subcommittees during the 114th Congress.[144] Although this Committee supports robust and thorough oversight of the Department, having too many committees involved may actually be hurting the Department. First, di-

---

[140] NDAA of 2017, Pub. L. No. 114–328 (114th Cong.) (2016) at sec. 1913(a)(2), § 201(d)(26)(A).
[141] *Id.* at sec. 1913(a)(3), § 527(d).
[142] *Cybersecurity Act of 2015*, Pub. L. 114–113 (114th Cong.), Div. N (included the *Cybersecurity Information Sharing Act, National Cybersecurity Protection Advancement Act of 2015, Federal Cybersecurity Enhancement Act of 2015*, and the *Federal Cybersecurity Workforce Assessment Act of 2015*).
[143] Pub. L. 107–296 (107th Cong.) (2002).
[144] Information provided by the Dep't of Homeland Sec. to Committee Staff (on file with the Committee).

versified congressional jurisdiction and oversight of DHS has required the Department to dedicate significant resources to responding to inquiries and oversight requests from many congressional committees. Second, diversified congressional jurisdiction and oversight of Congress has presented a logistical and political challenge for Congress to fully reauthorize the Department along with its components and programs. This has made it more difficult for Congress to pass comprehensive authorizing language, including to address recommendations made by watchdogs, and even to make technical and conforming changes to existing Federal statute.

DHS reported that it participated in 211 hearings, providing 304 witnesses, and gave 4,157 briefings to Congress during the 114th Congress.[145] DHS reported having 1,703 engagements with 16 of the 21 standing House committees and 1,295 engagements with 16 of the 20 standing Senate committees.[146]

This Act requires a report on the resources needed to comply with congressional requests so Congress can have better information on the full scope of the resources DHS dedicates to complying with congressional engagements. It also authorizes a Commission to review congressional oversight of DHS. The Commission is required to conduct a comprehensive study and make recommendations to increase efficiency of the Department's interactions with Congress and ease the administrative burden.

In addition to establishing the Commission, Title VII of the Act makes a number of technical and conforming changes to law.

III. Legislative History

H.R. 2825 was introduced on June 8, 2017, by Representative Michael McCaul (R–TX–10) and Representative Clay Higgins (R–LA–3). The Act has eleven additional cosponsors. The Department of Homeland Security Reauthorization Act was considered under suspension of the rules and passed by the House of Representatives on July 20, 2017, by a vote of 386 to 41. The Act was received in the Senate and referred to the Committee on Homeland Security and Governmental Affairs on July 20, 2017.

The Committee considered H.R. 2825 at a business meeting on February 28, 2018, and continued its consideration on March 7, 2018. A substitute amendment as modified was offered by Chairman Ron Johnson and Ranking Member Claire McCaskill and accepted by unanimous consent.

Senator McCaskill offered McCaskill Amendment 1 as modified to adjust the authorization of appropriations levels for certain preparedness grant programs. The amendment was not adopted by a roll call vote of 7 yeas to 8 nays. Senators McCaskill, Carper, Heitkamp, Peters, Hassan, Harris and Jones voted in favor of the amendment. Senators Johnson, Portman, Paul, Lankford, and Daines voted against the amendment, and Senators McCain, Enzi and Hoeven voted against the amendment by proxy.

Senator Rand Paul offered Paul Amendment 2 as modified. The amendment provides that a Federal employee who uncovers waste at an agency and saves the agency money is eligible for a cash reward. That amendment was adopted by voice vote with Senators

[145] *Id.*
[146] *Id.*

Johnson, Portman, Paul, Lankford, Daines, McCaskill, Carper, Heitkamp, Peters, Hassan, Harris, and Jones present. Senator Carper voted "no" for the record.

Senator Steve Daines offered two amendments. Daines Amendment 1 would broaden the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 to apply to qualifying cyber incidents. Daines Amendment 4 would prohibit DHS from conducting searches or seizures of an electronic device of a U.S. person when entering the United States. Senator Daines withdrew both amendments.

Two amendments related to election security were offered by Senator Margaret Hassan and Senator James Lankford. Hassan Amendment 1 would authorize the Secretary of Homeland Security to carry out activities to assist in securing election infrastructure. Senator Hassan withdrew this amendment. Lankford Amendment 1 would designate DHS as the lead Federal agency for election security-related information sharing and require certain information sharing between DHS and other agencies as well as DHS and state election agencies and service providers. Senator Lankford withdrew this amendment.

Senator Heidi Heitkamp offered and withdrew Heitkamp Amendment 1 regarding a floodwall on a property in North Dakota.

Senator Kamala Harris offered and withdrew Harris Amendment 6, that would waive the replacement fees for passports and immigration documents destroyed during a disaster.

Senator Harris also offered Harris Amendment 7, thrice modified, that requires FEMA to establish guidelines for and conduct oversight of Operation Stonegarden grants. That amendment was adopted by voice vote with Senators Johnson, Portman, Paul, Lankford, Hoeven, McCaskill, Heitkamp, Peters, Hassan, Harris and Jones present.

Twenty-six amendments were adopted by voice vote *en bloc* with Senators Johnson, Portman, Paul, Lankford, Daines, McCaskill, Carper, Heitkamp, Peters, Hassan, Harris, and Jones. Those amendments were: Carper-Heitkamp Amendment 2 and Carper Amendment 4 as thrice modified; Daines Amendment 2 as modified and Amendment 3; Hassan Amendment 2 as modified; Harris Amendment 1 as modified, 2 as modified, 3 as amended by a Johnson Second Degree Amendment, and 4 as modified; Heitkamp Amendments 2, 3, and 4; Jones Amendment 1 as modified; McCaskill Amendment 3 as twice modified; Paul Amendment 3 as modified, 4, 6 as modified, and 10; Peters Amendment 1 as modified; and Portman Amendment 1 and 2, Portman-Carper Amendment 3 as modified, Portman-Carper Amendment 4, Portman Amendment 5 as twice modified, Portman-Hassan Amendment 6 as modified, and Portman-Hassan Amendment 7 as modified.

The Act, as amended by the substitute amendment as modified and twenty-eight amendments, was ordered reported favorably by a roll call vote of 10 yeas to 1 nays. Senators Johnson, Portman, Lankford, Hoeven, McCaskill, Heitkamp, Peters, Hassan, Harris, and Jones voted in the affirmative. Senator Paul voted in the negative. Senators McCain, Enzi, Daines and Carper were recorded for the record only as voting yea by proxy.

Consistent with Committee Rule 11, the Committee reports the Act with a technical amendment by mutual agreement of the Chairman and Ranking Member.

IV. SECTION-BY-SECTION ANALYSIS OF THE ACT, AS REPORTED

Section 1. Short title; table of contents

This section designates the title of the Act as the "Department of Homeland Security Authorization Act" and lists the table of contents.

Title I—Department of Homeland Security Headquarters

SUBTITLE A—HEADQUARTERS OPERATIONS

Section 1101. Functions and components of Headquarters of Department of Homeland Security

Subsection (1) renames the office listed under Section 112 of title 6, United States Code, through which the Secretary coordinates with non-Federal entities, to be the "Office of Partnership and Engagement." Subsection (2) authorizes the individual components of the Department's Headquarters.

Section 1102. Responsibilities and functions of Chief Privacy and FOIA Officer

This section officially names the Department's senior official responsible for privacy established in Section 142 of title 6, United States Code, as the Chief Privacy Officer. This section also expands the Chief Privacy Officer's responsibilities to include serving as the Department's Chief Freedom of Information Act (FOIA) Officer and overseeing all agency components and activities to ensure Department-wide compliance with established privacy and FOIA policies.

Section 1103. Responsibilities of Chief Financial Officer

This section clarifies and strengthens the role that the Department Chief Financial Officer (CFO) plays in leading and overseeing the integration of DHS's mission, strategic objectives and priorities, and performance against the objectives with its financial resource management. Additionally, this section establishes greater accountability of Department expenditures on conferences, requiring CFO oversight and component reports on expenditures above certain levels.

Section 1104. Chief Information Officer

Subsection (a)(1) designates the Department Chief Information Officer (CIO), with responsibilities outlined in Section 3506 of title 44, United States Code, and Section 11319 of title 40, United States Code, as an advisor to all Department leadership in any information technology-related activities. Subsection (a)(3) enhances information resource management by requiring the CIO to create and report on implementation of a strategic plan with clear metrics and resource alignments to accomplish DHS's information technology priorities. Subsection (b) requires the CIO to provide Congress with the Department software license policy required by the MEGABYTE Act of 2016 (40 U.S.C. 11302 note) and a biennial report on DHS's inventory and management of software licenses.

Subsection (c) mandates a Comptroller General Review of implementation of this section's requirements by FY 2019.

Section 1105. Quadrennial homeland security review

This section refines the approach for development of the Quadrennial Homeland Security Review (Review), required by Section 706 of the Homeland Security Act of 2002, as redesignated by this Act. DHS is required to engage with statutorily-established advisory committees on homeland security issues, implement a risk management approach in its strategic planning, and identify all resource requirements rather than purely budgetary elements in the Review. Subsection (a)(4) adjusts the annual deadline for the Review from December 31 to September 30 to better ensure integration of the findings from the review into agency strategic and budgetary planning. This subsection also requires DHS to retain records of key information leveraged in development of the Review and provide Congress information on the Department's integration of the Review's findings into its acquisitions and financial management plans.

Section 1106. Office of Strategy, Policy, and Plans

Subsection (a) abolishes the Department's Office of International Affairs and transfers its resources and functions to the Office of Strategy, Policy, and Plans.

Subsection (b) designates eleven Assistant Secretary positions for the Department, three of which require Presidential appointments and eight appointed by the Secretary. This subsection also removes the limit of twelve Assistant Secretaries established by Section 113 of title 6, United States Code, but mandates that the Department receive statutory authorization to add additional Assistant Secretary positions.

Subsection (c) authorizes the establishment of the Homeland Security Advisory Council and its role to advise the Secretary on homeland security issues.

Subsection (d) establishes the Office of Legislative Affairs within DHS and requires the Assistant Secretary for Legislative Affairs to establish a reporting structure for departmental components' communications with Congress.

Subsection (e) establishes an Office of Private Sector to advise the Secretary on private sector innovations and challenges, foster communications with industry, and assess the impact of the Department's activities and policies on the private sector.

Subsection (f) includes definitions for "assets", "functions", and "personnel".

Subsection (g) requires DHS to identify and remediate any duplicative efforts across the Department, especially in components involved in international affairs, and report to Congress on actions taken pursuant to DHS and GAO findings regarding duplicated efforts.

Section 1107. Chief Procurement Officer

This section authorizes the Chief Procurement Officer position and its role as the Department's senior procurement executive for purposes of Section 1702 of title 41, United States Code. The Chief Procurement Officer's duties include, among other things, advising

Department leadership on procurement issues, leading management of procurement policies and activities, and ensuring appropriate oversight, accountability, and compliance with statutory requirements for DHS's procurement practices. This section also provides a definition for "head of contracting activity."

Section 1108. Chief Security Officer

This section authorizes the Chief Security Officer position under DHS's USM. The Chief Security Officer's listed duties include supporting the Department in all security-related activities, including security policy management and educating the Department's workforce.

Section 1109. Office of Inspector General

This section requires the proactive and timely reporting by Department components to the Inspector General of any allegations of misconduct regarding areas under the Inspector General's authorities for investigation, unless waived by the Inspector General.

Section 1110. Office for Civil Rights and Civil Liberties

This section authorizes the Office for Civil Rights and Civil Liberties under the direction of the Chief Civil Rights and Civil Liberties Officer. The Office for Civil Rights and Civil Liberties shall advise and manage Department components in handling of equal opportunity policies, programs, and issues, and it investigates possible civil rights or civil liberty abuses. All Department components must appoint a senior level Federal employee as the Component Civil Rights and Civil Liberty Officer.

Section 1111. Science and Technology

This section clarifies the role of the Under Secretary for Science and Technology as the senior advisor to the Secretary on the Department's research and development efforts and priorities. Subsection (b) replaces the Homeland Security Advanced Research Projects Agency with the Office of the Chief Scientist, which will be led by a Chief Scientist appointed by the Under Secretary for Science and Technology who fulfills the qualification requirements of this subsection. The Chief Scientist is responsible for advancing the Department's research and development capabilities to promote revolutionary changes to homeland security technologies and must meet advanced education requirements. The DHS Secretary is authorized to leverage an experimental personnel management system and use the hiring authorities established in the Strom Thurmond National Defense Authorization Act for Fiscal year 1999 to hire personnel for the Science and Technology Directorate.

Section 1112. Department of Homeland Security Rotation Program

Subsection (a) specifies enhancements to the management, protections, and accountability of the DHS's Rotation Program. It clarifies that Rotation Program participation is not required for all DHS employees, but only for certain personnel. The subsection emphasizes the purpose of the Rotation Program, specifically to enhance cross-office integration and skills through the diversity of exposure offered by the Rotation Program. The Rotation Program is required to establish administrative procedures to ensure fair ac-

cess to information and equal opportunity for DHS employees as well as to protect the rights and competitiveness of the selected detailees during their rotation and upon their return to their home office. It also requires the establishment of an Intelligence Rotational Assignment Program under the same parameters to enhance the DHS Intelligence Enterprise employees' knowledge of other subject areas. The CHCO must also perform regular evaluations of and submit an annual report on the Homeland Security Rotation Program.

Subsection (b) requires the Secretary to provide a status report to Congress on implementation of the Department's Rotation Programs.

Section 1113. Future Years Homeland Security Program

This section amends the timeline, content, and reporting requirements of the DHS Future Years Homeland Security Program report established in Section 454 of title 6, United States Code. DHS must submit this report annually to the House Committee on Homeland Security and Senate Homeland Security and Governmental Affairs Committee within 60 days of submission of the President's budget. The report content must cover a period of five fiscal years and detail projected acquisition estimates and deployment schedules for major acquisitions for that time period. The Department must make these reports public, insofar as they do not include classified information. Classified information may be submitted to Congress in a separate document and not made public.

Section 1114. Field efficiencies plan

This section requires DHS to develop and submit to Congress within 270 days of this Act's enactment a field efficiencies plan to evaluate opportunities for consolidation and economy of resources across the Department. In the plan, DHS must review the physical infrastructure and administrative functions of its components and propose recommendations driven by cost-benefit analyses for consolidation of facility, administrative, and logistical components and functions.

Section 1115. Management

Section (a) requires DHS through FY 2023 to submit with its annual budget request information on any instances of the Secretary reprogramming or transferring funds to address unforeseen costs and address operational surges, or if any limitations on reprogramming funds affected the Secretary's ability to do so, over the previous year.

Subsection (b) codifies a senior executive services position of the Chief Facilities and Logistics Officer for the Department, responsible for overseeing management of and providing mission support services for DHS's real property, facilities, and environmental and energy programs. This subsection also requires the USM to develop and update, in consultation with the Administrator of the General Services Administration (GSA), a five-year strategy for real property management for the Department. The strategy must be geographically organized and identify opportunities for optimization and consolidation to drive better efficiencies and cost savings, and include information on the Department Headquarters consolidation

project. The Secretary must provide the regional strategies to Congress and, within its second updated strategy, report on the impacts of the strategy's implementation on the Department's operations and costs. This section also requires DHS to establish appropriate leadership and accountability within the Department to drive implementation of this plan. Components are required to identify a senior career employee to serve as regional property manager and a central point of contact, provide data to the USM on the component's real property holdings, and certify their implementation of the strategy to the USM. The Inspector General is required to review the regional real property strategies and issue findings on the effectiveness of the Department's efforts to manage its real property.

Section 1116. Report to Congress on cost savings and efficiency

This section requires DHS to submit a report on the Department's management, physical, and personnel resources and activities as well as areas identified for potential cost savings, avoidances, and efficiencies across the Department. The report must examine each components' management and administrative costs and activities, the Department's major physical assets, and the Department's workforce composition and disposition to then provide management recommendations for addressing shortcomings and enhancing efficiencies. The report must be unclassified, though the Department may also submit a classified annex.

Section 1117. Countering weapons of mass destruction office

This section establishes the CWMDO for DHS and an Assistant Secretary to oversee it. CWMDO's mission is to lead coordination and strategic policy for the Department to detect and protect against the transfer or storage of chemical, biological, radiological, and nuclear materials as well as any attack using such agents. The offices and senior executive leadership positions of the DNDO and the Office of Health Affairs are abolished by this section, and all of the aforementioned office's personnel and resources are transferred to the CWMDO. This section requires DHS to assess and report to Congress on the organization of the Department's chemical, biological, radiological, and nuclear activities to identify mission and efficiency enhancements achieved through the establishment of the CWMDO.

This section also makes the DHS Chief Medical Officer appointed by the Secretary rather than the President and reorganizes the position to sit within the CWMDO. The Chief Medical Officer's responsibilities include providing medical operational support to departmental components and coordinating with state, local, and tribal governments, DHS components, and the medical community on medical and public health matters. The DHS USM, in coordination with the Chief Medical Officer, are responsible for overseeing and coordinating the Department's workforce health and medical activities, to include establishing medical, health, veterinary, and occupational health exposure policy, strategies, and initiatives for all DHS human and animal personnel. The Chief Medical Officer will be DHS' primary point of contact with other departments and agencies, and State, local, and tribal governments. The Chief Med-

ical Officer will also coordinate the biodefense activities of the Department, as well as medical preparedness activities and training.

There is a sunset provision for all provisions within this section. On the date five years after enactment of this Act, unless reauthorized, the CWMDO and the position of Assistant Secretary for CWMDO will be abolished after transferring all functions, personnel, and assets to the DNDO and OHA.

Section 1118. Activities related to international agreements; activities related to children

This section requires DHS to consider the needs of children in homeland security policy and planning by incorporating organizations representing the needs of children into the Department's stakeholder outreach under the Office of Strategy, Policy, and Plans.

Section 1119. Canine detection research and development

This section obligates the Secretary, acting through the Under Secretary for Science and Technology, to conduct research and development of canine detection technology, which may include scientific advances, user techniques and procedures, national security policies, emerging threat protection, and training aids.

SUBTITLE B—HUMAN RESOURCES AND OTHER MATTERS

Section 1131. Chief Human Capital Officer responsibilities

This section expands the responsibilities of the DHS's CHCO to ensure workforce management within the Department measures effectiveness of strategic resource planning and is driven by industry best practices. The CHCO must also assess the resourcing requirements of the Department's mission support functions to minimize allocation of mission-critical staff to these support roles. To enhance transparency and participation Department-wide, the CHCO is also required to maintain a catalogue of development opportunities, including rotational programs, that can be easily accessed by all Department employees. In addition, the CHCO must assess the Department's efforts to recruit and retain employees in rural areas, make policy recommendations to the Secretary and Congress, and monitor significant employment contracts be developing performance measures.

Section 1132. Employee engagement and retention action plan

This section requires the Secretary, through the CHCO, to create and implement a plan annually to enhance employee engagement, retention, morale, and communications across the Department. DHS must ensure the plan integrates input from all categories and locations of Department employees as well as through a variety of feedback mechanisms, including surveys. Each departmental component is then required to develop and implement a component-specific employee engagement plan that aligns with the Department-wide plan. The components must report on the status of implementation of their engagement plans to the CHCO. The Department and components must also submit their employee engagement plans to the House and Senate homeland security commit-

tees. This section shall terminate five years after the date of enactment of this Act.

Section 1133. Report discussing Secretary's responsibilities, priorities, and an accounting of the Department's work regarding election infrastructure

This section requires the Secretary to continue to prioritize providing assistance, as appropriate, to state and local election officials. DHS must report to Congress annually on the Department's responsibilities and activities conducted coordinating the election infrastructure critical infrastructure sector and its priorities for enhancing the sector's security. The report must be unclassified but may have a classified annex.

Section 1134. Policy, guidance, training, and communication regarding law enforcement personnel

In order to streamline and modernize training for law enforcement personnel, this section requires the Secretary to assess the current training and implement a new strategic plan. The Secretary must take into account the amount of hours for training and continuing education currently provided, best practices, the technology being used, reviews and feedback about the training by law enforcement personnel, and potentially duplicative training programs. One year after enactment, the Secretary must submit a report on the progress of the strategic plan to HSGAC and the House Committee on Homeland Security. Two years after enactment, the Secretary must submit another assessment of the training programs to both committees. Finally, in the event of any Executive order or memorandum that changes law enforcement conduct policy, the Secretary must develop, implement, and publish a written plan to communicate the new policy to law enforcement and ensure they are trained accordingly. The Secretary must submit to both homeland security committees a report describing the plan and actions taken.

Section 1135. Hack DHS bug bounty pilot program

This section provides a definition for "bug bounty program," in which DHS hires and temporarily authorizes an approved individual or organization to identify and report vulnerabilities of Internet-facing information technology. The section establishes a pilot program, no later than 180 days after enactment, in which the Secretary shall award a competitive contract to an entity to manage the pilot program, designate mission-critical operations excluded from the program, and develop a process for interested entities to register for participation in the program. 180 days after the program ends, the Secretary must submit a report to both homeland security committees detailing the number of participants, the number of vulnerabilities reported, how those vulnerabilities are being remediated, and lessons learned.

Section 1136. Cost savings enhancements

This section allows the Inspector General of the DHS (DHS IG) to pay a cash award to employees other than the Secretary who save the Department money by disclosing fraud, waste, or mismanagement of surplus funds to the DHS IG. Surplus funds are

defined as funds that are not required for the purpose for which the amounts were made available or those funds that exceed the needed amounts to fully execute the purpose(s) for which those funds were made available. The cash award per employee cannot exceed the lesser of $10,000 or 1 percent of the cost savings to the Department resulting from the employee's disclosure.

After determining that the surplus funds meet the surplus fund definitional requirements, the Department's CFO is responsible for transferring the surplus funds to the general fund of the Treasury, which must use the savings for deficit reduction. However, the Department can retain up to 10 percent of the surplus savings to pay for cash awards and other Department needs. The DHS Secretary is also responsible for submitting to the Secretary of the Treasury an annual report identifying the total savings achieved during the previous fiscal year under the program. This report is due by September 30th of each fiscal year. The Secretary should also include the savings information in its budget request to the Office of Management and Budget. The Secretary of the Treasury is responsible for submitting an annual report to the House and Senate Appropriations Committees detailing the cost savings and cash awards. This provision includes a sunset provision that ends the program after six years from the date of enactment.

Section 1137. Cybersecurity research and development projects

This section directs the Under Secretary for Science to support the research and development of new cybersecurity technologies. The DHS Secretary is responsible for submitting a report detailing the new cybersecurity projects to the House Committee on Homeland Security, the House Committee on Science, Space, and Technology, and the Senate Homeland Security and Governmental Affairs Committee. The Secretary is also responsible for developing a training program for acquisitions staff involved in acquiring new cybersecurity technologies. No additional funds are authorized to implement this section.

Section 1138. Cybersecurity talent exchange

This section establishes a pilot cybersecurity talent exchange program with private sector cybersecurity firms. The program allows DHS employees to work for a cybersecurity firm in the private sector and for private sector cybersecurity experts to work as Congressional detailees at the DHS for up to four years. The Department and private sector firms each pay their respective employees while participating in the exchange program. The Secretary of the DHS must present a report on the program to congressional homeland security committees six years after the program is enacted. The program automatically terminates seven years after the enactment of this Act.

SUBTITLE C—OTHER MATTERS

Section 1141. Protection of personally identifiable information

This section amends the Tariff Act of 1930 to require CBP to remove any personally identifiable information from vessel or aircraft manifests available for public disclosure before those manifests are disclosed.

Section 1142. Technical and conforming amendments

This section makes technical amendments to the Homeland Security Act of 2002. The amendments include removing several outdated or completed reporting requirements for DHS to report to Congress on the status of key initiatives. This section also abolishes the position of Director of Shared Services and the Office of Counternarcotics at the DHS.

Title II—Department of Homeland Security Acquisition Accountability and Efficiency

Section 1201. Definitions

This section provides definitions to ensure common understanding of key acquisitions terms referenced in the acquisitions title, Title II, of this Act. This section references the statutory definition of "acquisition" established in Section 131 of title 41, United States Code, and also provides definitions for terms including "acquisition decision authority," "acquisition program baseline," "breach," "life cycle cost," and "major acquisition program."

SUBTITLE A—ACQUISITION AUTHORITIES

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

This section codifies the DHS USM as the Department's Chief Acquisitions Officer. The USM will lead the Department's acquisition oversight and maintain the authority to approve, pause, modify, or cancel major acquisition programs. This section also establishes the USM's role in overseeing Department components' acquisition activities, especially in their functional capabilities and their compliance with Department acquisition policies. Subsection (3) establishes criteria for the USM to delegate acquisition decision authority to a Component Acquisition Executive based on program life cycle cost estimates and functional maturity of component acquisition operations and leadership. This section also clarifies the role for the Under Secretary for Science and Technology in DHS acquisitions management to enable the Science and Technology Directorate to effectively support current and future acquisition requirements. The Under Secretary for Science and Technology shall work with the USM to oversee and ensure necessary operational testing, evaluation, and independent validation of technologies and systems for major acquisition programs.

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

This section requires the DHS CFO to coordinate with the USM in overseeing the Department's acquisition activities to ensure that programs will be affordable and adequately funded over their life cycle.

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

This section authorizes the DHS CIO to oversee the management of the Homeland Security Enterprise Architecture and ensure that information technology acquisitions meet all requirements of the

Department's information technology management policies and standards. The CIO is also responsible for advising the Acquisition Review Board on information technology programs and developing strategic guidance for the Department's information technology acquisitions.

Section 1214. Acquisition authorities for Program Accountability and Risk Management

This section authorizes the PARM office within the DHS Management Directorate. An Executive Director shall lead the PARM office and be responsible for overseeing implementation of Department acquisition program policy to ensure accountability for performance, reliability of data, and consistency of acquisitions operations across the Department. The Executive Director is also responsible for supporting development of an acquisitions workforce strategy and creating certification standards for Department acquisition program managers.

This section also emphasizes the requirement for all Department components to comply with existing acquisitions laws, regulations, and departmental directives. The responsibilities of the component leadership include documenting requirements, developing and verifying life cycle cost estimates, and maintaining schedules for the component's major acquisition programs.

This section establishes the responsibility for the Secretary and relevant component leadership to ensure thorough, timely, and accurate documentation of acquisition activities and requirements. DHS components must submit certain acquisition documentation to the Secretary for a quarterly report to Congress on acquisitions. The Secretary may waive this requirement on a case-by-case basis, but must report to Congress annually on the waivers it issues under this authority.

Section 1215. Acquisition innovation

This section recognizes the need for government to enable innovative approaches to streamline and improve acquisitions programs necessary for resourcing government initiatives and capabilities. The DHS USM is authorized to designate a Department lead for managing Department-wide acquisition innovation efforts. The USM is permitted to test emerging acquisitions best practices and leverage performance metrics for evaluating acquisition innovation effectiveness. DHS may also conduct industry outreach to assess the impacts of its acquisition innovation efforts on the private sector.

This section requires DHS to report to the House and Senate homeland security committees to enable congressional oversight of the effectiveness of the Department's acquisition innovation activities. The report must include information regarding testing and dissemination of emerging acquisitions best practices; the measured performance of the departmental acquisitions activities; impacts of innovative DHS acquisitions mechanisms on the private sector; and any recommendations for improving departmental acquisitions innovation.

SUBTITLE B—ACQUISITION PROGRAM MANAGEMENT DISCIPLINE

Section 1221. Acquisition Review Board

This section codifies the DHS Acquisition Review Board, chaired by the USM, which ensures accountability and consistency in review of departmental acquisitions activities and programs. The Board convenes at the discretion of the Secretary to review major acquisition programs requiring authorization to proceed through its lifecycle phases or programs in breach of its requirements. The Board shall meet regularly to maintain oversight of Department acquisitions programs and ensure appropriate scheduled progress of major acquisition programs. Responsibilities of the Board include reviewing and overseeing acquisitions to determine compliance with and fulfillment of established requirements of the set acquisition life cycle framework, overseeing alignment and implementation of individual acquisitions with Department strategic initiatives, and ensuring development of requirements in consideration of trade-offs among cost, schedule, and performance objectives.

This section also requires DHS to report to Congress following any decision by the Department to authorize a major acquisition program to proceed into the planning phase without the Department approving an acquisition program baseline. DHS must provide advanced written notice of the decision to Congress within one week of the signing of the acquisition decision memorandum and then submit the report detailing the rationale of the decision and associated action plan for establishing the baseline within 60 days of the memorandum's signature. The USM must also report annually to Congress through FY 2022 with information regarding the Board's meetings, results of acquisition program and document reviews, and efforts to implement acquisition oversight processes throughout the Department.

Section 1222. Department leadership councils

This section authorizes the Secretary to establish Department leadership councils, including a Joint Requirements Council, to assist in coordination, improve management, and reduce duplication in acquisition programs. The mission of the Joint Requirements Council is to validate joint requirements that support the Department's mission activities, ensure integration of efficiencies in management of joint requirements, and recommend prioritized capabilities for validated joint requirements. The Council shall include senior leadership representing Department components as well as a chairperson appointed by the Secretary. This section also requires the Secretary to ensure that the DHS Future Years Homeland Security Program, as amended by this Act, is consistent with the recommendations of the Joint Requirements Council.

Section 1223. Excluded party list system waivers

This section requires the Homeland Security Office of Legislative Affairs to submit to Congress notice of any waiver issued by the DHS Chief Procurement Officer or CFO permitting a Federal agency to engage in business with a contractor in the Excluded Party List System maintained by the GSA. DHS must report the waiver within five days of its issuance and explain the finding and rationale behind the USM's granting of the waiver.

Section 1224. Inspector General oversight of suspension and debarment

This section requires the Inspector General of DHS to conduct audits to identify the improper awarding of grants or contracts to a suspended or debarred entity. The Inspector General is also required to review and assess the suspension and debarment program and the criteria for Department-wide implementation.

Section 1225. Suspension and debarment program and past performance

This section codifies a suspension and debarment program within DHS and the components. It also mandates DHS institute policies to document decisions, refer suspensions or debarments to other Federal agencies, share information on contractors, and log a suspension or debarment decision in Government-wide databases. This section includes a requirement for Department or component lead procurement official to evaluate past performance reviews in solicitations. The section also provides a waiver option for the Department's Chief Procurement Officer.

SUBTITLE C—ACQUISITION PROGRAM MANAGEMENT ACCOUNTABILITY AND TRANSPARENCY

Section 1231. Congressional notification for major acquisition programs

This section establishes internal Department lines and thresholds of reporting as well as external reporting requirements to Congress in the case of a breach or a significant variance from the targeted cost or schedule of a major acquisition program. After any breach of a major acquisition program, the program manager must submit to Department leadership a root cause analysis that assesses the reasons for the shortcomings and provides a remediation plan to correct the issues. Within 30 days of the program manager's submission of the remediation plan, the USM shall report to Congress a review of the corrective actions taken pursuant to the remediation plan. If a likely cost overrun for a major acquisition program is greater than 20 percent or an anticipated delay is over 12 months from the specified acquisition program baseline, the USM is required to notify Congress. This section also provides definitions for acquisitions-related terms in this section such as "acquisition program baseline," "best practices," "breach," and "component acquisition executive."

Section 1232. Multiyear acquisition strategy

This section requires DHS to brief the appropriate congressional committees on a multiyear acquisition strategy to provide guidance and agility for the direction of the Department's acquisitions programs and activities. All updates of the acquisition strategy must be included in each annual Future Years Homeland Security Program required by this Act.

Section 1233. Report on bid protests

This section establishes a requirement for the DHS Inspector General, in consultation with GAO, to evaluate and report to Congress on the prevalence and impact of bid protests on the Depart-

ment's acquisition process. Among other things, the report must provide information including trends in bid protests filed with Federal courts and GAO, analysis and comparison of bid protests by varying criteria, an assessment of the cost and schedule impact of successful and unsuccessful bid protests, time spent preventing and responding to bid protests, and any resultant recommendations from the Inspector General.

Section 1234. Prohibition and limitations on use of cost-plus contracts

This section restricts the Department's ability to use cost-type contracts, requiring the Secretary to modify departmental acquisition regulations to only permit fixed-price type contracts for any acquisitions, including major acquisition programs. Exceptions to this prohibition are only permitted where DHS justifies in writing that the level of program risk requires use of the cost-type contract model and that the Department will take necessary steps to enable fixed-price awarding for any follow-on contracts for the same products or service. Subsection (c) authorizes the DHS Acquisition Review Board to approve the use of a cost-type contract for a major acquisition program only after generating a written determination that the Department's efforts in attempting to define requirements for a fixed-price contract for the program have been exhausted and that the program's complexity necessitates the use of a cost-type contract.

Section 1235. Bridge contracts

This section requires the DHS Chief Procurement Officer to consult with the Office of Federal Procurement Policy to develop policies and procedures to minimize the Department's use of bridge contracts and ensure appropriate planning by contracting officials. The policies must ensure sufficient time and planning to review contract requirements and establish notifications to the Chief Procurement Officer for contracts not meeting timeliness standards or that require entering into bridge contracts. The Chief Procurement Officer shall provide public notice within 30 days of entering into a bridge contract and shall report to the House and Senate homeland security committees on a common definition for bridge contract and the status of departmental use of these contracts.

Section 1236. Acquisition reports

This section requires the DHS USM to prepare and submit to Congress a semi-annual program accountability report that assesses the condition of the Department's acquisition programs. Component Acquisition Executives must also identify and report to the USM all component level 3 acquisition programs, and the component's policies and guidance regarding level 3 acquisitions. The USM is responsible for reporting to Congress that all such programs were identified and that Department components' policies comply with Department-wide guidance. DHS must also establish a repeatable process for identifying level 3 programs.

Title III—Intelligence and Information Sharing

SUBTITLE A—DEPARTMENT OF HOMELAND SECURITY INTELLIGENCE ENTERPRISE

Section 1301. Homeland intelligence doctrine

This section directs the development of Department-wide guidance on the treatment and production of homeland security and terrorism-related information and intelligence to enhance component collaboration efforts. The Secretary, through the DHS Chief Intelligence Officer, shall create and disseminate written, unclassified guidance for all Department offices and components regarding the processing, analysis, production, and dissemination of homeland security and terrorism information. For five fiscal years upon enactment of this section, the Secretary shall annually review and make any necessary revisions to the established guidance.

Section 1302. Personnel for the Chief Intelligence Officer

This section requires that DHS resource the Chief Intelligence Officer with an experienced and expert staff able to leverage an understanding of Department component programs and proficiency in intelligence functions to assist the Chief Intelligence Officer in his or her duties. This section recognizes the need for capable staff supporting the Chief Intelligence Officer role and enhancing coordination across the DHS Intelligence Enterprise.

Section 1303. Annual homeland terrorist threat assessments

This section requires that the DHS Secretary, through the Under Secretary for Intelligence and Analysis, coordinate with all Department intelligence components and programs to conduct an annual, classified assessment of the terrorist threat to the homeland for five fiscal years following the enactment of this Act. The assessment shall leverage DHS component data to the greatest extent practicable to identify emerging and persistent threats conducting or facilitating terrorism, including terrorism-related threats to critical infrastructure and Federal civilian networks. The assessment must also provide information on individuals suspected of involvement in terrorist activity who were subsequently subjected to criminal or civil proceedings or denied entry into the United States.

This section also requires the Secretary to submit an annual report to Congress detailing the status of and metrics used to evaluate DHS' anti-terrorism programs and policies. The report must include an accounting of the grants received and how they were used, DHS-sponsored training, and lessons learned. The Office of Civil Rights and Civil Liberties must also conduct an annual review to ensure that all anti-terrorism activities are respecting the privacy and civil rights and liberties of all persons.

This section also amends 6 U.S.C. 609(b)(1) to specify that grant funds may not be used to support any organization or group that has funded, engaged in, or recruited to domestic or international terrorism.

There is a sunset provision for the annual report provision: five years after enactment, the provision will be repealed.

Section 1304. Department of Homeland Security data framework

Subsection (a) directs the DHS Secretary to develop a data framework, an ongoing DHS initiative to integrate component systems and homeland security data for access by authorized Department employees to support their duties. Subsection (b) outlines qualifications for employees permitted access to the data framework and requires that the Secretary establish guidance incentivizing a duty to share information across components. Subsection (c) permits the exclusion of certain information from the data framework, such as that with the potential to compromise sources and methods or criminal investigations. Subsection (d) directs the Secretary to implement mechanisms to identify security risks and safeguard civil liberties and privacy within the data framework systems capabilities. Subsection (e) gives the Department two years to implement the data framework. Subsection (f) establishes consistent communications requirements for DHS to report progress on the data framework's implementation and highlight any use cases of data framework information assisting in the disruption of terrorist activities. Subsection (g) includes definitions for the terms "national intelligence" and "appropriate congressional committee."

Section 1305. Establishment of Insider Threat Program

This section requires the Secretary to establish an Insider Threat Program, with the goal of preventing and responding to insider threat risks to critical assets. The Secretary must also establish a Steering Committee of key DHS leadership to manage and coordinate Department activities related to insider threats to DHS critical assets. This section outlines the responsibilities of both the Chief Intelligence Officer and the Chief Security Officer to coordinate with the Steering Committee in developing a Department strategy to mitigate insider threat risk and protect critical assets. DHS is required to establish a framework for disciplining employees engaged in insider misconduct, and this section establishes punishment criteria for misconduct and procedures for an employee to appeal allegations of insider misconduct. The Steering Committee must ensure not to use authorities provided in this section to deter, detect, or mitigate lawful disclosures of information, such as those established to protect whistleblowers. Definitions for several key terms, including "critical assets", "insider misconduct", and "insider threat" are provided in this section. Additionally, the DHS Secretary must report to Congress on the Department's implementation of its insider threat risk mitigation strategy and the effectiveness of the Insider Threat Program.

Section 1306. Report on applications and threats of blockchain technology

This section requires the Secretary, in conjunction with the Secretary of the Treasury, the Attorney General, and the Director of National Intelligence, to assess the threat posed by blockchain technology, and submit a report to the Senate Committees on Armed Services; Intelligence; Banking, Housing, and Urban Affairs; and Homeland Security and Government Affairs' and the House Committees on Armed Services, Financial Services, and Homeland Security. The report must assess the potential offensive

and defensive applications of blockchain and other distributed ledger technologies, the threat posed by the use of such technology by state sponsors of terrorism, the use or planned use of the technology by the Federal government, and the vulnerability of the U.S. critical infrastructure to attacks using such technology.

This section also provides a definition for the terms "foreign terrorist organization" and "state sponsor of terrorism."

Section 1307. Transnational criminal organizations threat assessment

Subsection (a) requires the Under Secretary for Intelligence and Analysis to develop a threat assessment on whether human smuggling organizations and transnational criminal organizations are exploiting vulnerabilities in border security screening to enter the United States. Subsection (b) states that the Secretary of Homeland Security shall use this assessment to determine whether changes are needed regarding border security. Subsection (c) requires the Under Secretary to share threat information with appropriate state, local, and tribal law enforcement including officials operating within fusion centers consistent with requirements for classified information.

Section 1308. Department of Homeland Security Counter Threats Advisory Board

This section authorizes DHS to create a Counter Threats Advisory Board for the following two years after enactment of this Act and details the requirements for the Board. The Board shall consist of senior departmental component and headquarters representatives and coordinate intelligence and policy activities across DHS that relate to countering threats, such as in advising the Secretary on issuance of terrorism alerts under Section 124 of title 6, United States Code. The Under Secretary for Intelligence and Analysis shall chair the Board. The Secretary of Homeland Security, acting through the Under Secretary for Intelligence and Analysis, shall report to Congress on the status and activities of the Board within 90 days of enactment of this Act.

Section 1309. Briefing on pharmaceutical-based agent threats

This section requires the Assistant Secretary for the CWMDO, in consultation with other departments, to brief congressional committees on threats related to pharmaceutical-based agents. The briefing must assess the threats posed and the materiel and non-materiel Federal capabilities to combat such threats, and must identify a strategy to address any capability gaps. This section also provides a definition for "pharmaceutical-based agent."

SUBTITLE B—STAKEHOLDER INFORMATION SHARING

Section 1311. Department of Homeland Security Fusion Center Partnership Initiative

This section renames DHS's State, Local, and Regional Fusion Center Initiative as the "Department of Homeland Security Fusion Center Partnership Initiative". The section mandates that principal officials of fusion centers take steps to support interagency coordination and lists those required actions, such as coordination with

other heads to provide analytic intelligence advice. The Secretary shall make available criteria for sharing information and deploying personnel to support fusion centers in the National Network of Fusion Centers. In addition, the Secretary shall provide the fusion centers with training in protecting civil rights, encourage the full participation of the National Network, and track all Federal funding to each fusion center. Fusion centers along land or maritime borders shall be a priority for border intelligence efforts. Annually through 2024, the Under Secretary for Intelligence and Analysis shall report to Congress on the efforts of the Fusion Center Partnership Initiative. Within 180 days of enactment of this Act, the Comptroller General must submit a report to Congress on databases and datasets deployed to address gaps in information sharing across the National Network of Fusion Centers.

Section 1312. Fusion center personnel needs assessment

This section requires the Comptroller General to conduct an assessment of DHS personnel assigned to fusion centers, including a determination of whether additional personnel are needed to enhance the Department's mission. The assessment should account for information regarding current personnel deployments, roles and responsibilities for required positions, and general Federal resources allocated across the fusion centers. It also provides definitions for the terms "fusion center" and "National Network of Fusion Centers."

Section 1313. Strategy for fusion centers supporting counternarcotics initiatives through intelligence information sharing and analysis

The Under Secretary for Intelligence and Analysis shall submit to Congress a strategy for the fusion centers providing support to law enforcement counternarcotics investigations through intelligence information sharing and analysis. Additionally, the Under Secretary shall provide guidelines and best practices to fusion center leadership and employees to enhance their counternarcotics activities.

Section 1314. Program for State and local analyst clearances

This section establishes greater congressional oversight of DHS's efforts providing access to classified information to state, local, tribal, and territorial analysts to ensure consistency with need to know requirements established in Executive Order No. 13526 (50 U.S.C. 3161). Within two years of the enactment of this section, the Under Secretary for Intelligence and Analysis must submit a report regarding the process for determining eligibility and issuance of Top Secret clearances, the effects of provisioning clearances on information sharing with non-Federal government partners, and the risks associated with providing such clearances.

Section 1315. Information technology assessment

This section requires DHS to evaluate its information systems used to share homeland security information between the Department and the fusion centers. The assessment shall be led by the Department CIO and representatives from the National Network of Fusion Centers. The evaluation should include a review of the ac-

cessibility and ease of use of the systems by the fusion centers, an assessment of participation levels in using the information systems, and determinations of actions to improve interoperability of department information systems with those of the fusion centers.

Section 1316. Department of Homeland Security classified facility inventory

This section gives the Secretary the responsibility, to the extent practicable, to maintain an inventory of DHS facilities that are certified to house classified infrastructure of systems at the secret level or above. The Secretary must update and share the inventory with appropriate Department and non-Federal Government personnel. The inventory shall include the location of the facilities, information regarding their physical dimensions and room capacity, the entities running the facilities, and the dates they were established.

Section 1317. Terror inmate information sharing

Subsection (a) requires the Secretary, in coordination with other Federal officials when appropriate, to release information from a Federal correctional facility of individuals who may pose a terrorist threat. Subsection (b) specifies that the scope of the information shared must pertain to homeland security and regard individuals convicted of a Federal crime. Subsection (c) mandates Federal officials provide fusion centers at all levels with periodic threat assessments regarding the overall threat known from known or suspected terrorists. This includes the assessed risks of the population of their activity upon release. Subsection (e) emphasizes that this section does not require the establishment of a list of registry of individuals.

Section 1318. Annual report on Office for State and Local Law Enforcement

This section mandates that between FY 2019 and FY 2023, the Assistant Secretary for State and Local Law Enforcement shall submit a report on the activities of the Office for State and Local Law Enforcement. The report shall describe the Office's efforts to coordinate and share information with state, local, and tribal law enforcement agencies as well as their feedback on efforts. The report must also evaluate the Office's effectiveness by assessing progress against its performance metrics.

Section 1319. Annual catalog on Department of Homeland Security training, publications, programs, and services for State, local, and tribal law enforcement agencies

This section requires that the Assistant Secretary for State and Local Law Enforcement produce and make available an annual catalog that summarizes opportunities for training, publications, and services from the Department and its components available to law enforcement agencies. The Assistant Secretary shall also coordinate with DHS components and other Federal agencies to consolidate and make available information on Federal resources intended to support fusion centers.

Section 1320. Chemical, biological, radiological, and nuclear intelligence and information sharing

This section mandates that the DHS Office of Intelligence and Analysis provide intelligence analysis of terrorist actors and chemical, biological, radiological, or nuclear threats to support homeland security efforts, including in sharing information to support state, local, tribal, or other Federal agency authorities. The Office shall integrate such analysis into risk assessments of these homeland security hazards. As appropriate, the Office of Intelligence and Analysis shall coordinate efforts and information sharing with other relevant Department components, including CWMDO, and the National Counter Proliferation Center. The DHS Secretary must report annually to Congress on the Department's progress in implementing chemical, biological, radiological, and nuclear intelligence and information sharing activities specified in this section.

Section 1321. Duty to report

This section requires the Federal Government agency responsible for leading the investigation of an act of terrorism to provide an unclassified report to Congress on such act within one year after the investigation has been completed. The primary agency should collaborate with the Secretary of Homeland Security, the Attorney General, and the Director of the Federal Bureau of Investigation in generating this report. The report should include facts about the incident, an explanation of security gaps that could be addressed to prevent such acts, and any recommendations for additional measures to be taken to improve homeland security. This requirement may be waived in instances where the aforementioned parties or the head of the National Counterterrorism Center determine that such a report would jeopardize an ongoing investigation or prosecution.

Section 1322. Strategy for information sharing regarding narcotics trafficking in international mail

This section requires the Secretary, in coordination with CBP, to share counternarcotics information related to international mail, including best practices and known shippers of illegal narcotics, between DHS component, USPS, express consignment operators, and peer-to-peer payment platforms.

Section 1323. Constitutional limitations

This section ensures that all gathering and information sharing activities under this title are carried out in accordance with the Constitution.

Title VI—Emergency Preparedness, Response, and Communications

SUBTITLE A—GRANTS, TRAINING, EXERCISES, AND COORDINATION

Section 1401. Urban Area Security Initiative

This section requires states to provide relevant high-risk urban areas with an accounting of items and services purchased with funds given to the state under the UASI within 90 days of the use of the funds. This section also requires that a threat and hazard

identification risk assessment and capability assessment be conducted as a prerequisite of receiving a grant under this section.

Section 1402. State Homeland Security Grant Program

This section requires states participating in the SHSGP to conduct and submit a risk assessment of threats and hazards, including an assessment of capabilities to address the state's risk. The period of performance for grant recipients under the Program is established as no less than 36 months.

Section 1403. Grants to directly eligible tribes

This section requires that the Secretary makes the funds available from grant awards to directly eligible tribes for a period of at least 36 months.

Section 1404. Law enforcement terrorism prevention

Subsection (a) emphasizes the need for prioritization of grants under the SHSGP and UASI that enhance law enforcement terrorism prevention activities. Specifically, the Assistant Secretary for State and Local Law Enforcement must work with the FEMA Administrator to ensure that the 25 percent of grants set aside for these law enforcement purposes are in fact implemented to focus on such activities. To provide accountability to Congress on these efforts, this section requires the Administrator to report annually through FY 2022 on the use of grants for law enforcement prevention terrorism prevention activities. Subsection (b) establishes that the Office of State and Local Law Enforcement now exists within the Office of Partnership and Engagement, as established in this Act.

Section 1405. Prioritization

This section provides clarification to states and high-risk urban areas applying for grants under the UASI or the SHSGP. Applicants must use the population data requested as a consideration in its risk formula and assessment, including in accounting for population categories such as tourists, commuters, and military personnel. The FEMA Administrator is also directed to consider threat information from other relevant Federal agencies and field offices besides DHS as a consideration when allocating grants.

Section 1406. Allowable uses

This section expands the scope in which funds may be used by recipients of grants under the SHSGP and the UASI to include enhancing medical preparedness or cybersecurity. Grant recipients' expenditures on communications are also required to align with the Statewide Communication Interoperability Plan and coordinate with the appropriate interoperability governance body for their State.

Section 1407. Approval of certain equipment

This section requires the FEMA Administrator to establish and implement a review process for examining applications submitted under the SHSGP or UASI to use grants to purchase equipment or systems that do not meet national voluntary consensus standards, as established in Section 747 of title 6, United States Code. The re-

view process should consider any use of the proposed system by Federal agencies and the nature of the ability of the system to fill a critical capability gap for the applicant. Within three years of enactment of this Act, the DHS Inspector General must submit to the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs a report assessing implementation of this review process.

Section 1408. Authority for explosive ordnance disposal units to acquire new or emerging technologies and capabilities

This section authorizes the Secretary to grant an explosive ordnance disposal unit the authority to acquire technologies and capabilities that are not specified in the unit's authorized equipment allowance.

Section 1409. Memoranda of understanding

This section requires the FEMA Administrator to enter into a memorandum of understanding with certain Department component leadership to outline responsibilities regarding policy and guidance for grant decisions. This will ensure that appropriate subject matter expertise from the components is integrated into management and guidance relating to the SHSGP, UASI, Port Security Grant Program, and Transit Security Grant Program.

Section 1410. Grants metrics

This section requires the Administrator of FEMA to assess the impact of funds allocation and supported activities under the SHSGP and UASI have been used effectively to close capability gaps. The Administrator shall use information from the States and high-risk urban areas provided in their Threat and Hazard Identification and Risk Assessments and State Preparedness Reports (now known as the Stakeholder Preparedness Review by FEMA) to conduct the assessment. FEMA must provide an assessment of the data to Congress, which must include a comparison and assessment of the value of successive State Preparedness Reports and Hazard Identification and Risk Assessments. The DHS Inspector General must report to Congress with an evaluation of FEMA's assessment.

Section 1411. Grant management best practices

This section requires the Administrator of FEMA to post information on the Agency's website with a summary of findings of areas identified by the DHS OIG for improvement and methods to address the shortcomings found in grant audits. FEMA shall also make public information on innovative approaches and projects used by grant recipients from the SHSGP and UASI.

Section 1412. Prohibition on consolidation

This section mandates that the Secretary of DHS must receive authorization from Congress before implementing the National Preparedness Grant Program or any successor consolidated grant program. DHS is also required to conduct a study to determine any efficiencies and effectiveness a consolidated grant program would provide.

Section 1413. Maintenance of grant investments

This section requires grant applicants under the SHSGP or the UASI to develop a plan for the maintenance of any equipment purchased with grant funds.

Section 1414. Transit Security Grant Program

This section permits grant recipients under the Transit Security Grant Program to use funds to pay for backfill when personnel are sent to security training for a period of at least 36 months.

Section 1415. Port Security Grant Program

This section requires the Secretary to provide funding for the Port Security Grant Program's period of performance for at least 36 months.

Section 1416. Cyber preparedness

This section enhances information sharing that will contribute to management of cybersecurity risk by non-Federal government entities. The DHS National Cybersecurity and Communications Integration Center is required to share information and analysis of cybersecurity threats, vulnerabilities, and defense measures with State, local and regional fusion centers. DHS must share this information in a timely manner and in an unclassified form, whenever appropriate.

Section 1417. Operation Stonegarden

This section establishes "Operation Stonegarden," a DHS program to award grants for law enforcement agencies to enhance border security. The grant may be used to support equipment acquisition and maintenance, personnel, and border security activities. The Administrator must collect and maintain information on the Operation Stonegarden grants and establish guidelines for oversight of the program. The Administrator must also develop guidelines for financial review of the grants.

The Administrator shall, in coordination with CBP, report at least annually from FY 2018 to FY 2022 to Congress on the expenditure of grants made under Operation Stonegarden. Each report must include information on how each grant recipient expended the funds and a list of all operations carried out using Operation Stonegarden grants.

Section 1418. Non-Profit Security Grant Program

This section establishes the DHS "Non-Profit Security Grant Program" to award grants for eligible non-profit organizations to make security enhancements to protect against terrorist attacks. Eligibility for non-profit organizations is dependent upon the FEMA Administrator determining the organization to be at risk of a terrorist attack. The Administrator shall ensure that no less than 30% of the total funds appropriated under the Program are used for grants for eligible nonprofit organizations. The period of performance for this grant program is established as not less than 36 months.

Section 1419. Study of the use of grant funds for cybersecurity

This section requires the Comptroller General to determine how grant funds under the SHSGP and UASI are used in preparation

for and response to cybersecurity risks and incidents. The study must include information on obstacles and challenges in using grant funds for cybersecurity enhancement and any future plans for grant funds to support cybersecurity capabilities.

Section 1420. Joint counterterrorism awareness workshop series

This section requires the Secretary, in coordination with the Director of National Counterterrorism Center and the Director of the Federal Bureau of Investigation, to establish a Counterterrorism Awareness Workshop Series to address emerging terrorist threats and help state and locals prevent and react to terrorist attacks. The workshop series shall review existing response and interdiction plans related to terrorist attacks and identify any gaps in such plans. The series must seek to improve situational awareness and information sharing, and to provide training and exercise in the event of an attack. The officials who participate in the series must submit a report after the conclusion of the series that addresses key findings and potential mitigation strategies to address gaps that were identified. This section authorizes $1,000,000 in appropriations for each of fiscal years 2018 through 2022.

Section 1421. Exercise on terrorist and foreign fighter travel; national exercise program

The Secretary shall develop and conduct an exercise to test capabilities and responsiveness to the terrorist and foreign fighter threat. The exercise shall include a scenario involving persons traveling to the United States to join a terrorist organization or terrorists infiltrating into the United States, and the exercise must include coordination with relevant Federal agencies and other key stakeholders. The Emerging Threats in the National Exercise Program will include exercises addressing emerging terrorist threats. No additional funds are authorized to carry out the requirements of this section.

Section 1422. Grants accountability

This section permits the Inspector General, in his or her oversight of grants provided by the Department, to examine any records of its subcontractors or any agency in receipt of any grant awarded. The Inspector General may also interview any employee of the grantee regarding transactions relating to the contract. The Administrator or the Secretary shall provide a user-friendly means for grant recipients to comply with all reporting requirements. Five years after the date on which grants funds are distributed under a covered grant, the authority of a covered grant recipient is terminated. Upon the termination of this authority, any grant amounts that have not been expended shall return to the Administrator.

SUBTITLE B—COMMUNICATIONS

Section 1431. Responsibilities of Assistant Director for Emergency Communications

This section makes technical amendments to the responsibilities of the Assistant Director for Emergency Communications. It also expands the responsibilities of the Director to include assessing the

impact of emerging technologies on interoperable emergency communications.

Section 1432. Annual reporting on activities of the Emergency Communications Division

This section requires the Assistant Director for Emergency Communications to report annually to Congress on the activities of the Office, including on outreach efforts to State, regional, local and tribal governments. Outreach efforts by the Emergency Communications Division to support interoperable communications by local governments and public safety agencies.

Section 1433. National Emergency Communications Plan

This section requires the DHS Secretary in conjunction with the Director for Emergency Communications, to update the National Emergency Communications Plan at least every five years. DHS shall also, in its updates of the Communications Plan, consider the impact of emerging technologies on the ability to achieve emergency communication interoperability.

Section 1434. Technical edit

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

Section 1435. Communications training

This section requires the USM of DHS to develop a mechanism to verify that radio users within the Department receive initial and ongoing training on the use of the radio systems.

SUBTITLE C—OTHER MATTERS

Section 1451. Technical and conforming amendments

This section makes technical amendments to the Homeland Security Act of 2002 regarding the content of Title IV of this Act. The section also defines the term "Nuclear Incident Response Team."

Title V—Federal Emergency Management Agency

Section 1501. Short title

This section states that this division may be cited as the "FEMA Reauthorization Act of 2018."

Section 1502. Reauthorization of Federal Emergency Management Agency

This section authorizes appropriations for FEMA as follows: $1,049,000,000 for FY 2018; $1,065,784,000 for FY 2019; and $1,082,836,544 for FY 2020.

Section 1503. National Domestic Preparedness Consortium

This section authorizes the NDPC, as established under FEMA in Section 1102 of title 6, United States Code, to facilitate visibility, creation, validation, and delivery of training to emergency response providers. The Consortium is required to ensure whenever possible that the training it provides for emergency responders simulate real response environments. For the Center for Domestic Preparedness, this section authorizes the following appropriations:

$63,939,000 for FY 2018; $64,962,024 for FY 2019; and $66,001,416 for FY 2020. For the members of the Consortium, as established in Section 1102 of title 6, United States Code, this section authorizes the following appropriations: $101,000,000 for FY 2018; $102,606,000 for FY 2019; and $104,247,856 for FY 2020. This section also amends the savings provision in statute for the Department to protect emergency preparedness spending for five of the seven Consortium members, requiring the Secretary to ensure that future amounts provided to these entities meet or exceed their provisions in FY 2015.

Section 1504. Rural Domestic Preparedness Consortium

This section authorizes FEMA's Rural Domestic Preparedness Consortium, which consists of universities and non-profit organizations qualified to train emergency response providers in rural communities. The Rural Domestic Preparedness Consortium develops, tests, and provides training for emergency response providers of rural communities. This section authorizes the Consortium $5,000,000 of any appropriations for Continuing Training Grants.

Section 1505. Center for Faith-Based and Neighborhood Partnerships

This section codifies the Center for Faith-Based and Neighborhood Partnerships. The Center leads outreach efforts between faith-based and community organizations and DHS security and emergency response efforts. The Director of the Center, appointed by the Secretary of DHS, is responsible for developing exercises and providing guidance to engage faith-based and community organizations in enhancing their hazard and emergency response capabilities, including in how to secure their facilities and in combating human trafficking.

Section 1506. Emergency support functions

This section enhances readiness and accountability in the development and implementation of the National Response Framework. FEMA must update the National Response Framework, as required in Section 314 of title 6, United States Code, at least every five years. Additionally, the President is required to work through the Administrator of FEMA to establish performance metrics for Federal entities with key responsibilities under the Framework's emergency support functions.

Section 1507. Review of National Incident Management System

This section amends the requirement for the FEMA Administrator to "periodically" review the National Incident Management System, pursuant to Section 314 of title 6, United States Code, by mandating a review be conducted no less than every five years. This will help ensure consistent review by leadership and stakeholders as well as help ensure readiness of national emergency response capabilities.

Section 1508. Remedial action management program

This section requires the FEMA Administrator to coordinate with the National Council on Disability and the National Advisory Council to establish a remedial action management program. The

FEMA Administrator is required to work with other Federal agencies to use the program to learn from corrective actions identified during exercises or real-world events responding to natural or man-made disasters or emergency situations, including terrorism response. FEMA is required to report annually for five years on Federal agency corrective actions and their progress. FEMA must also, whenever possible, provide participants in simulated or real-world emergency responses after-action reports highlighting lessons learned and corrective actions.

Section 1509. Center for Domestic Preparedness

This section requires FEMA to develop an implementation plan to address findings from the 2017 Management Review Team's report on live agent training at the Chemical, Ordnance, Biological, and Radiological Training Facility at the Center for Domestic Preparedness. The review examined the circumstances surrounding the discovery that the training facility was unknowingly using a highly toxic strain of ricin, ricin holotoxin, rather than the less toxic strain, ricin A-chain, it had intended to use for training. The Administrator must provide Congress updates with information on the plan's implementation efforts to address the Management Review Team's recommendations to prevent such an incident from occurring in the future.

Section 1510. FEMA Senior Law Enforcement Advisor

This section codifies the position of Senior Law Enforcement Advisor at FEMA, which shall be appointed by the FEMA Administrator and serve as an expert advisor to strengthen FEMA's coordination with law enforcement entities. The section mandates that the Advisor possess requisite qualifying experience in law enforcement, intelligence, information sharing, and emergency response. The Advisor's responsibilities include coordinating with and ensuring adequate consideration of state, local, and tribal law enforcement in efforts to protect against and respond to natural and man-made disasters and acts of terrorism.

Section 1511. Technical expert authorized

This section codifies FEMA's Children's Technical Expert, responsible for understanding and integrating the needs of children into FEMA's emergency response activities. This expert, appointed by the Administrator of FEMA, shall ensure adequate representation and consideration of the unique needs of children in Agency initiatives, consistent with the requirement for the Department Office of Strategy, Policy, and Plans to consider children's needs established in Section 1120 of this Act.

Section 1512. Mission support

This section requires the Administrator of FEMA to designate a chief management official to serve as the principal advisor to the Administrator on management issues and activities, including emergency management operations and programs. The chief management official shall support the Administrator's management of five management lines of business: procurement, human resources, information technology and communications, real property, and security. In this role, the chief management official shall assist in de-

velopment and implementation of management controls to enhance oversight and improve operations of FEMA. This section also clarifies that the roles of the chief management official in no way affect the responsibilities of the Assistant Administrator for National Continuity Programs if the issues relate to weather emergency operations-affiliated facilities. The Administrator is also required to report to Congress within 270 of enactment of this Act with a review of key management functions of the FEMA headquarters and regional offices as well as a strategy to capture data related to the management functions.

Section 1513. Strategic human capital plan

This section reinstates a requirement from the Post Katrina Emergency Management Reform Act of 2006 (5 U.S.C. 10102(c)) that required the Administrator of FEMA to develop and submit to Congress a strategic human capital plan for improving FEMA's workforce. The plan must include a workforce gap analysis assessing required and current competencies, a plan of action for addressing any gaps in critical skills, performance metrics, and an assessment of the Agency's Surge Capacity Force workforce. The report is due no later than May 1, 2018, and resubmitted annually for the subsequent five years with updates on implementation status.

Section 1514. Office of Disability Integration and Coordination of Department of Homeland Security

This section codifies the Office of Disability Integration and Coordination (ODIC) within FEMA, which is responsible for ensuring integration of needs of and communication with individuals with disabilities and any special access or functional needs into emergency management activities. The Office shall have a Director, responsible for establishing guidance on matters related to individuals with disabilities in emergency planning and response efforts and overseeing integration of the Office's mission across the FEMA regional offices. The Director must also coordinate with key stakeholders, including organizations representing individuals with disabilities, to collaborate on issues regarding access and functional needs during emergencies and integrate them in Agency emergency response planning and activities. The Administrator of FEMA shall submit a report to Congress within 120 days of enactment of this Act regarding the funding and staffing needs of the ODIC.

Section 1515. Management costs

This section establishes fixed rates for the FEMA Administrator to reimburse states and local governments to cover both direct and indirect costs of administrating the disaster recovery projects. Reimbursement under hazard mitigation (Section 403 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act) is set as no more than 15 percent of the total amount of the grant award. Reimbursement under essential assistance, repair and replacement of damaged facilities, debris removal, or transportation assistance (Sections 403, 406, 407, and 507 of the Stafford Act, respectively) will not total more than 12 percent of the total award.

Section 1516. Performance of services

The FEMA Administrator may appoint temporary personnel who have served continuously for three years to positions in FEMA in the same manner as competitive service employees. If appointed under this subsection, a person shall become a career-conditional employee.

Section 1517. Study to streamline and consolidate information collection

The FEMA Administrator shall conduct a study and develop a plan with the goal of making the collection of information from disaster assistance application and grantees more streamlined, efficient, and less duplicative. FEMA shall coordinate with the Small Business Administration and the Department of Housing and Urban Development to develop and provide to Congress a plan to regularly collect and report on information on Federal disaster assistance awarded.

Section 1518. Agency accountability

This section enhances the transparency and accountability of disaster relief resource allocation. The FEMA Administrator must publish on FEMA's website specifics of any public assistance grant award, and mission assignment regarding a major disaster, or any contract amounting to over $1,000,000. The information provided in these reports will provide public visibility on the nature and impact of spending on disaster relief efforts. The Administrator shall also publish a monthly disaster relief report with information regarding resources used in support of disaster relief, including the amount of obligations for non-catastrophic events, as well as a description of FEMA's methodology in development of the report.

Section 1519. National public infrastructure predisaster hazard mitigation

This section expands the scope of the President's ability to use funds from the National Predisaster Mitigation Fund to include carrying out enforcement activities to implement the latest standards for design, construction, and maintenance of eligible residential facilities. The President is also permitted to withdraw amounts of financial assistance made available to a state that remain unobligated three years after funds were initially allocated. To be eligible for this financial assistance from the President, states must have received a major disaster declaration during the previous seven-year period. This section also allows the President to set aside an additional investment of up to six percent of the estimated aggregate of specified assistance grants to provide technical and financial assistance for national public infrastructure predisaster mitigation.

The Administrator must also submit a report to Congress detailing the implications of the above additional use of the National Predisaster Fund and the redistribution of unobligated state funds. The report must include a justification, cost-benefit analysis, and assessment of the stress placed on the Disaster Relief Fund by the extra spending. In addition, the report must provide an expenditure plan and an assessment of how to allocate the funds to mitigate risks to the most costly disaster impacts.

Section 1520. Technical amendments to national emergency management

This section makes a number of technical changes to the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.) in language regarding the functions, responsibilities, and requirements of FEMA and related activities for emergency management. Subsection (a)(3) amends language about types of disasters to which FEMA responds to include incidents that impact critical infrastructure. This subsection also adds a requirement for the FEMA Administrator to develop integrated frameworks that incorporate existing Government plans addressing various aspects of emergency planning and response.

Section 1521. Integrated public alert and warning system subcommittee

This section adds to the list of recommendations made by the Integrated Public Alert Subcommittee of the National Advisory council to include recommendations for best practices of State, tribal, and local government officials to authenticate civil emergencies and initiate, modify, and cancel alerts. It also requires the Subcommittee to submit a second report to Congress detailing the recommendations described above. The termination of the Subcommittee is amended to five years after enactment, instead of three.

The Administrator shall consider the Subcommittee recommendations and establish minimum requirements for State, tribal, and local government participation in the Integrated Public Alert and Warning System. The Administrator must also establish a process to ensure the incident management and warning tools used by those governments meet the established minimum requirements. In addition, the Administrator must ensure that the memoranda of understanding between the Agency and those governments ensure compliance with the minimum requirements.

This section also places the authority to use the public alert and warning system to warn the public of a missile launch with the Federal Government, but allows the Secretary to delegate that authority to a State, tribal, or local entity after submitting a report to Congress explaining that the delegation is either more feasible or in the national security interest. The section also authorizes the President, upon verification of a missile threat, to alert the public of the threat.

The Secretary is also required to establish a process to notify a State warning point of follow-up actions to a missile launch alert and work with the Governor of a State warning point to implement responsive action plans. The Secretary shall also report to Congress on the feasibility of establishing an alert designation that would concurrently alert the public and a State warning point of a missile threat. No later than one year after enactment, the Administrator must review the Emergency Operations Center of the Agency, the National Watch Center, and each Regional Watch Center of the Agency, and submit a report to Congress.

This section also provides a definition for "public alert and warning system."

Title VI—Cybersecurity and Infrastructure

Section 1601. Cybersecurity and Infrastructure Security Agency

This section renames and reorganizes the DHS National Protection and Programs Directorate to be the new CISA, headed by a Director of Cybersecurity and Infrastructure Security. This section establishes the roles and responsibilities of CISA's leadership as well as the functions and responsibilities of CISA's three divisions: the Cybersecurity Division, the Infrastructure Security Division, and the Emergency Communications Division.

The CISA Director is responsible for leading cybersecurity and critical infrastructure protection operations and policy for the CISA and coordinating with appropriate stakeholders to carry out the CISA's mission. A Deputy Director of Cybersecurity and Infrastructure Security shall assist the Director in management of the CISA's duties and activities. This section empowers the DHS Secretary to receive and analyze law enforcement information and intelligence from government and private sector entities to assess threats against and vulnerabilities of the United States homeland. The Secretary may, after notifying Congress, reallocate the functions established for CISA in this title.

This section also establishes several reporting requirements to enhance congressional oversight of the newly-established CISA. CISA must report to Congress on its activities and the improved operations of the functions previously established for the National Protection and Program Directorate after being reorganized under the CISA. CISA must also report annually to Congress on threats and activities relating to electromagnetic pulses and geomagnetic disturbances, and the DHS cybersecurity workforce.

Section 1602. Transfer of other entities

This section transfers the Office of Biometric Identity Management under the Department's Management Directorate. Within 90 days of GAO completing its review of the Federal Protective Service's organization placement, The DHS Secretary must submit to Congress and the Office of Management and Budget a recommendation regarding an appropriate placement in the executive branch for the Federal Protective Service.

Section 1603. DHS report on cloud-based cybersecurity

This section requires DHS to coordinate with the Office of Management and Budget and GSA to create and submit to Congress a report on the Department's role in cloud-based cybersecurity deployments for civilian Federal departments and agencies. This report will include information on the Department's plan for offering software-based Security Operations Center as a service (SOC-as-a-Service) capabilities. DHS must also discuss how the Department will adapt capabilities of its key cybersecurity programs, including the CDM Program and the intrusion detection and prevention system, to cloud environments.

Section 1604. Rule of construction

This section establishes that nothing within Title VI of the Act may be construed as endowing the DHS Secretary with new au-

thorities or limiting the statutory authority of any other Federal agency.

Section 1605. Prohibition on additional funding

This section states that no additional funds are authorized for appropriation to carry out the provisions of this title in establishing the CISA.

Title VII—Other Matters

SUBTITLE A—MISCELLANEOUS

Section 1701. Authorization of appropriations for Office of Inspector General

This section authorizes an appropriation of $175 million to the DHS OIG for each of FYs 2018 and 2019.

Section 1702. Canine teams

This section authorizes DHS components to request additional canine teams for the drug detection mission at the border if needed.

Section 1703. Report on resource requirements to respond to congressional requests

This section requires the DHS Secretary to report annually to Congress on requests made by Congress to the Department over the preceding five fiscal years. The report shall include information such as numbers of requests, breakdowns of requests by Congressional entity, and information on requests for duplicative briefings. The report must also include the number of written testimony and reports the Department had to prepare, a list of congressional document requests and subpoenas, a list of congressional questions for the record, and a list of congressional letter requests for information. DHS must submit this report to Congress for the next five years after passage of the Act.

Section 1704. Report on cooperation with the People's Republic of China to combat illicit opioid shipments

This section requires the DHS Secretary to submit a report to Congress on the current and future plans to work with Chinese government to reduce the flow of opioids from China to America. The report must be delivered within 90 days after the enactment of this Act.

SUBTITLE B—COMMISSION TO REVIEW THE CONGRESSIONAL OVERSIGHT OF THE DEPARTMENT OF HOMELAND SECURITY

Section 1711. Short title

This section establishes that this subtitle may be cited as the "Congressional Commission to Review the Congressional Oversight of the Department of Homeland Security Act of 2018."

Section 1712. Establishment

This section establishes a legislative branch commission called the "Congressional Commission to Review Congressional Oversight of the Department of Homeland Security."

Section 1713. Members of the Commission

This section establishes the membership composition of the Commission to be six members appointed within 45 days of enactment of this Act: two appointed by the Senate majority, two by the Senate minority, and one each by the House majority and minority. Commission members shall have expertise in homeland security and have prior senior leadership experience in the executive or legislative branches. Each member shall be appointed for the duration of the Commission, and shall not receive compensation. The appropriate Federal agencies shall cooperate with the Commission to expedite providing the members appropriate security clearances to the extent possible.

Sec 1714. Duties of the Commission

This section outlines the Commission's duties. The Commission shall conduct a comprehensive study of the Department of Homeland Security, to include congressional oversight of the Department, in order to make recommendations on how committee jurisdictions in Congress could be modified to promote the mission of the agency and more effective oversight. If at least four members of the Commission vote in approval, the Commission shall submit to the President and Congress a statements of its findings based on the study as well as recommendations for legislation to remedy the issues presented.

Section 1715. Operation and powers of the Commission

This section requires the heads of relevant executive branch agencies must consult with the Commission on matters within their respective areas of responsibility. The Commission shall meet within 30 days after the date on which the majority of the members are appointed and at the call of the chairperson. This section also requires the chairperson and vice chairperson to establish written rules of procedure, hold hearings, and may contract with government and private agencies for any purpose necessary to carry out its mission.

Sec 1716. Funding

This section permits the chairperson of the Commission to receive a transfer from the Department of up to $1,000,000 to carry out its duties. The amounts transferred shall remain available until the Commission is terminated.

Sec 1717. Personnel

This section requires the designation of an Executive Director for the Congressional Commission to Review Congressional Oversight of the Department of Homeland Security. The Executive Director shall be appointed by the chairperson and the vice chairperson and may appoint additional staff as they consider appropriate. Additionally, this section authorizes any Federal Government employee may be detailed to the Commission.

Sec 1718. Termination

This section establishes the termination date of the Congressional Commission to Review Congressional Oversight of the De-

partment of Homeland Security to be not later than 12 months after the date of enactment of this Act.

SUBTITLE C—TECHNICAL AND CONFORMING AMENDMENTS

Section 1731. Technical amendments to the Homeland Security Act of 2002

This section makes technical amendments to the Homeland Security Act of 2002 to integrate changes from this title.

V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this Act and determined that the Act will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the Act contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, April 26, 2018.

Hon. RON JOHNSON,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2825, the DHS Authorization Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz.

Sincerely,

KEITH HALL,
Director.

Enclosure.

H.R. 2825—DHS Authorization Act

Summary: H.R. 2825 would authorize the appropriation of nearly $2.7 billion over the 2019–2023 period for programs in the Department of Homeland Security (DHS), mostly for activities carried out by the Federal Emergency Management Agency (FEMA). In addition, CBO estimates, the act would effectively authorize the appropriation of about $1.2 billion over the five-year period, mostly for other FEMA programs.

Assuming appropriation of the authorized and estimated amounts, CBO estimates that implementing H.R. 2825 would cost about $3.2 billion over the 2019–2023 period. Enacting the legislation would affect direct spending; therefore, pay-as-you-go procedures apply. However, we estimate that those effects would be insignificant in each year. The act would not affect revenues.

CBO estimates that enacting H.R. 2825 would not significantly increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

H.R. 2825 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA).

Estimated cost to the Federal Government: The estimated budgetary effect of H.R. 2825 is shown in the following table. The costs of the legislation fall within budget functions 450 (community and regional development), 500 (education, training, employment, and social services), and 750 (administration of justice).

	By fiscal year, in millions of dollars—						
	2018	2019	2020	2021	2022	2023	2019–2023
INCREASES IN SPENDING SUBJECT TO APPROPRIATION							
FEMA Programs:							
Authorization Level	1,215	1,235	1,254	1	1	0	2,491
Estimated Outlays	0	652	1,008	492	182	73	2,407
DHS Inspector General:							
Authorization Level	175	175	0	0	0	0	175
Estimated Outlays	0	158	18	0	0	0	175
Congressional Commission:							
Estimated Authorization Level	0	1	0	0	0	0	1
Estimated Outlays	0	1	0	0	0	0	1
Other FEMA Programs:							
Estimated Authorization Level	0	192	196	200	205	209	1,002
Estimated Outlays	0	13	42	82	128	173	438
FEMA Predisaster Hazard Mitigation Program:							
Estimated Authorization Level	0	120	24	24	24	24	216
Estimated Outlays	0	6	25	54	40	32	157
Reports:							
Estimated Authorization Level	0	9	3	3	3	3	20
Estimated Outlays	0	8	3	3	3	3	20
Total Changes:							
Estimated Authorization Level	1,390	1,732	1,477	228	233	236	3,906
Estimated Outlays	0	838	1,097	631	352	281	3,199

Components may not sum to totals because of rounding; DHS = Department of Homeland Security; FEMA = Federal Emergency Management Agency.

The act would authorize the appropriation of $1,390 million for 2018. CBO does not estimate any outlays for those authorizations because appropriations for 2018 have already been provided.

CBO estimates that enacting H.R. 2825 would increase direct spending by less than $500,000 over the 2019–2028 period.

Basis of estimate: For this estimate, CBO assumes that H.R. 2825 will be enacted near the end of fiscal year 2018. H.R. 2825 would authorize appropriations totaling $1.39 billion for fiscal year 2018. CBO does not estimate outlays for the 2018 authorizations because appropriations for 2018 have already been provided.

CBO estimates that implementing H.R. 2825 would cost about $3.2 billion over the 2019–2023 period. For this estimate, CBO assumes that the authorized and estimated amounts will be provided each year beginning in 2019 and that spending will follow historical patterns.

Programs with specified authorizations

H.R. 2825 would authorize the appropriation of nearly $2.7 billion over the 2019–2023 period for programs in DHS, mostly for activities carried out by FEMA.

FEMA Programs. Titles V and VI of H.R. 2825 would authorize a total of about $2.5 billion in fiscal years 2019 and 2020 for the management and administration of FEMA.

The legislation would specifically authorize the following annual appropriations:

- About $1.1 billion through 2020 for overall FEMA management and administration,
- About $165 million through 2020 in grants to the National Domestic Preparedness Consortium, and
- $1 million through 2022 for a joint counterterrorism awareness workshop.

CBO estimates that implementing those provisions would cost about $2.4 billion over the 2019–2023 period.

DHS Inspector General. H.R. 2825 would authorize the appropriation of $175 million for fiscal year 2019 for the DHS Office of Inspector General. CBO estimates that implementing the provision would cost $175 million over the 2019–2020 period.

Congressional Commission. H.R. 2825 would authorize the appropriation of $1 million for a commission to review Congressional oversight of DHS; the commission would terminate within one year of enactment of the legislation. Because the legislation does not specify a schedule for the authorization, CBO assumes that the funding will be provided in fiscal year 2019. CBO estimates that implementing the provision would cost $1 million that year.

Other programs

CBO estimates that carrying out the other activities described below would require appropriations of about $1.2 billion over the 2019–2023 period.

Other FEMA Programs. H.R. 2825 would strike provisions of current law that authorize appropriations for Transit Security Grants through 2011 and for Port Security Grants through 2013. Although those authorizations have expired, the programs received funds in 2018. The legislation would not change the nature of those programs' responsibilities. By striking the expired authorization but leaving the underlying programs in place, the legislation would effectively permanently authorize those programs. Using information from FEMA on current program funding and accounting for anticipated inflation, CBO estimates implementing H.R. 2825 would authorize appropriations for FEMA over the 2019–2023 period as follows:

- $469 million for the Transit Security Grant Program, and
- $533 million for the Port Security Grant Program.

CBO estimates that implementing those provisions would cost $438 million over the 2019–2023 period and $564 million after 2023.

FEMA Predisaster Mitigation Fund. H.R. 2825 would create the National Public Infrastructure Predisaster Mitigation Fund. For each major disaster declared after August 1, 2017, an amount equal to 6 percent of the total estimated funding FEMA expects to provide for certain disaster response grants would be transferred into the proposed fund from amounts in the Disaster Relief Fund. The new fund would be used to provide technical and financial assistance to states and localities for hazard mitigation designed to reduce injury, loss of life, and damage and destruction of property. Amounts in the fund could be spent without further appropriation.

After enactment, CBO estimates, about $120 million—6 percent of the estimated $2 billion in relevant disaster response grants expected to be made for disasters declared after August 1, 2017—would be transferred to the proposed fund in 2019. In recent years,

FEMA has been provided an average of $400 million a year for the relevant disaster response grants. Assuming that the Congress provides similar amounts in subsequent years, CBO estimates that $24 million (6 percent of $400 million) would be transferred to the fund each year.

Because the provision does not change any underlying authority to provide disaster relief, in CBO's view the legislation implicitly authorizes the appropriation of amounts equal to the amounts that would be transferred from the Disaster Relief Fund to the Predisaster Mitigation Fund. Thus, on the basis of historical spending patterns, CBO estimates that spending under this section would total $157 million over the 2019–2023 period and $59 million after 2023.

Reports and Reviews. H.R. 2825 would require DHS and the Government Accountability Office to prepare about 45 program reviews or reports (some annually) on various topics within the department's purview. Based on the cost of similar activities, CBO estimates that it would cost about $20 million over the 2019–2023 period to prepare those reports and reviews.

Pay-As-You-Go considerations: H.R. 2825 would increase direct spending for additional workers' compensation claims from private-sector employees working with DHS. The act would allow certain private-sector employees who are injured in the course of their work at the department to have related medical expenses paid through the federal workers' compensation program; such payments are considered mandatory spending. Based on the projected number of affected private-sector employees who will work with DHS, CBO estimates that the additional liability will increase direct spending by $50,000 to $100,000 per year, starting in 2021, and by less than $500,000 over the 2019–2028 period.

The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. CBO estimates that enacting H.R. 2825 would have no significant effect on direct spending in any year. The bill would not affect revenues.

Increase in long-term direct spending and deficits: CBO estimates that enacting H.R. 2825 would not significantly increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

Mandates: H.R. 2825 contains no intergovernmental or private-sector mandates as defined in UMRA.

Previous CBO estimate: On July 20, 2017, CBO transmitted a cost estimate for H.R. 2825, the DHS Authorization Act of 2017, as reported by the House Committee on Homeland Security on June 28, 2017. CBO estimated that implementing that version of the legislation would cost $5.6 billion over the 2018–2022 period, assuming appropriation of the necessary amounts. The differences in the cost estimates are attributable to differences in provisions, differences in CBO's assumptions about the enactment date for each version of the legislation, and the fact that appropriations for 2018 have already been provided.

Estimate prepared by: Federal costs: Robert Reese (FEMA); Mark Grabowicz (all Other DHS); Meredith Decker (workers' compensation); Mandates: Andrew Laughlin.

Estimate reviewed by: Kim P. Cawley, Chief, Natural and Physical Resources Cost Estimates Unit; H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE ACT, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002."

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

Sec. 1. * * *

* * * * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

Sec. 104. Insider Threat Program.

[TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION]

TITLE II—INFORMATION ANALYSIS

[SUBTITLE A—INFORMATION AND ANALYSIS AND INFRASTRUCTURE PROTECTION; ACCESS TO INFORMATION]

Subtitle A—Information and Analysis; Access to Information

[Sec. 201. Information and Analysis and Infrastructure Protection.]
Sec. 201. Information and analysis.

* * * * * * *

[Sec. 210A. Department of Homeland Security State, Local, and Regional Information Fusion Center Initiative.]
Sec. 210A. Department of Homeland Security Fusion Center Partnership Initiative.

* * * * * * *

[Sec. 210E. National Asset Database.]
Sec. 210E. Classified Information Advisory Officer.
[Sec. 210F. Classified Information Advisory Officer.]
Sec. 210F. Homeland intelligence doctrine.
Sec. 210G. Homeland terrorist threat assessments.
Sec. 210H. Report on terrorism prevention activities.
Sec. 210I. Departmental coordination to counter threats.
Sec. 210J. Chemical, biological, radiological, and nuclear intelligence and information sharing.

[SUBTITLE B—CRITICAL INFRASTRUCTURE INFORMATION]

[Sec. 211. Short title.]
[Sec. 212. Definitions.]
[Sec. 213. Designation of critical infrastructure protection program.]
[Sec. 214. Protection of voluntarily shared critical infrastructure information.]
[Sec. 215. No private right of action.]

[SUBTITLE C—INFORMATION SECURITY]

Subtitle B—Information Security

Sec. 221. * * *
Sec. 222. * * *
[Sec. 223. Enhancement of Federal and non-Federal cybersecurity.]
[Sec. 224. Net guard.]
[Sec. 225. Cyber Security Enhancement Act of 2002.]
[Sec. 226. Cybersecurity recruitment and retention.]
[Sec. 227. National cybersecurity and communications integration center.]
[Sec. 228. Cybersecurity plans.]
[Sec. 228A. Cybersecurity strategy.]
[Sec. 229. Clearances.]
[Sec. 230. Federal intrusion detection and prevention system.]

[SUBTITLE D—OFFICE OF SCIENCE AND TECHNOLOGY]

Subtitle C—Office of Science and Technology

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

[Sec. 307. Homeland Security Advanced Research Projects Agency.]
Sec. 307. Office of the Chief Scientist.

* * * * * * *

[Sec. 317. Promoting antiterrorism through international cooperation program.]
[Sec. 319. EMP and GMD mitigation research and development.]
[Sec. 318. Social media working group.]
[Sec. 319. Transparency in research and development.]
Sec. 317. Promoting antiterrorism through international cooperation program.
Sec. 318. Social media working group.
Sec. 319. Transparency in research and development.
Sec. 320. EMP and GMD mitigation research and development.
Sec. 321. Canine detection research and development.
Sec. 322. Cybersecurity Research and Development.

TITLE IV—BORDER, MARITIME, AND TRANSPORTATION SECURITY

* * * * * * *

SUBTITLE C—MISCELLANEOUS PROVISIONS

* * * * * * *

[Sec. 431. Office of Cargo Security Policy.]

* * * * * * *

SUBTITLE F—GENERAL IMMIGRATION PROVISIONS

* * * * * * *

[Sec. 475. Director of Shared Services.]
Sec. 476. * * *
Sec. 477. * * *
[Sec. 478. Immigration functions.]
Sec. 478. Annual report on immigration functions.

* * * * * * *

TITLE V—NATIONAL EMERGENCY MANAGEMENT

Sec. 501. * * *
[Sec. 502. Definition.]

* * * * * * *

[Sec. 513. Disability Coordinator.]
Sec. 513. Office of Disability Integration and Coordination.
Sec. 514. * * *
Sec. 515. * * *
[Sec. 516. Chief medical officer.]

* * * * * * *

[Sec. 524. Voluntary private sector preparedness accreditation and certification program.]

* * * * * * *

Sec. 529. Joint Counterterrorism Awareness Workshop Series.
Sec. 530. Center for Faith-Based and Neighborhood Partnerships.
Sec. 531. Senior Law Enforcement Advisor.

* * * * * * *

TITLE VII—MANAGEMENT

* * * * * * *

[Sec. 705. Establishment of Officer for Civil Rights and Civil Liberties.]
[Sec. 706. Consolidation and co-location of offices.]
[Sec. 707. Quadrennial Homeland Security Review.]
[Sec. 708. Joint Task Forces.]
[Sec. 709. Office of Strategy, Policy, and Plans.]
Sec. 705. Civil Rights and Civil Liberties.
Sec. 706. Quadrennial homeland security review.
Sec. 707. Joint task forces.
Sec. 708. Office of Strategy, Policy, and Plans.
Sec. 709. Chief Procurement Officer.
Sec. 710. Chief Security Officer.
Sec. 711. Annual submittal to Congress of information on reprogramming or transfers of funds to respond to operational surges.
Sec. 712. Chief Facilities and Logistics Officer.
Sec. 713. Long term real property strategies.
Sec. 714. Workforce health and medical support.
Sec. 715. Employee Engagement and Retention Action Plan.
Sec. 716. Acquisition Authorities for Program Accountability and Risk Management.
Sec. 717. Acquisition documentation.
Sec. 718. Acquisition innovation.

TITLE VIII—COORDINATION WITH NON–FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

SUBTITLE B—INSPECTOR GENERAL

[Sec. 811. Authority of the Secretary.]
[Sec. 812. Law enforcement powers of Inspector General agents.]
Sec. 811. Law enforcement powers of Inspector General agents.

* * * * * * *

SUBTITLE D—ACQUISITIONS

* * * * * * *

Sec. 836. Acquisition Review Board.
Sec. 837. Congressional notification and other requirements for major acquisition program breach.
Sec. 838. Multiyear acquisition strategy.
Sec. 839. Acquisition policies and guidance.

SUBTITLE E—HUMAN RESOURCES MANAGEMENT

* * * * * * *

[Sec. 857. Review and report by Comptroller General.]
[Sec. 858. Identification of new entrants into the Federal marketplace.]
Sec. 857. Identification of new entrants into the Federal marketplace.

* * * * * * *

SUBTITLE H—MISCELLANEOUS PROVISIONS

Sec. 871. * * *
[Sec. 872. Reorganization.] [147]

[147] The bill as reported by the Committee retained a provision in H.R. 2825 as passed by the House of Representatives that would have removed Section 872 of the Homeland Security Act of 2002. Retaining this provision of the House bill was a drafting error by the Committee that will be corrected before any action is taken by the full Senate on the bill on the floor. The Chairman favors DHS retaining its ability to reorganize under Section 872.

Sec. 873. * * *
[Sec. 874. Future Year Homeland Security Program.]
Sec. 874. Future Years Homeland Security Program.

* * * * * * *

[Sec. 878. Counternarcotics officer.]
[Sec. 879. Office of International Affairs.]
Sec. 880. Prohibition of the Terrorism Information and Prevention System.
[Sec. 881. Review of pay and benefit plans.]

* * * * * * *

Sec. 890B. Department Leadership Councils.

* * * * * * *

TITLE XVIII—EMERGENCY COMMUNICATIONS

[Sec. 1801. Office for Emergency Communications.]
Sec. 1801. Emergency Communications Division.

* * * * * * *

[TITLE XIX—DOMESTIC NUCLEAR DETECTION OFFICE]

TITLE XIX—COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE

Sec. 1900. Definitions.
[Sec. 1901. Domestic Nuclear Detection Office.]

Subtitle A—Countering Weapons of Mass Destruction Office

Sec. 1901. Countering Weapons of Mass Destruction Office.
[Sec. 1902. Mission of Office.]
[Sec. 1903. Hiring Authority.]
[Sec. 1904. Testing Authority.]
[Sec. 1905. Relationship to other Department entities and Federal agencies.]
[Sec. 1906. Contracting and grant making authorities.]
[Sec. 1907. Joint annual interagency review of global nuclear detection architecture.]

Subtitle B—Mission of the Office

Sec. 1921. Mission of the Office.
Sec. 1922. Relationship to other department entities and Federal agencies.
Sec. 1923. Responsibilities.
Sec. 1924. Hiring authority.
Sec. 1925. Testing authority.
Sec. 1926. Contracting and grant making authorities.
Sec. 1927. Joint annual interagency review of global nuclear detection architecture.

Subtitle C—Chief Medical Officer

Sec. 1931. Chief Medical Officer.

TITLE XX—HOMELAND SECURITY GRANTS

* * * * * * *

Sec. 2009. Operation Stonegarden.
Sec. 2010. Non-Profit Security Grant Program.

SUBTITLE B—GRANTS ADMINISTRATION

* * * * * * *

Sec. 2024. Memoranda of understanding with departmental components and officer regarding the policy and guidance.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Subtitle A—Cybersecurity and Infrastructure Security

Sec. 2201. Definitions.
Sec. 2202. Cybersecurity and Infrastructure Security Agency.
Sec. 2203. Cybersecurity Division.
Sec. 2204. Infrastructure Security Division.
Sec. 2205. Enhancement of Federal and non-Federal cybersecurity.
Sec. 2206. Net guard.

Sec. 2207. Cyber Security Enhancement Act of 2002.
Sec. 2208. Cybersecurity recruitment and retention.
Sec. 2209. National cybersecurity and communications integration center.
Sec. 2210. Cybersecurity plans.
Sec. 2211. Cybersecurity strategy.
Sec. 2212. Clearances.
Sec. 2213. Federal intrusion detection and prevention system.
Sec. 2214. National Asset Database.

Subtitle B—Critical Infrastructure Information

Sec. 2221. Short title.
Sec. 2222. Definitions.
Sec. 2223. Designation of critical infrastructure protection program.
Sec. 2224. Protection of voluntarily shared critical infrastructure information.
Sec. 2225. No private right of action.

SEC. 2. DEFINITIONS.

In this chapter, the following definitions apply—

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

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

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

(B) review, including approving, pausing, modifying, or canceling, an acquisition throughout the life cycle of the acquisition;

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

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

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

(3) The term "acquisition decision event" means, with respect to an acquisition program, a predetermined point within each of the acquisition phases at which the person exercising the acquisition decision authority determines whether the acquisition program shall proceed to the next phase.

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

(5) The term "acquisition program" means the totality of activities directed to accomplish specific goals and objectives, which may—

(A) provide new or improved capabilities in response to approved requirements or sustain existing capabilities; and

(B) have multiple projects to obtain specific capability requirements or capital assets.

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

[(1)]*(7)* * *

[(2)]*(8)* * *

[(3)]*(9)* * *

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

(A) identifying and validating needs;

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

(C) establishing requirements;

(D) developing cost estimates and schedules that consider the work necessary to develop, plan, support, and install a program or solution;

(E) identifying sources of funding that match resources to requirements;

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

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

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

(I) ensuring an adequate, well-trained, and diverse workforce that is qualified and sufficient in number to perform necessary functions;

(J) developing innovative, effective, and efficient processes and strategies;

(K) integrating risk management and mitigation techniques for national security considerations; and

(L) integrating the capabilities described in subparagraphs (A) through (K) into the mission and business operations of the Department.

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

(12) The term "congressional homeland security committees" means—

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

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

(13) The term "Component Acquisition Executive" means the senior acquisition official within a component who is designated in writing by the Under Secretary for Management, in consultation with the component head, with authority and responsibility for leading a process and staff to provide acquisition and program management oversight, policy, and guidance

to ensure that statutory, regulatory, and higher level policy requirements are fulfilled, including compliance with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives established by the Under Secretary for Management.

(14) The term "cost-type contract" means a contract that—

(A) provides for payment of allowable incurred costs, to the extent prescribed in the contract; and

(B) establishes an estimate of total cost for the purpose of obligating funds and establishing a ceiling that the contractor may not exceed, except at the risk of the contractor, without the approval of the contracting officer.

[(4)]*(15)* * *

[(5)]*(16)* * *

[(6)]*(17)* * *

[(7)]*(18)* * *

[(8)]*(19)* * *

(20) The term "fixed-price contract" means a contract that provides for a firm price or, in appropriate cases, an adjustable price.

[(9)]*(21)* * *

[(10)]*(22)* * *

[(11)]*(23)* The term "intelligence component of the Department" means any element or entity of the Department that collects, gathers, processes, analyzes, produces, or disseminates intelligence information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence, as defined under section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)), except—(A) the United States Secret Service; and (B) the Coast Guard, when operating under the direct authority of the Secretary of Defense or Secretary of the Navy pursuant to section 3 of title 14, United States Code, except that nothing in this paragraph shall affect or diminish the authority and responsibilities of the Commandant of the Coast Guard to command or control the Coast Guard as an armed force or the authority of the Director of National Intelligence with respect to the Coast Guard as an element of the intelligence community (as defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

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

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

[(13)]*(26)* * *

(27) The term "major acquisition program" means a Department acquisition program that is estimated by the Secretary or a designee of the Secretary to require an eventual total expenditure of not less than $300,000,000 (based on fiscal year 2017 constant dollars) over the life cycle cost of the program.

[(14)]*(28)* * *

[(15)](29) * * *
[(16)](30) * * *
[(17)](31) * * *
[(18)](32) * * *
[(19)](33) * * *
[(20)](34) * * *

* * * * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

SEC. 102. SECRETARY; FUNCTIONS.

(a) * * *

(b) FUNCTIONS.—The Secretary—

(1) * * *

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

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

(4) shall establish a Homeland Security Advisory Council to provide advice and recommendations on homeland security-related matters, including advice with respect to the preparation of the quadrennial homeland security review under section 706.

(c) COORDINATION WITH NON-FEDERAL ENTITIES.—With respect to homeland security, the Secretary shall coordinate [through the Office of State and Local Coordination (established under section 801 of this title)] *through the Office of Partnership and Engagement* (including the provision of training and equipment) with State and local government personnel, agencies, and authorities, with the private sector, and with other entities, including by—

* * * * * * *

(h) HEADQUARTERS.—

(1) IN GENERAL.—There is in the Department a Headquarters.

(2) COMPONENTS.—The Department Headquarters shall include each of the following:

(A) The Office of the Secretary, which shall include—

(i) the Deputy Secretary;

(ii) the Chief of Staff; and

(iii) the Executive Secretary.

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

(C) The Science and Technology Directorate.

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

(E) The Office of the General Counsel.

(F) The Office of the Chief Privacy and FOIA Officer.

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

(H) The Office of Operations Coordination.

(I) The Office of Intelligence and Analysis.
(J) The Office of Legislative Affairs.
(K) The Office of Public Affairs.
(L) The Office of the Inspector General.
(M) The Office of the Citizenship and Immigration Services Ombudsman.
(N) The Countering Weapons of Mass Destruction Office.
(O) The Office of Partnership and Engagement.

SEC. 103. OTHER OFFICERS.

(a) DEPUTY SECRETARY; UNDER SECRETARIES; *ASSISTANT SECRETARIES AND OTHER OFFICERS.*—

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

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

* * * * * * *

(E) A Director of the ⟦Bureau of⟧ *United States* Citizenship and Immigration Services.

* * * * * * *

⟦(H) An Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department.⟧

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

⟦(I) Not more than 12 Assistant Secretaries.⟧

(I) An Administrator of the Transportation Security Administration.

* * * * * * *

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

(2) ASSISTANT SECRETARIES.—The following Assistant Secretaries shall be appointed by the President or the Secretary, as the case may be, without the advice and consent of the Senate:

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

(i) The Assistant Secretary for Public Affairs.
(ii) The Assistant Secretary for Legislative Affairs.
(iii) The Assistant Secretary for the Countering Weapons of Mass Destruction Office.
(iv) The Chief Medical Officer.

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

(i) The Assistant Secretary for International Affairs.
(ii) The Assistant Secretary for Threat Prevention and Security Policy.

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

(iv) The Assistant Secretary for Cybersecurity, Infrastructure, and Resilience Policy.

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

(vi) The Assistant Secretary for State and Local Law Enforcement.

(vii) The Assistant Secretary for Partnership and Engagement.

(viii) The Assistant Secretary for Private Sector.

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

(b) * * *

(c) * * *

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

(1) A Director of Secret Service.

(2) A Chief Information Officer.

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

[(4) A Director for Domestic Nuclear Detection.**]**

[(5)**]***(4)* Any Director of a Joint Task Force under **[**section 708**]** *section 707.*

(e) * * *

(f) SPECIAL ASSISTANT TO THE SECRETARY.—The Secretary shall appoint a Special Assistant to the Secretary who shall be responsible for—

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

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

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

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

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

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

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

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

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

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

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

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

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

[(9)](2) coordinating industry efforts, with respect to functions of the Department of Homeland Security, to identify private sector resources and capabilities that could be effective in supplementing Federal, State, and local government agency efforts to prevent or respond to a terrorist attack;

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

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

(g) * * *

(h) OFFICE OF LEGISLATIVE AFFAIRS.—

(1) IN GENERAL.—Notwithstanding any other provision of law, any report that the Department or a component of the Department is required to submit to the Committee on Appropriations of the Senate or the Committee on Appropriations of the House of Representatives under any provision of law shall be submitted concurrently to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives.

(2) APPLICABILITY.—Paragraph (1) shall apply with respect to any report described in paragraph (1) that is submitted on or after the date of enactment of the DHS Authorization Act.

(3) NOTICE.—The Secretary shall notify, in writing, the chairmen and ranking members of the authorizing and appropriating committees of jurisdiction regarding policy memoranda, management directives, and reprogramming notifications issued by the Department.

(i) OFFICE OF PRIVATE SECTOR.—The Assistant Secretary for Private Sector shall be responsible for—

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

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

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

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

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

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

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

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

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

SEC. 104. INSIDER THREAT PROGRAM.

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

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

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

(3) conduct risk mitigation activities for insider threats.

(b) STEERING COMMITTEE.—

(1) IN GENERAL.—

(A) ESTABLISHMENT.—The Secretary shall establish a Steering Committee within the Department.

(B) MEMBERSHIP.—The membership of the Steering Committee shall be as follows:

(i) The Under Secretary for Management and the Under Secretary for Intelligence and Analysis shall serve as the Co-Chairpersons of the Steering Committee.

(ii) The Chief Security Officer, as the designated Senior Insider Threat Official, shall serve as the Vice Chairperson of the Steering Committee.

(iii) The other members of the Steering Committee shall be comprised of representatives of—

(I) the Office of Intelligence and Analysis;

(II) the Office of the Chief Information Officer;

(III) the Office of the General Counsel;

(IV) the Office for Civil Rights and Civil Liberties;

(V) the Privacy Office;

(VI) the Office of the Chief Human Capital Officer;

(VII) the Office of the Chief Financial Officer;

(VIII) the Federal Protective Service;

(IX) the Office of the Chief Procurement Officer;

(X) the Science and Technology Directorate; and

(XI) other components or offices of the Department as appropriate.

(C) MEETINGS.—The members of the Steering Committee shall meet on a regular basis to discuss cases and issues related to insider threats to the Department's critical assets, in accordance with subsection (a).

(2) RESPONSIBILITIES.—Not later than 1 year after the date of the enactment of this section, the Under Secretary for Management, the Under Secretary for Intelligence and Analysis, and the Chief Security Officer, in coordination with the Steering Committee, shall—

(A) develop a holistic strategy for Department-wide efforts to identify, prevent, mitigate, and respond to insider threats to the Department's critical assets;

(B) develop a plan to implement the insider threat measures identified in the strategy developed under subparagraph (A) across the components and offices of the Department;

(C) document insider threat policies and controls;

(D) conduct a baseline risk assessment of insider threats posed to the Department's critical assets;

(E) examine programmatic and technology best practices adopted by the Federal Government, industry, and research institutions to implement solutions that are validated and cost-effective;

(F) develop a timeline for deploying workplace monitoring technologies, employee awareness campaigns, and education and training programs related to identifying, preventing, mitigating, and responding to potential insider threats to the Department's critical assets;

(G) consult with the Under Secretary for Science and Technology and other appropriate stakeholders to ensure the Insider Threat Program is informed, on an ongoing basis, by current information regarding threats, best practices, and available technology; and

(H) develop, collect, and report metrics on the effectiveness of the Department's insider threat mitigation efforts.

(c) PRESERVATION OF MERIT SYSTEM RIGHTS.—

(1) IN GENERAL.—The Steering Committee shall not seek to, and the authorities provided under this section shall not be used to, deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)) (commonly known as the 'Intelligence Community Whistleblower Protection Act of 1998'), chapter 12 or 23 of title 5, United States Code, the Inspector

General Act of 1978 (5 U.S.C. App.), or any other whistleblower statute, regulation, or policy.

(2) IMPLEMENTATION.—

(A) IN GENERAL.—Any activity carried out under this section shall be subject to section 115 of the Whistleblower Protection Enhancement Act of 2012 (5 U.S.C. 2302 note).

(B) REQUIRED STATEMENT.—Any activity to implement or enforce any insider threat activity or authority under this section or Executive Order 13587 (50 U.S.C. 3161 note) shall include the statement required by section 115 of the Whistleblower Protection Enhancement Act of 2012 (5 U.S.C. 2302 note) that preserves rights under whistleblower laws and section 7211 of title 5, United States Code, protecting communications with Congress.

(d) DEFINITIONS.—In this section:

(1) CRITICAL ASSETS.—The term "critical assets" means the resources, including personnel, facilities, information, equipment, networks, or systems necessary for the Department to fulfill its mission.

(2) EMPLOYEE.—The term "employee" has the meaning given the term in section 2105 of title 5, United States Code.

(3) INSIDER.—The term "insider" means—

(A) any person who has or had authorized access to Department facilities, information, equipment, networks, or systems and is employed by, detailed to, or assigned to the Department, including members of the Armed Forces, experts or consultants to the Department, industrial or commercial contractors, licensees, certificate holders, or grantees of the Department, including all subcontractors, personal services contractors, or any other category of person who acts for or on behalf of the Department, as determined by the Secretary; or

(B) State, local, tribal, territorial, and private sector personnel who possess security clearances granted by the Department.

(4) INSIDER THREAT.—The term "insider threat" means the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States, including damage to the United States through espionage, terrorism, the unauthorized disclosure of classified national security information, or through the loss or degradation of departmental resources or capabilities.

(5) STEERING COMMITTEE.—The term "Steering Committee" means the Steering Committee established under subsection (b)(1)(A).

TITLE II—INFORMATION ANALYSIS [AND INFRASTRUCTURE PROTECTION]

* * * * * * *

Subtitle A—Information and Analysis [and Infrastructure Protection]; Access to Information

* * * * * * *

SEC. 201. INFORMATION AND ANALYSIS [AND INFRASTRUCTURE PROTECTION].

(a) INTELLIGENCE AND ANALYSIS [AND INFRASTRUCTURE PROTECTION].—There shall be in the Department an Office of Intelligence and Analysis [and an Office of Infrastructure Protection].

(b) UNDER SECRETARY FOR INFORMATION AND ANALYSIS [AND ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION].—

(1) * * *

(2) * * *

[(3) OFFICE OF INFRASTRUCTURE PROTECTION.—The Office of Infrastructure Protection shall be headed by an Assistant Secretary for Infrastructure Protection, who shall be appointed by the President.]

(c) DISCHARGE OF RESPONSIBILITIES.—The Secretary shall ensure that the responsibilities of the Department relating to information analysis [and infrastructure protection], including those described in subsection (d), are carried out through the Under Secretary for Intelligence and Analysis [or the Assistant Secretary for Infrastructure Protection, as appropriate].

(d) RESPONSIBILITIES OF SECRETARY RELATING TO INTELLIGENCE AND ANALYSIS [AND INFRASTRUCTURE PROTECTION].—The responsibilities of the Secretary relating to intelligence and analysis [and infrastructure protection] shall be as follows:

(1) * * *

* * * * * * *

[(5) To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.]

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

[(7)]*(5)* To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), including homeland security information, terrorism information, and weapons of mass destruction information, and any policies, guidelines, procedures, instructions, or standards established under that section.

[(8)]*(6)* To disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relat-

ing to homeland security, [and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.] *to State, local, and tribal governments and private entities with such responsibilities, and, as appropriate, to the public, in order to assist in preventing, deterring, or responding to acts of terrorism against the United States.*

[(9)]*(7)* * *

[(10)]*(8)* * *

[(11)]*(9)* * *

[(12)]*(10)* * *

[(13)]*(11)* * *

[(14)]*(12)* * *

[(15)]*(13)* * *

[(16)]*(14)* * *

[(17)]*(15)* * *

[(18)]*(16)* * *

[(19)]*(17)* * *

[(20)]*(18)* * *

[(21)]*(19)* * *

[(22)]*(20)* * *

[(23)]*(21)* * *

[(24)]*(22)* * *

[(25) To prepare and submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security in the House of Representatives, and to other appropriate congressional committees having jurisdiction over the critical infrastructure or key resources, for each sector identified in the National Infrastructure Protection Plan, a report on the comprehensive assessments carried out by the Secretary of the critical infrastructure and key resources of the United States, evaluating threat, vulnerability, and consequence, as required under this subsection. Each such report—(A) shall contain, if applicable, actions or countermeasures recommended or taken by the Secretary or the head of another Federal agency to address issues identified in the assessments; (B) shall be required for fiscal year 2007 and each subsequent fiscal year and shall be submitted not later than 35 days after the last day of the fiscal year covered by the report; and (C) may be classified.]

[(26)]*(23)*

(A) * * *

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

(i) be based on findings of the research and development conducted under [section 319]*section 320*;

* * * * * * *

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

(27) To carry out section 210G (relating to homeland terrorist threat assessments) and section 210H (relating to terrorism prevention activities).

(e) STAFF.—

(1) IN GENERAL.—The Secretary shall provide the Office of Intelligence and Analysis [and the Office of Infrastructure Protection] with a staff of analysts having appropriate expertise and experience to assist such offices in discharging responsibilities under this section. *The Secretary shall also provide the Chief Intelligence Officer with a staff having appropriate component intelligence program expertise and experience to assist the Chief Intelligence Officer.*

* * * * * * *

SEC. 202. ACCESS TO INFORMATION.

(a) * * *

(b) * * *

(c) TREATMENT UNDER CERTAIN LAWS.—The Secretary shall be deemed to be a Federal law enforcement, intelligence, protective, national defense, immigration, or national security official, and shall be provided with all information from law enforcement agencies that is required to be given to the [Director of Central Intelligence] *Director of National Intelligence*, under any provision of the following:

(1) The USA PATRIOT Act of 2001 (Public Law 107–56).

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

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

(d) ACCESS TO INTELLIGENCE AND OTHER INFORMATION.—

(1) * * *

(2) SHARING OF INFORMATION.—The Secretary, in consultation with the [Director of Central Intelligence] *Director of National Intelligence*, shall work to ensure that intelligence or other information relating to terrorism to which the Department has access is appropriately shared with the elements of the Federal Government referred to in paragraph (1), as well as with State and local governments, as appropriate.

* * * * * * *

SEC. 204. HOMELAND SECURITY INFORMATION SHARING.

(a) * * *

(b) * * *

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

(1) ESTABLISHMENT OF BUSINESS PROCESSES.—The Secretary, acting through the Under Secretary for Intelligence and Analysis or the [Assistant Secretary for Infrastructure Protection] *Director of the Cybersecurity and Infrastructure Security Agency*, as appropriate, shall—

* * * * * * *

(d) Training and Evaluation of Employees.—

(1) Training.—The Secretary, acting through the Under Secretary for Intelligence and Analysis or the [Assistant Secretary for Infrastructure Protection]*Director of the Cybersecurity and Infrastructure Security Agency*, as appropriate, shall provide to

employees of the Department opportunities for training and education to develop an understanding of—

* * * * * * *

SEC. 210A. [DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL, AND REGIONAL INFORMATION FUSION CENTER INITIATIVE.] *DEPARTMENT OF HOMELAND SECURITY FUSION CENTER PARTNERSHIP INITIATIVE.*

(a) ESTABLISHMENT.—The Secretary in consultation with the program manager of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), the Attorney General, the Privacy Officer of the Department, the Officer for Civil Rights and Civil Liberties of the Department, and the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note), shall establish a Department of Homeland Security State, Local, and Regional Fusion Center Initiative to establish partnerships with State, local, and regional fusion centers. *Beginning on the date of enactment of the Department of Homeland Security Authorization Act, such Initiative shall be known as the "Department of Homeland Security Fusion Center Partnership Initiative".*

[(b)**]**

(b) INTERAGENCY SUPPORT AND COORDINATION.—Through the Department of Homeland Security Fusion Center Partnership Initiative, in coordination with principal officials of fusion centers in the National Network of Fusion Centers and the officers designated as the Homeland Security Advisors of the States, the Secretary shall—

(1) coordinate with the heads of other Federal departments and agencies to provide operational, analytic, and reporting intelligence advice and assistance to the National Network of Fusion Centers and to align homeland security intelligence activities with other field based intelligence activities;

(2) support the integration of fusion centers into the information sharing environment, including by—

(A) providing for the effective dissemination of information within the scope of the information sharing environment to the National Network of Fusion Centers;

(B) conducting outreach to such fusion centers to identify any gaps in information sharing;

(C) consulting with other Federal agencies to develop methods to—

(i) address any such gaps identified under subparagraph (B), as appropriate; and

(ii) deploy or access such databases and datasets, as appropriate; and

(D) review information that is gathered by the National Network of Fusion Centers to identify that which is within the scope of the information sharing environment, including homeland security information (as defined in section 892), terrorism information, and weapons of mass destruction information and incorporate such information, as appropriate, into the Department's own such information;

(3) facilitate close communication and coordination between the National Network of Fusion Centers and the Department and other Federal departments and agencies;

(4) facilitate information sharing and expertise from the national cybersecurity and communications integration center under section 2209 to the National Network of Fusion Centers;

(5) coordinate the provision of training and technical assistance, including training on the use of Federal databases and datasets described in paragraph (2), to the National Network of Fusion Centers and encourage participating fusion centers to take part in terrorism threat-related exercises conducted by the Department;

(6) ensure the dissemination of cyber threat indicators and information about cybersecurity risks and incidents to the national Network of Fusion Centers;

(7) ensure that each fusion center in the National Network of Fusion Centers has a privacy policy approved by the Chief Privacy Officer of the Department and a civil rights and civil liberties policy approved by the Officer for Civil Rights and Civil Liberties of the Department;

(8) develop and disseminate best practices on the appropriate levels for staffing at fusion centers in the National Network of Fusion Centers of qualified representatives from State, local, tribal, and territorial law enforcement, fire, emergency medical, and emergency management services, and public health disciplines, as well as the private sector;

(9) to the maximum extent practicable, provide guidance, training, and technical assistance to ensure fusion centers operate in accordance with and in a manner that protects privacy, civil rights, and civil liberties afforded by the Constitution of the United States;

(10) to the maximum extent practicable, provide guidance, training, and technical assistance to ensure fusion centers are appropriately aligned with and able to meaningfully support Federal homeland security, national security, and law enforcement efforts, including counterterrorism;

(11) encourage the full participation of the National Network of Fusion Centers in all assessment and evaluation efforts conducted by the Department;

(12) track all Federal funding provided to each fusion center on an individualized basis as well as by funding source;

(13) ensure that none of the departmental information or data provided or otherwise made available to fusion center personnel is improperly disseminated, accessed for unauthorized purposes, or otherwise used in a manner inconsistent with Department guidance; and (14) carry out such other duties as the Secretary determines appropriate.

(c) [PERSONNEL ASSIGNMENT] *RESOURCE ALLOCATION.*—

[(1) IN GENERAL.—The Under Secretary for Intelligence and Analysis shall, to the maximum extent practicable, assign officers and intelligence analysts from components of the Department to participating State, local, and regional fusion centers.

[(2) PERSONNEL SOURCES.—Officers and intelligence analysts assigned to participating fusion centers under this subsection may be assigned from the following Department components, in coordination with the respective component head and in consultation with the principal officials of participating fusion centers:

[(A) Office of Intelligence and Analysis.

[(B) [Office of Infrastructure Protection] *Cybersecurity and Infrastructure Security Agency*.

[(C) Transportation Security Administration.

[(D) United States Customs and Border Protection.

[(E) United States Immigration and Customs Enforcement.

[(F) United States Coast Guard.

[(G) Other components of the Department, as determined by the Secretary.]

(1) INFORMATION SHARING AND PERSONNEL ASSIGNMENT.—

(A) INFORMATION SHARING.—The Under Secretary for Intelligence and Analysis shall ensure that, as appropriate—

(i) fusion centers in the National Network of Fusion Centers have access to homeland security information sharing systems; and

(ii) Department personnel are deployed to support fusion centers in the National Network of Fusion Centers in a manner consistent with the mission of the Department.

(B) PERSONNEL ASSIGNMENT.—Department personnel referred to in subparagraph (A)(ii) may include the following:

(i) Intelligence officers.

(ii) Intelligence analysts.

(iii) Other liaisons from components and offices of the Department, as appropriate.

(C) MEMORANDA OF UNDERSTANDING.—The Under Secretary for Intelligence and Analysis shall negotiate memoranda of understanding between the Department and a State or local government, in coordination with the appropriate representatives from fusion centers in the National Network of Fusion Centers, regarding the exchange of information between the Department and such fusion centers. Such memoranda shall include the following:

(i) The categories of information to be provided by each entity to the other entity that are parties to any such memoranda

(ii) The contemplated uses of the exchanged information that is the subject of any such memoranda.

(iii) The procedures for developing joint products.

(iv) The information sharing dispute resolution processes.

(v) Any protections necessary to ensure the exchange of information accords with applicable law and policies.

(2) SOURCES OF SUPPORT.—Information shared and personnel assigned pursuant to paragraph (1) may be shared or provided, as the case may be, by the following Department components and offices, in coordination with the respective component or office head and in consultation with the principal officials of fusion centers in the National Network of Fusion Centers:

(A) The Office of Intelligence and Analysis.

(B) Cybersecurity and Infrastructure Security Agency.

(C) The Transportation Security Administration.

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

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

(F) The Coast Guard.

(G) The national cybersecurity and communications integration center under section 2209.

(H) Other components or offices of the Department, as determined by the Secretary.

(3) [QUALIFYING CRITERIA] *RESOURCE ALLOCATION CRITERIA.*—

[(A) IN GENERAL.—The Secretary shall develop qualifying criteria for a fusion center to participate in the assigning of Department officers or intelligence analysts under this section.]

(A) IN GENERAL.—The Secretary shall make available criteria for sharing information and deploying personnel to support a fusion center in the National Network of Fusion Centers in a manner consistent with the Department's mission and existing statutory limits.

(B) * * *

(4) PREREQUISITE.—

(A) * * *

(B) Prior work experience in area.—In determining the eligibility of an officer or intelligence analyst to be assigned to a fusion center under this section, the Under Secretary for Intelligence and Analysis shall consider the familiarity of the officer or intelligence analyst with the State, locality, or region in which such fusion center is located, as determined by such factors as whether the officer or intelligence analyst—

* * * * * * *

(d) RESPONSIBILITIES.—An officer or intelligence analyst assigned to a fusion center under this section shall—

(1) * * *

(2) * * *

(3) create intelligence and other information products derived from such information and other homeland security-relevant information provided by the Department; [and]

(4) assist, in coordination with the national cybersecurity and communications integration center under section 2209, fusion centers in using information relating to cybersecurity risks to develop a comprehensive and accurate threat picture;

[(4)]*(5)* assist in the dissemination of such products, as coordinated by the Under Secretary for Intelligence and Analysis, to law enforcement agencies and other emergency response providers of State, local, and tribal [government] *governments*, other fusion centers, and appropriate Federal agencies[.]; *and*

(6) use Department information, including information held by components and offices, to develop analysis focused on the mission of the Department under section 101(b).

(e) BORDER INTELLIGENCE PRIORITY.—

[(1) IN GENERAL.—The Secretary shall make it a priority to assign officers and intelligence analysts under this section from United States Customs and Border Protection, United States Immigration and Customs Enforcement, and the Coast Guard to participating State, local, and regional fusion centers

located in jurisdictions along land or maritime borders of the United States in order to enhance the integrity of and security at such borders by helping Federal, State, local, and tribal law enforcement authorities to identify, investigate, and otherwise interdict persons, weapons, and related contraband that pose a threat to homeland security.]

(1) IN GENERAL.—To the greatest extent practicable, the Secretary shall make it a priority to allocate resources, including departmental component personnel with relevant expertise, to support the efforts of fusion centers along land or maritime borders of the United States to facilitate law enforcement agency identification, investigation, and interdiction of persons, weapons, and related contraband that pose a threat to homeland security.

(2) BORDER INTELLIGENCE PRODUCTS.—When performing the responsibilities described in subsection (d), officers and intelligence analysts assigned to [participating State, local, and regional fusion centers] *fusion centers in the National Network of Fusion Centers* under this section shall have, as a primary responsibility, the creation of border intelligence products that—

* * * * * * *

(j) DEFINITIONS.—In this section—

(1) the term "cybersecurity risk" has the meaning given such term in section 2209;

[(1)](*2*) * * *

[(2)](*3*) * * *

[(3)](*4*) * * *

[(4)](*5*) the term "intelligence-led policing" means the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision making at the tactical and strategic levels; [and]

(6) the term "National Network of Fusion Centers" means a decentralized arrangement of fusion centers intended to enhance individual State and urban area fusion centers ability to leverage the capabilities and expertise of all fusion centers for the purpose of enhancing analysis and homeland security information sharing nationally; and

[(5)](*7*) * * *

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

* * * * * * *

SEC. 210[F]*E.* CLASSIFIED INFORMATION ADVISORY OFFICER.

* * * * * * *

SEC. 210F. HOMELAND INTELLIGENCE DOCTRINE.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Secretary, acting through the Chief Intelligence Officer of the Department, in coordination with intelligence components of the Department, the Office of the General

Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties, shall develop and disseminate written Department-wide guidance for the processing, analysis, production, and dissemination of homeland security information (as such term is defined in section 892) and terrorism information (as such term is defined in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485)).

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

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

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

(3) Guidance for the processing, analysis, and production of such information, including descriptions of component or program specific datasets that facilitate the processing, analysis, and production.

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

(5) A statement of intent regarding how the dissemination of homeland security information and terrorism information to the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))) and Federal law enforcement agencies should assist the intelligence community and Federal law enforcement agencies in carrying out their respective missions.

(6) A statement of intent regarding how the dissemination of homeland security information and terrorism information to State, local, tribal, and territorial government agencies, including law enforcement agencies, should assist the agencies in carrying out their respective missions.

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

(d) ANNUAL REVIEW.—For each of the 5 fiscal years beginning with the first fiscal year that begins after the date of the enactment of this section, the Secretary shall conduct a review of the guidance required under subsection (a) and, as appropriate, revise such guidance.

SEC. 210G. HOMELAND TERRORIST THREAT ASSESSMENTS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this section and for each of the following 5 fiscal years (beginning in the first fiscal year that begins after the date of the enactment of this section), the Secretary, acting through the Under Secretary for Intelligence and Analysis, and using departmental information, including component information coordinated with each

intelligence component of the Department and programs of each such intelligence component, and information provided through State and major urban area fusion centers, shall conduct an assessment of the terrorist threat to the homeland.

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

(1) Empirical data assessing terrorist activities and incidents over time in the United States, including terrorist activities and incidents planned or supported by foreign or domestic terrorists or persons outside of the United States to occur in the homeland.

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

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

(4) Detailed information on all individuals suspected of involvement in terrorist activity and subsequently—

(A) prosecuted for a Federal criminal offense, including details of the criminal charges involved;

(B) placed into removal proceedings, including details of the removal processes and charges used;

(C) denied entry into the United States, including details of the denial processes used; or

(D) subjected to civil proceedings for revocation of naturalization.

(5) The efficacy and reach of foreign and domestic terrorist organization propaganda, messaging, or recruitment, including details of any specific propaganda, messaging, or recruitment that contributed to terrorist activities identified pursuant to paragraph (1).

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

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

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

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

(1) shall, to the extent practicable, utilize existing component data collected and existing component threat assessments; and

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

(d) FORM.—The assessments required under subsection (a) shall be shared with the appropriate congressional committees and submitted in unclassified form, but may include separate classified annexes, if appropriate.

SEC. 210H. REPORT ON TERRORISM PREVENTION ACTIVITIES OF THE DEPARTMENT.

(a) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this section, and annually thereafter, the Secretary shall submit to Congress an annual report that shall include the following:

(1) A description of the status of the programs and policies of the Department for countering violent extremism and similar activities in the United States.

(2) A description of the efforts of the Department to cooperate with and provide assistance to other Federal departments and agencies.

(3) Qualitative and quantitative metrics for evaluating the success of the programs and policies described in paragraph (1) and the steps taken to evaluate the success of those programs and policies.

(4) An accounting of—

(A) grants and cooperative agreements awarded by the Department to counter violent extremism; and

(B) all training specifically aimed at countering violent extremism sponsored by the Department.

(5) In coordination with the Under Secretary for Intelligence and Analysis, an analysis of how the activities of the Department to counter violent extremism correspond and adapt to the threat environment.

(6) A summary of how civil rights and civil liberties are protected in the activities of the Department to counter violent extremism.

(7) An evaluation of the use of grants and cooperative agreements awarded under sections 2003 and 2004 to support efforts of local communities in the United States to counter violent extremism, including information on the effectiveness of those grants and cooperative agreements in countering violent extremism.

(8) A description of how the Department incorporated lessons learned from the countering violent extremism programs and policies and similar activities of foreign, State, local, tribal, and territorial governments and stakeholder communities.

(9) A description of the decision process used by the Department to rename or refocus the entities within the Department that are focused on the issues described in this subsection, including a description of the threat basis for that decision.

(b) ANNUAL REVIEW.—Not later than 1 year after the date of enactment of this section, and annually thereafter, the Office for Civil Rights and Civil Liberties of the Department shall—

(1) conduct a review of the countering violent extremism and similar activities of the Department to ensure that all such activities of the Department respect the privacy, civil rights, and civil liberties of all persons; and

(2) make publicly available on the website of the Department a report containing the results of the review conducted under paragraph (1).

SEC. 210I. DEPARTMENTAL COORDINATION ON COUNTER THREATS.

(a) ESTABLISHMENT.—There is authorized in the Department, for a period of 2 years beginning after the date of enactment of this sec-

tion, a Counter Threats Advisory Board (in this section referred to as the "Board") which shall—(1) be composed of senior representatives of departmental operational components and headquarters elements; and (2) coordinate departmental intelligence activities and policy and information related to the mission and functions of the Department that counter threats.

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

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

(2) be reviewed and updated as appropriate.

(c) MEMBERS.—

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

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

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

(A) The Transportation Security Administration.

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

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

(D) The Federal Emergency Management Agency.

(E) The Coast Guard.

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

(G) The United States Secret Service.

(H) The Cybersecurity and Infrastructure Security Agency.

(I) The Office of Operations Coordination.

(J) The Office of the General Counsel.

(K) The Office of Intelligence and Analysis.

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

(M) The Science and Technology Directorate.

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

(O) The Privacy Office.

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

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

(d) MEETINGS.—The Board shall—

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

(2) make recommendations to the Secretary.

(e) TERRORISM ALERTS.—The Board shall advise the Secretary on the issuance of terrorism alerts under section 203.

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

SEC. 210J. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR INTELLIGENCE AND INFORMATION SHARING.

(a) IN GENERAL.—The Office of Intelligence and Analysis of the Department shall—

(1) support homeland security-focused intelligence analysis of terrorist actors, their claims, and their plans to conduct attacks

involving chemical, biological, radiological, or nuclear materials against the United States;

(2) support homeland security-focused intelligence analysis of global infectious disease, public health, food, agricultural, and veterinary issues;

(3) support homeland security-focused risk analysis and risk assessments of the homeland security hazards described in paragraphs (1) and (2), including the transportation of chemical, biological, nuclear, and radiological materials, by providing relevant quantitative and nonquantitative threat information;

(4) leverage existing and emerging homeland security intelligence capabilities and structures to enhance prevention, protection, response, and recovery efforts with respect to a chemical, biological, radiological, or nuclear attack;

(5) share information and provide tailored analytical support on these threats to State, local, and tribal authorities, other Federal agencies, and relevant national biosecurity and biodefense stakeholders, as appropriate; and

(6) perform other responsibilities, as assigned by the Secretary.

(b) COORDINATION.—Where appropriate, the Office of Intelligence and Analysis shall coordinate with other relevant Department components, including the Countering Weapons of Mass Destruction Office, the National Biosurveillance Integration Center, other agencies within the intelligence community, including the National Counter Proliferation Center, and other Federal, State, local, and tribal authorities, including officials from high-threat urban areas, State and major urban area fusion centers, and local public health departments, as appropriate, and enable such entities to provide recommendations on optimal information sharing mechanisms, including expeditious sharing of classified information, and on how such entities can provide information to the Department.

(c) DEFINITIONS.—In this section:

(1) FUSION CENTER.—The term "fusion center" has the meaning given the term in section 210A.

(2) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(3) NATIONAL BIOSECURITY AND BIODEFENSE STAKEHOLDERS.—The term "national biosecurity and biodefense stakeholders' means officials from Federal, State, local, and tribal authorities and individuals from the private sector who are involved in efforts to prevent, protect against, respond to, and recover from a biological attack or other phenomena that may have serious health consequences for the United States, including infectious disease outbreaks.

* * * * * * *

Subtitle C—Information Strategy

* * * * * * *

SEC. 222. PRIVACY OFFICER.

(a) APPOINTMENT AND RESPONSIBILITIES.—The Secretary shall appoint a senior official in the Department, *to be the Chief Privacy and FOIA Officer of the Department*, who shall report directly [to the Secretary, to assume] *to the Secretary. Such official shall have* primary responsibility for privacy policy, including—

(1) * * *

* * * * * * *

(5) coordinating with the Officer for Civil Rights and Civil Liberties to ensure that—

(A) * * *

(B) Congress receives appropriate reports on such programs, policies, and procedures; [and]

[(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974 [5 U.S.C. 552a], internal controls, and other matters.]

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

(7) establishing a mechanism to ensure such components are in compliance with Federal regulatory and statutory and Department privacy requirements, mandates, directives, and policies, including requirements under section 552 of title 5, United States Code (commonly known as the "Freedom of Information Act");

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

(9) serving as the Chief FOIA Officer of the Department for purposes of section 552(j) of title 5, United States Code (commonly known as the "Freedom of Information Act");

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

(11) carrying out such other responsibilities as the Secretary determines are appropriate, consistent with this section.

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

SEC. 302. RESPONSIBILITIES AND AUTHORITIES OF THE UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.

[The Secretary, acting through the Under]*The Under* Secretary for Science and Technology, shall have the responsibility for—

(1) * * *

(2) developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for, identifying priorities, goals, objectives and policies for, and coordinating the Federal Government's civilian efforts to identify and develop countermeasures to chemical, [biological,,] *biological,*

and other emerging terrorist threats, including the development of comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts;

(3) supporting the Under Secretary for Intelligence and Analysis and the [Assistant Secretary for Infrastructure Protection] *Director of the Cybersecurity and Infrastructure Security Agency*, by assessing and testing homeland security vulnerabilities and possible threats;

(4) conducting basic and applied research, development, demonstration, testing, [and evaluation]*evaluation, and standards coordination and development* activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, except that such responsibility does not extend to human health-related research and development activities;

(5) * * *

(A) preventing the importation of chemical, [biological,,] *biological,* and related weapons and material; and

* * * * * * *

SEC. 307. [HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY] *OFFICE OF THE CHIEF SCIENTIST*.

(a) DEFINITIONS.—In this section:

[(1) Fund.—The term "Fund" means the Acceleration Fund for Research and Development of Homeland Security Technologies established in subsection (c).]

[(2)] *(1)* HOMELAND SECURITY RESEARCH.—The term "homeland security research" means research relevant to the detection of, prevention of, protection against, response to, attribution of, and recovery from homeland security threats, particularly acts of terrorism.

[(3) HSARPA.—The term "HSARPA" means the Homeland Security Advanced Research Projects Agency established in subsection (b).]

[(4)] *(2)* Under secretary.—The term "Under Secretary" means the Under Secretary for Science and Technology.

[(b) HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY.—

[(1) ESTABLISHMENT.—There is established the Homeland Security Advanced Research Projects Agency.

[(2) DIRECTOR.—HSARPA shall be headed by a Director, who shall be appointed by the Secretary. The Director shall report to the Under Secretary.

[(3) RESPONSIBILITIES.—The Director shall administer the Fund to award competitive, merit-reviewed grants, cooperative agreements or contracts to public or private entities, including businesses, federally funded research and development centers, and universities. The Director shall administer the Fund to—

[(A) support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security;

[(B) advance the development, testing and evaluation, and deployment of critical homeland security technologies;

[(C) accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities; and

[(D) conduct research and development for the purpose of advancing technology for the investigation of child exploitation crimes, including child victim identification, trafficking in persons, and child pornography, and for advanced forensics.

[(4) TARGETED COMPETITIONS.—The Director may solicit proposals to address specific vulnerabilities identified by the Director.

[(5) COORDINATION.—The Director shall ensure that the activities of HSARPA are coordinated with those of other relevant research agencies, and may run projects jointly with other agencies.

[(6) PERSONNEL.—In hiring personnel for HSARPA, the Secretary shall have the hiring and management authorities described in section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note; Public Law 105–261). The term of appointments for employees under subsection (c)(1) of that section may not exceed 5 years before the granting of any extension under subsection (c)(2) of that section.

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

[(c) FUND.—

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

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

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

(b) OFFICE OF THE CHIEF SCIENTIST.—

(1) ESTABLISHMENT.—There is established the Office of the Chief Scientist.

(2) CHIEF SCIENTIST.—The Office of the Chief Scientist shall be headed by a Chief Scientist, who shall be appointed by the Under Secretary.

(3) QUALIFICATIONS.—The Chief Scientist shall—

(A) be appointed from among distinguished scientists with specialized training or significant experience in a field

related to counterterrorism, traditional homeland security missions, or national defense; and

(B) have earned an advanced degree at an institution of higher education (as defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)).

(4) RESPONSIBILITIES.—The Chief Scientist shall oversee all research and development to—

(A) support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security;

(B) advance the development, testing and evaluation, standards coordination and development, and deployment of critical homeland security technologies;

(C) accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities;

(D) promote the award of competitive, merit-reviewed grants, cooperative agreements or contracts to public or private entities, including business, federally funded research and development centers, and universities; and

(E) oversee research and development for the purpose of advancing technology for the investigation of child exploitation crimes, including child victim identification, trafficking in persons, and child pornography, and for advanced forensics.

(5) COORDINATION.—The Chief Scientist shall ensure that the activities of the Directorate for Testing and Evaluation of Science and Technology are coordinated with those of other relevant research agencies, and may oversee projects jointly with other agencies.

(6) PERSONNEL.—In hiring personnel for the Science and Technology Directorate, the Secretary shall have the hiring and management authorities described in section 1599h of title 10, United States Code. The term of appointments for employees under subsection (c)(1) of that section may not exceed 5 years before the granting of any extension under subsection (c)(2) of that section.

(7) DEMONSTRATIONS.—The Chief Scientist, periodically, shall hold homeland security technology demonstrations, pilots, field assessments, and workshops to improve contact among technology developers, vendors, component personnel, State, local, and tribal first responders, and acquisition personnel.

* * * * * * *

SEC. 315. EMERGENCY COMMUNICATIONS INTEROPERABILITY RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.— * * *

(1) * * *

(2) interoperable emergency communications capabilities among emergency response providers and relevant government officials, including by—

(A) supporting research on a competitive basis, including through the **[**Directorate of Science and Technology and Homeland Security Advanced Research Projects Agency**]**

Directorate Science and Technology and the Chief Scientist; and

(B) considering the establishment of a Center of Excellence under the Department of Homeland Security Centers of Excellence Program focused on improving emergency response providers' communication capabilities.

(b) * * *

(c) * * *

SEC. 316. NATIONAL BIOSURVEILLANCE INTEGRATION CENTER.

(a) IN GENERAL.—The [Secretary shall] *Secretary, acting through the Assistant Secretary for Countering Weapons of Mass Destruction Office, shall* establish, operate, and maintain a national Biosurveillance Integration Center (referred to in this section as the "NBIC"), which shall be headed by a Directing Officer, under an office or directorate of the Department that is in existence as of the date of the enactment of this section.

SEC. 317. PROMOTING ANTITERRORISM THROUGH INTERNATIONAL COOPERATION PROGRAM.

(a) * * *

(b) SCIENCE AND TECHNOLOGY HOMELAND SECURITY INTERNATIONAL COOPERATIVE PROGRAMS OFFICE.—

(1) * * *

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

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

(B) * * *

(3) * * *

(4) COORDINATION.—The Director shall ensure that the activities under this subsection are coordinated with [the Office of International Affairs and] the Department of State and, as appropriate, the Department of Defense, the Department of Energy, and other relevant Federal agencies or interagency bodies. The Director may enter into joint activities with other Federal agencies.

* * * * * * *

(f) ANIMAL AND ZOONOTIC DISEASES.—As part of the international cooperative activities authorized in this section, the Under Secretary, in coordination with [the Chief Medical Officer,] *the Assistant Secretary for the Countering of Weapons of Mass Destruction Office,* the Department of State, and appropriate officials of the Department of Agriculture, the Department of Defense, and the Department of Health and Human Services, may enter into cooperative activities with foreign countries, including African nations, to strengthen American preparedness against foreign animal and zoonotic diseases overseas that could harm the Nation's agricultural and public health sectors if they were to reach the United States.

* * * * * * *

[SEC. 319.] *SEC. 320.* EMP AND GMD MITIGATION RESEARCH AND DEVELOPMENT.

(a) * * *

(b) * * *

(c) EXEMPTION FROM DISCLOSURE.—

(1) INFORMATION SHARED WITH THE FEDERAL GOVERNMENT.—[Section 214] *Section 2224*, and any regulations issued pursuant to such section, shall apply to any information shared with the Federal Government under this section.

(2) INFORMATION SHARED BY THE FEDERAL GOVERNMENT.—Information shared by the Federal Government with a State, local, or tribal government under this section shall be exempt from disclosure under any provision of State, local, or tribal freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring the disclosure of information or records.

SEC. 321. CANINE DETECTION RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—In furtherance of domestic preparedness and response, the Secretary, acting through the Under Secretary for Science and Technology, and in consultation with other relevant executive agencies, relevant State, local, and tribal governments, and academic and industry stakeholders, shall, to the extent practicable, conduct research and development of canine detection technology to mitigate the risk of the threats of existing and emerging weapons of mass destruction.

(b) SCOPE.—The scope of the research and development under subsection (a) may include the following:

(1) Canine-based sensing technologies.

(2) Chem-Bio defense technologies.

(3) New dimensions of olfaction biology.

(4) Novel chemical sensing technologies.

(5) Advances in metabolomics and volatilomics.

(6) Advances in gene therapy, phenomics, and molecular medicine.

(7) Reproductive science and technology.

(8) End user techniques, tactics, and procedures.

(9) National security policies, standards and practices for canine sensing technologies.

(10) Protective technology, medicine, and treatments for the canine detection platform.

(11) Domestic capacity and standards development.

(12) Emerging threat detection.

(13) Training aids.

(14) Genetic, behavioral, and physiological optimization of the canine detection platform.

(c) COORDINATION AND COLLABORATION.—The Secretary, acting through the Under Secretary for Science and Technology, shall ensure research and development activities are conducted in coordination and collaboration with academia, all levels of government, and private sector stakeholders.

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

SEC. 322. CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—The Under Secretary for Science and Technology shall support the research, development, testing, evaluation, and transition of cybersecurity technologies, including fundamental

research to improve the sharing of information, information security, analytics, and methodologies related to cybersecurity risks and incidents, consistent with current law.

(b) ACTIVITIES.—The research and development supported under subsection (a) shall serve the components of the Department and shall—

(1) advance the development and accelerate the deployment of more secure information systems;

(2) improve and create technologies for detecting and preventing attacks or intrusions, including real-time continuous diagnostics, real-time analytic technologies, and full life cycle information protection;

(3) improve and create mitigation and recovery methodologies, including techniques and policies for real-time containment of attacks and development of resilient networks and information systems;

(4) assist the development and support infrastructure and tools to support cybersecurity research and development efforts, including modeling, testbeds, and data sets for assessment of new cybersecurity technologies;

(5) assist the development and support of technologies to reduce vulnerabilities in industrial control systems;

(6) assist the development and support cyber forensics and attack attribution capabilities;

(7) assist the development and accelerate the deployment of full information life cycle security technologies to enhance protection, control, and privacy of information to detect and prevent cybersecurity risks and incidents;

(8) assist the development and accelerate the deployment of information security measures, in addition to perimeter-based protections;

(9) assist the development and accelerate the deployment of technologies to detect improper information access by authorized users;

(10) assist the development and accelerate the deployment of cryptographic technologies to protect information at rest, in transit, and in use;

(11) assist the development and accelerate the deployment of methods to promote greater software assurance;

(12) assist the development and accelerate the deployment of tools to securely and automatically update software and firmware in use, with limited or no necessary intervention by users and limited impact on concurrently operating systems and processes; and

(13) assist in identifying and addressing unidentified or future cybersecurity threats.

(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate activities with—

(1) the Director of Cybersecurity and Infrastructure Security;

(2) the heads of other relevant Federal departments and agencies, as appropriate; and

(3) industry and academia.

(d) TRANSITION TO PRACTICE.—The Under Secretary for Science and Technology shall—

(1) support projects carried out under this title through the full life cycle of such projects, including research, development, testing, evaluation, pilots, and transitions;

(2) identify mature technologies that address existing or imminent cybersecurity gaps in public or private information systems and networks of information systems, protect sensitive information within and outside networks of information systems, identify and support necessary improvements identified during pilot programs and testing and evaluation activities, and introduce new cybersecurity technologies throughout the homeland security enterprise through partnerships and commercialization; and

(3) target federally funded cybersecurity research that demonstrates a high probability of successful transition to the commercial market within 2 years and that is expected to have a notable impact on the public or private information systems and networks of information systems.

(e) DEFINITIONS.—In this section:

(1) CYBERSECURITY RISK.—The term "cybersecurity risk" has the meaning given the term in section 2209.

(2) HOMELAND SECURITY ENTERPRISE.—The term "homeland security enterprise" means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.

(3) INCIDENT.—The term "incident" has the meaning given the term in section 2209.

(4) INFORMATION SYSTEM.—The term "information system" has the meaning given the term in section 3502 of title 44, United States Code.

(5) SOFTWARE ASSURANCE.—The term "software assurance" means confidence that software—

(A) is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during the life cycle of the software; and

(B) functioning in the intended manner.

* * * * * * *

TITLE IV—BORDER, MARITIME, AND TRANSPORTATION SECURITY

* * * * * * *

Subtitle C—Miscellanous Provisions

* * * * * * *

SEC. 427. COORDINATION OF INFORMATION AND INFORMATION TECHNOLOGY.

(a) * * *
(b) * * *
[(c)] * * *

* * * * * * *

[SEC. 431. OFFICE OF CARGO SECURITY POLICY.]

* * * * * * *

Subtitle F—General Immigration Provisions

* * * * * * *

[SEC. 475. DIRECTOR OF SHARED SERVICES.]

SEC. 476. SEPARATION OF FUNDING.

(a) IN GENERAL.—There shall be established separate accounts in the Treasury of the United States for appropriated funds and other deposits available for the [Bureau of Citizenship and Immigration Services] *United States Citizenship and Immigration Services* and the [Bureau of Border Security] *U.S. Immigration and Customs Enforcement.*

(b) SEPARATE BUDGETS.—To ensure that the [Bureau of Citizenship and Immigration Services] *United States Citizenship and Immigration Services* and the [Bureau of Border Security] *U.S. Immigration and Customs Enforcement* are funded to the extent necessary to fully carry out their respective functions, the Director of the Office of Management and Budget shall separate the budget requests for each such entity.

(c) FEES.—Fees imposed for a particular service, application, or benefit shall be deposited into the account established under subsection (a) that is for the bureau with jurisdiction over the function to which the fee relates.

(d) FEES NOT TRANSFERABLE.—No fee may be transferred between [the Bureau of Citizenship and Immigration Services] *United States Citizenship and Immigration Services* and [the Bureau of Border Security] *U.S. Immigration and Customs Enforcement* for purposes not authorized by section

* * * * * * *

SEC. 478. *ANNUAL REPORT ON* IMMIGRATION FUNCTIONS.

(a) ANNUAL [REPORT.—

[(1) IN GENERAL.—One year]*REPORT.—One year* after the date of the enactment of this Act, and each year thereafter, the Secretary shall submit a report to the President, to the Committees on the Judiciary and Government Reform of the House of Representatives, and to the Committees on the Judiciary and Government Affairs of the Senate, on the impact the transfers made by this subtitle has had on immigration functions.

[(2)]*(b)* [MATTER INCLUDED] *MATTER INCLUDED.*—The report shall address the following with respect to the period covered by the report:

[(A)]*(1)* The aggregate number of all immigration applications and petitions received, and processed, by the Department.

[(B)]*(2)* Region-by-region statistics on the aggregate number of immigration applications and petitions filed by an alien (or filed on behalf of an alien) and denied, disaggregated by category of denial and application or petition type.

[(C)]*(3)* The quantity of backlogged immigration applications and petitions that have been processed, the aggregate number

awaiting processing, and a detailed plan for eliminating the backlog.

[(D)]*(4)* The average processing period for immigration applications and petitions, disaggregated by application or petition type.

[(E)]*(5)* The number and types of immigration-related grievances filed with any official of the Department of Justice, and if those grievances were resolved.

[(F)]*(6)* Plans to address grievances and improve immigration services.

[(G)]*(7)* Whether immigration-related fees were used consistent with legal requirements regarding such use.

[(H)]*(8)* Whether immigration-related questions conveyed by customers to the Department (whether conveyed in person, by telephone, or by means of the Internet) were answered effectively and efficiently.

[(b) SENSE OF CONGRESS REGARDING IMMIGRATION SERVICES.—It is the sense of Congress that—

[(1) the quality and efficiency of immigration services rendered by the Federal Government should be improved after the transfers made by this subtitle take effect; and

[(2) the Secretary should undertake efforts to guarantee that concerns regarding the quality and efficiency of immigration services are addressed after such effective date.]

* * * * * * *

TITLE V—NATIONAL EMERGENCY MANAGEMENT

SEC. 501. DEFINITIONS.

In this title—

(1) * * *

* * * * * * *

(8) the term [“National Response Plan”] *“National Response Framework”* means the [National Response Plan] *National Response Framework* or any successor plan prepared under section [502(a)(6)] *504(a)(6)*;

(9) the term “Nuclear Incident Response Team” means a resource that includes—

(A) those entities of the Department of Energy that perform nuclear or radiological emergency support functions (including accident response, search response, advisory, and technical operations functions), radiation exposure functions at the medical assistance facility known as the Radiation Emergency Assistance Center/Training Site (REAC/TS), radiological assistance functions, and related functions; and

(B) those entities of the Environmental Protection Agency that perform such support functions (including radiological emergency response functions) and related functions.

[(9)]*(10)* * * *

[(10)]*(11)* * * *

[(11)]*(12)* * * *

[(12)]*(13)* * * *

[(13)]*(14)* the term "tribal government" means the government of any entity described in [section 2(13)(B)]*section 2(26)(B)*; and

[(14)]*(15)* * * *

[SEC. 502. DEFINITION.]

SEC. 503. FEDERAL EMERGENCY MANAGEMENT AGENCY.

(a) * * *

(b) MISSION.—

(1) * * *

(2) SPECIFIC ACTIVITIES.—In support of the primary mission of the Agency, the Administrator shall—

(A) lead the Nation's efforts to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents *and incidents impacting critical infrastructure*;

* * * * * * *

(G) provide funding, training, exercises, technical assistance, planning, and other assistance to build tribal, local, State, regional, and national capabilities (including communications capabilities), necessary to respond to a natural disaster, act of terrorism, or other man-made disaster; [and]

(H) develop and coordinate the implementation of a risk-based, all-hazards strategy for preparedness that builds those common capabilities necessary to respond to natural disasters, acts of terrorism, and other man-made disasters while also building the unique capabilities necessary to respond to specific types of incidents that pose the greatest risk to our Nation[.]*; and*

(I) identify and integrate the needs of children into activities to prepare for, protect against, respond to, recover from, and mitigate against natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents, including by appointing a technical expert, who may consult with relevant outside organizations and experts, as necessary, to coordinate such activities, as necessary.

(c) * * *

SEC. 504. AUTHORITY AND RESPONSIBILITIES.

(a) * * *

(1) * * *

(2) * * *

(3) providing the Federal Government's response to terrorist attacks and major disasters, [including—] *(which shall include incidents impacting critical infrastructure), including—*

* * * * * * *

(4) aiding the recovery from terrorist attacks and major disasters*, including incidents impacting critical infrastructure*;

(5) building a comprehensive national incident management system with Federal, State, [and local] *local, and tribal* government personnel, agencies, and authorities, to respond to such attacks and disasters;

(6) consolidating existing Federal Government emergency response plans into a single, coordinated [national response plan] *national response framework, which shall be reviewed and updated as required but not less than every 5 years*;

(7) developing integrated frameworks, to include consolidating existing Government plans addressing prevention, protection, mitigation, and recovery with such frameworks reviewed and updated as required, but not less than every 5 years;

[(7)]*(8)* * * *

[(8)]*(9)* * * *

[(9)]*(10)* * * *

[(10)]*(11)* * * *

[(11)]*(12)* * * *

[(12)]*(13)* * * *

[(13)]*(14)* administering, *periodically updating (but not less than once every 5 years),* and ensuring the implementation of the [National Response Plan] *National Response Framework*, including coordinating and ensuring the readiness of each emergency support function under the National Response Plan;

[(14)]*(15)* * * *

[(15)]*(16)* * * *

[(16)]*(17)* * * *

[(17)]*(18)* * * *

[(18)]*(19)* * * *

[(19)]*(20)* * * *

[(20)]*(21)* * * *

[(21)]*(22)* * * *

(b) * * *

SEC. 505. FUNCTIONS TRANSFERRED.

(a) * * *

(b) EXCEPTIONS.—The following within the Preparedness Directorate shall not be transferred:

(1) The Office of Infrastructure Protection.

(2) The National Communications System.

(3) The National Cybersecurity Division.

[(4) The Office of the Chief Medical Officer.]

[(5]]*(4)* The functions, personnel, assets, components, authorities, and liabilities of each component described under paragraphs (1) [through (4)] *through (3)*.

SEC. 506. PRESERVING THE FEDERAL EMERGENCY MANAGEMENT AGENCY

(a) * * *

[(b) REORGANIZATION.—Section 872 shall not apply to the Agency, including any function or organizational unit of the Agency.][148]

[(c)]*(b)* PROHIBITION ON CHANGES TO MISSIONS.—

(1) IN GENERAL.—The Secretary may not substantially or significantly reduce, including through a Joint Task Force established under [section 708] *section 707*, the authorities, responsibilities, or functions of the Agency or the capability of the

[148] The bill as reported by the Committee retained a provision in H.R. 2825 as passed by the House of Representatives that would have removed Section 872 of the Homeland Security Act of 2002. Retaining this provision of the House bill was a drafting error by the Committee that will be corrected before any action is taken by the full Senate on the bill on the floor. The Chairman favors DHS retaining its ability to reorganize under Section 872.

Agency to perform those missions, authorities, responsibilities, except as otherwise specifically provided in an Act enacted after the date of enactment of the Post-Katrina Emergency Management Reform Act of 2006.

(2) CERTAIN TRANSFERS PROHIBITED.—No asset, function, or mission of the Agency may be diverted to the principal and continuing use of any other organization, unit, or entity of the Department, including a Joint Task Force established under [section 708] *section 707*, except for details or assignments that do not reduce the capability of the Agency to perform its missions.

[(d)] *(c)* * * *

SEC. 507. REGIONAL OFFICES.

(a) * * *

(b) * * *

(c) RESPONSIBILITIES.—

(1) * * *

(2) RESPONSIBILITIES.—The responsibilities of a Regional Administrator include—

(A) * * *

* * * * * * *

(E) designating an individual responsible for the development of strategic and operational regional plans in support of the [National Response Plan] *National Response Framework*;

* * * * * * *

(3) TRAINING AND EXERCISE REQUIREMENTS.—

(A) TRAINING.—The Administrator shall require each Regional Administrator to undergo specific training periodically to complement the qualifications of the Regional Administrator. Such training, as appropriate, shall include training with respect to the National Incident Management System, the [National Response Plan] *National Response Framework*, and such other subjects as determined by the Administrator.

(B) * * *

(d) * * *

(e) * * *

(f) REGIONAL OFFICE STRIKE TEAMS.—

(1) * * *

(A) a designated Federal coordinating officer;

* * * * * * *

(G) individuals from the agencies with primary responsibility for each of the emergency support functions in the [National Response Plan] *National Response Framework*.

* * * * * * *

SEC. 508. NATIONAL ADVISORY COUNCIL.

(a) * * *

(b) RESPONSIBILITIES.—

(1) IN GENERAL.—The National Advisory Council shall advise the Administrator on all aspects of emergency management. The National Advisory Council shall incorporate State, local,

and tribal government and private sector input in the development and revision of the national preparedness goal, the national preparedness system, the National Incident Management System, the [National Response Plan] *National Response Framework*, and other related plans and strategies.

(2) * * *

(c) * * *

(d) RESPONSE SUBCOMMITTEE.—

(1) * * *

(2) MEMBERSHIP.—Notwithstanding subsection (c), the RESPONSE Subcommittee shall be composed of the following:

(A) [The Deputy Administrator, Protection and National Preparedness] *A Deputy Administrator* of the Federal Emergency Management Agency, or designee.

(B) * * *

(C) * * *

(D) The [Director of the Office of Emergency Communications of the Department of Homeland Security] *The Assistant Director for Emergency Communications*, or designee.

* * * * * * *

SEC. 509. NATIONAL INTEGRATION CENTER.

(a) IN GENERAL.—There is established in the Agency a National Integration Center.

(b) RESPONSIBILITIES.—

(1) IN GENERAL.—The Administrator, through the National Integration Center, and in consultation with other Federal departments and agencies and the National Advisory Council, shall ensure ongoing management and maintenance of the National Incident Management System, the [National Response Plan] *National Response Framework, National Protection Framework, National Prevention Framework, National Mitigation Framework, National Recovery Framework*, and any [successor] *successors* to such system or [plan] *framework*.

(2) SPECIFIC RESPONSIBILITIES.—The National Integration Center shall periodically, *but not less often than once every 5 years,* review, and revise as appropriate, the National Incident Management System and the [National Response Plan] *National Response Framework*, including—

(A) * * *

(B) * * *

(C) revising the Catastrophic Incident Annex, finalizing and releasing the Catastrophic Incident Supplement to the [National Response Plan] *National Response Framework*, and ensuring that both effectively address response requirements in the event of a catastrophic incident.

(c) INCIDENT MANAGEMENT.—

(1) IN GENERAL.—

(A) [NATIONAL RESPONSE PLAN] *NATIONAL RESPONSE FRAMEWORK.*—The Secretary, acting through the Administrator, shall ensure that the [National Response Plan] *National Response Framework* provides for a clear chain of command to lead and coordinate the Federal response to

any natural disaster, act of terrorism, or other man-made disaster.

(B) ADMINISTRATOR.—The chain of the command specified in the [National Response Plan] *National Response Framework* shall—

(2) PRINCIPAL FEDERAL OFFICIAL; JOINT TASK FORCE.—The Principal Federal Official (or the successor thereto) or Director of a Joint Task Force established under [section 708] *section 707* shall not—

(A) * * *

(B) * * *

SEC. 510. CREDENTIALING AND TYPING.

(a) IN GENERAL.—The Administrator shall [enter into a memorandum of understanding] *partner* with the administrators of the Emergency Management Assistance Compact, State, local, and tribal governments, and organizations that represent emergency response providers, to collaborate on developing standards for deployment capabilities, including for credentialing and typing of incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to natural disasters, acts of terrorism, and other manmade disasters.

(b) DISTRIBUTION.—

(1) IN GENERAL.— * * *

(A) each Federal agency that has responsibilities under the [National Response Plan] *National Response Framework* to aid that agency with credentialing and typing incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other man-made disaster; and

(B) * * *

(2) * * *

(c) CREDENTIALING AND TYPING OF PERSONNEL.—Not later than 6 months after receiving the standards provided under subsection (b), each Federal agency with responsibilities under the [National Response Plan] *National Response Framework* shall ensure that incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other manmade disaster are credentialed and typed in accordance with this section.

* * * * * * *

SEC. 513. DISABILITY COORDINATOR.

[(a) IN GENERAL.—After consultation with organizations representing individuals with disabilities, the National Council on Disabilities, and the Interagency Coordinating Council on Preparedness and Individuals with Disabilities, established under Executive Order No. 13347 (6 U.S.C. 312 note), the Administrator shall appoint a Disability Coordinator. The Disability Coordinator shall report directly to the Administrator, in order to ensure that the needs of individuals with disabilities are being properly addressed in emergency preparedness and disaster relief.

[(b) RESPONSIBILITIES.—The Disability Coordinator shall be responsible for—

[(1) providing guidance and coordination on matters related to individuals with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

[(2) interacting with the staff of the Agency, the National Council on Disabilities, the Interagency Coordinating Council on Preparedness and Individuals with Disabilities established under Executive Order No. 13347 (6 U.S.C. 312 note), other agencies of the Federal Government, and State, local, and tribal government authorities regarding the needs of individuals with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

[(3) consulting with organizations that represent the interests and rights of individuals with disabilities about the needs of individuals with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

[(4) ensuring the coordination and dissemination of best practices and model evacuation plans for individuals with disabilities;

[(5) ensuring the development of training materials and a curriculum for training of emergency response providers, State, local, and tribal government officials, and others on the needs of individuals with disabilities;

[(6) promoting the accessibility of telephone hotlines and websites regarding emergency preparedness, evacuations, and disaster relief;

[(7) working to ensure that video programming distributors, including broadcasters, cable operators, and satellite television services, make emergency information accessible to individuals with hearing and vision disabilities;

[(8) ensuring the availability of accessible transportation options for individuals with disabilities in the event of an evacuation;

[(9) providing guidance and implementing policies to ensure that the rights and wishes of individuals with disabilities regarding post-evacuation residency and relocation are respected;

[(10) ensuring that meeting the needs of individuals with disabilities are included in the components of the national preparedness system established under section 644 of the Post-Katrina Emergency Management Reform Act of 2006; and

[(11) any other duties as assigned by the Administrator.]

SEC. 513. OFFICE OF DISABILITY INTEGRATION AND COORDINATION.

(a) IN GENERAL.—There is established within the Agency an Office of Disability Integration and Coordination (in this section referred to as the "Office"), which shall be headed by a Director.

(b) MISSION.—The mission of the Office is to ensure that individuals with disabilities and other access and functional needs are included in emergency management activities throughout the Agency by providing guidance, tools, methods, and strategies for the purpose of equal physical program and effective communication access.

(c) RESPONSIBILITIES.—In support of the mission of the Office, the Director shall—

(1) provide guidance and coordination on matters related to individuals with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

(2) oversee Office employees responsible for disability integration in each regional office with respect to carrying out the mission of the Office;

(3) liaise with other employees of the Agency, including nonpermanent employees, organizations representing individuals with disabilities, other agencies of the Federal Government, and State, local, and tribal government authorities regarding the needs of individuals with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

(4) coordinate with the technical expert on the needs of children within the Agency to provide guidance and coordination on matters related to children with disabilities in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

(5) consult with organizations representing individuals with disabilities about access and functional needs in emergency planning requirements and relief efforts in the event of a natural disaster, act of terrorism, or other man-made disaster;

(6) ensure the coordination and dissemination of best practices and model evacuation plans for individuals with disabilities;

(7) collaborate with Agency leadership responsible for training to ensure that qualified experts develop easily accessible training materials and a curriculum for the training of emergency response providers, State, local, and tribal government officials, and others on the needs of individuals with disabilities;

(8) coordinate with the Emergency Management Institute, the Center for Domestic Preparedness, Center for Homeland Defense and Security, the United States Fire Administration, the national exercise program described in section 648(b) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 748(b)), and the National Domestic Preparedness Consortium to ensure that content related to persons with disabilities, access and functional needs, and children are integrated into existing and future emergency management trainings;

(9) promote the accessibility of telephone hotlines and websites regarding emergency preparedness, evacuations, and disaster relief;

(10) work to ensure that video programming distributors, including broadcasters, cable operators, and satellite television services, make emergency information accessible to individuals with hearing and vision disabilities;

(11) ensure the availability of accessible transportation options for individuals with disabilities in the event of an evacuation;

(12) provide guidance and implement policies to ensure that the rights and feedback of individuals with disabilities regarding post-evacuation residency and relocation are respected;

(13) ensure that meeting the needs of individuals with disabilities are included in the components of the national preparedness system established under section 644 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 744); and

(14) perform any other duties as assigned by the Administrator.

(d) DIRECTOR.—After consultation with organizations representing individuals with disabilities, the Administrator shall appoint a Director. The Director shall report directly to the Administrator, in order to ensure that the needs of individuals with disabilities are being properly addressed in emergency preparedness and disaster relief.

(e) ORGANIZATIONS REPRESENTING INDIVIDUALS WITH DISABILITIES DEFINED.—For purposes of this section, the term "organizations representing individuals with disabilities" means the National Council on Disabilities, the Interagency Coordinating Council on Preparedness and Individuals with Disabilities, and other appropriate disability organizations.

SEC. 514. DEPARTMENT AND AGENCY OFFICIALS.

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

[(b) CYBERSECURITY AND COMMUNICATIONS.—There is in the Department an Assistant Secretary for Cybersecurity and Communications.**]**

[(c)**]***(b)* UNITED STATES FIRE ADMINISTRATION.—The Administrator of the United States Fire Administration shall have a rank equivalent to an assistant secretary of the Department.

SEC. 515. NATIONAL OPERATIONS CENTER.

(a) * * *

(b) * * *

(c) STATE AND LOCAL EMERGENCY RESPONDER REPRESENTATION.—

(1) ESTABLISHMENT OF POSITIONS.—The Secretary shall establish a position, on a rotating basis, for a representative of State **[**and local**]**, *local, and tribal* emergency responders at the National Operations Center established under subsection (b) to ensure the effective sharing of information between the Federal Government and State **[**and local**]**, *local, and tribal* emergency response services.

(2) * * *

[SEC. 516. CHIEF MEDICAL OFFICER.]

* * * * * * *

SEC. 523. GUIDANCE AND RECOMMENDATIONS.

(a) IN GENERAL.—Consistent with their responsibilities and authorities under law, as of the day before the date of the enactment of this section, the Administrator and the **[**Assistant Secretary for Infrastructure Protection**]** *Director of Cybersecurity and Infrastructure Security*, in consultation with the private sector, may develop

guidance or recommendations and identify best practices to assist or foster action by the private sector in—

* * * * * * *

(c) SMALL BUSINESS CONCERNS.—In developing guidance or recommendations or identifying best practices under subsection (a), the Administrator and the [Assistant Secretary for Infrastructure Protection] *Director of Cybersecurity and Infrastructure Security* shall take into consideration small business concerns (under the meaning given that term in section 3 of the Small Business Act (15 U.S.C. 632)), including any need for separate guidance or recommendations or best practices, as necessary and appropriate.

(d) * * *

[SEC. 524. VOLUNTARY PRIVATE SECTOR PREPAREDNESS ACCREDITATION AND CERTIFICATION PROGRAM.]

SEC. 525. ACCEPTANCE OF GIFTS.

(a) AUTHORITY.—The [Secretary]*Administrator* may accept and use gifts of property, both real and personal, and may accept gifts of services, including from guest lecturers, for otherwise authorized activities of the Center for Domestic Preparedness that are related to efforts to prevent, prepare for, protect against, or respond to a natural disaster, act of terrorism, or other man-made disaster, including the use of a weapon of mass destruction.

(b) PROHIBITION.—The [Secretary]*Administrator* may not accept a gift under this section if the [Secretary] *Administrator* determines that the use of the property or services would compromise the integrity or appearance of integrity of—

(1) a program of the Department; or

(2) an individual involved in a program of the Department.

(c) REPORT.—

(1) IN GENERAL.—The [Secretary]*Administrator* shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an annual report disclosing—

(A) any gifts that were accepted under this section during the year covered by the report;

(B) how the gifts contribute to the mission of the Center for Domestic Preparedness; and

(C) the amount of Federal savings that were generated from the acceptance of the gifts.

(2) PUBLICATION.—Each report required under paragraph (1) shall be made publically available.

* * * * * * *

SEC. 528. COORDINATION OF DEPARTMENT OF HOMELAND SECURITY EFFORTS RELATED TO FOOD, AGRICULTURE, AND VETERINARY DEFENSE AGAINST TERRORISM.

(a) PROGRAM REQUIRED.—The Secretary, acting through the Assistant Secretary for [Health Affairs,] *the Countering Weapons of Mass Destruction Office,* shall carry out a program to coordinate the Department's efforts related to defending the food, agriculture, and veterinary systems of the United States against terrorism and other high-consequence events that pose a high risk to homeland

security. is in the Department a Chief Medical Officer, who shall be appointed by the President.

(b) * * *

(C) * * *

SEC. 529. JOINT COUNTERTERRORISM AWARENESS WORKSHOP SERIES.

(a) IN GENERAL.—The Administrator, in consultation with the Director of the National Counterterrorism Center and the Director of the Federal Bureau of Investigation, shall establish a Joint Counterterrorism Awareness Workshop Series (in this section referred to as the "Workshop Series") to—

(1) address emerging terrorist threats; and

(2) enhance the ability of State and local jurisdictions to prevent, protect against, respond to, and recover from terrorist attacks.

(b) PURPOSE.—The Workshop Series established under subsection (a) shall include—

(1) reviewing existing preparedness, response, and interdiction plans, policies, and procedures related to terrorist attacks of the participating jurisdictions and identifying gaps in those plans, operational capabilities, response resources, and authorities;

(2) identifying Federal, State, and local resources available to address the gaps identified under paragraph (1);

(3) providing assistance, through training, exercises, and other means, to build or sustain, as appropriate, the capabilities to close those identified gaps;

(4) examining the roles and responsibilities of participating agencies and respective communities in the event of a terrorist attack;

(5) improving situational awareness and information sharing among all participating agencies in the event of a terrorist attack; and

(6) identifying and sharing best practices and lessons learned from the Workshop Series.

(c) DESIGNATION OF PARTICIPATING CITIES.—The Administrator shall select jurisdictions to host a Workshop Series from those cities that—

(1) are currently receiving, or that previously received, funding under section 2003; and

(2) have requested to be considered.

(d) WORKSHOP SERIES PARTICIPANTS.—Individuals from State and local jurisdictions and emergency response providers in cities designated under subsection (c) shall be eligible to participate in the Workshop Series, including—

(1) senior elected and appointed officials;

(2) law enforcement;

(3) fire and rescue;

(4) emergency management;

(5) emergency medical services;

(6) public health officials;

(7) private sector representatives;

(8) representatives of nonprofit organizations; and

(9) other participants as deemed appropriate by the Administrator.

(e) REPORTS.—

(1) WORKSHOP SERIES REPORT.—The Administrator, in consultation with the Director of the National Counterterrorism Center, the Director of the Federal Bureau of Investigation, and officials from the city in which a Workshop Series is held, shall develop and submit to all of the agencies participating in the Workshop Series a report after the conclusion of the Workshop Series that addresses—

(A) key findings about lessons learned and best practices from the Workshop Series; and

(B) potential mitigation strategies and resources to address gaps identified during the Workshop Series.

(2) ANNUAL REPORTS.—Not later than 1 year after the date of enactment of this section and annually thereafter for 5 years, the Administrator, in consultation with the Director of the National Counterterrorism Center and the Director of the Federal Bureau of Investigation, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a comprehensive summary report of the key themes, lessons learned, and best practices identified during the Workshop Series held during the previous year.

(f) AUTHORIZATION.—There is authorized to be appropriated $1,000,000 for each of fiscal years 2018 through 2022 to carry out this section.

SEC. 530. CENTER FOR FAITH-BASED AND NEIGHBORHOOD PARTNERSHIPS.

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

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

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

(1) develop exercises that engage faith-based and community organizations to test capabilities for all hazards, including active shooter incidents;

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

(3) conduct outreach to faith-based and community organizations regarding guidance, training, and exercises and departmental capabilities available to assist faith-based and community organizations to secure their facilities against natural disasters, acts of terrorism, and other man-made disasters;

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

(5) deliver training and technical assistance to faith-based and community organizations and provide subject-matter exper-

tise related to anti-human trafficking efforts to help communities successfully partner with other components of the Blue Campaign of the Department; and

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

SEC. 531. SENIOR LAW ENFORCEMENT ADVISOR.

(a) ESTABLISHMENT.—The Administrator shall appoint a Senior Law Enforcement Advisor to serve as a qualified expert to the Administrator for the purpose of strengthening the Agency's coordination among State, local, and tribal law enforcement.

(b) QUALIFICATIONS.—The Senior Law Enforcement Advisor shall have an appropriate background with experience in law enforcement, information sharing, and other emergency response functions.

(c) RESPONSIBILITIES.—The Senior Law Enforcement Advisor shall—

(1) coordinate on behalf of the Administrator with the Office for State and Local Law Enforcement under section 2006 for the purpose of ensuring State, local, and tribal law enforcement receive consistent and appropriate consideration in policies, guidance, training, and exercises related to preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other man-made disasters within the United States;

(2) work with the Administrator and the Office for State and Local Law Enforcement under section 2006 to ensure grants to State, local, and tribal government agencies, including programs under sections 2003, 2004, and 2006(a), appropriately focus on terrorism prevention activities; and

(3) serve other appropriate functions as determined by the Administrator.

* * * * * * *

TITLE VII—MANAGEMENT

* * * * * * *

SEC. 701. UNDER SECRETARY FOR MANAGEMENT.

(a) IN GENERAL.— * * *

(1) The budget, appropriations, expenditures of funds, accounting, and finance.

(2) Procurement *and acquisition management.*

* * * * * * *

(d) ACQUISITION AND RELATED RESPONSIBILITIES.—

(1) IN GENERAL.—Notwithstanding subsection (a) of section 1702 of title 41, United States Code, the Under Secretary for Management—

(A) is the Chief Acquisition Officer of the Department;

(B) shall have the authorities and perform the functions specified in subsection (b) of such section; and

(C) shall perform all other functions and responsibilities delegated by the Secretary or described in this subsection.

(2) FUNCTIONS AND RESPONSIBILITIES.—In addition to the authorities and functions specified in section 1702(b) of title 41, United States Code, the functions and responsibilities of the

Under Secretary for Management related to acquisition include the following:

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

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

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

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

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

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

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

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

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

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

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

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

(J) Ensuring acquisition decision memoranda adequately document decisions made at acquisition decision events, including the rationale for decisions made to allow programs to deviate from the requirement to obtain approval by the

Department for certain documents at acquisition decision events.

(3) DELEGATION OF ACQUISITION DECISION AUTHORITY.—

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

(B) LEVEL 2 ACQUISITIONS.—The Under Secretary for Management may delegate acquisition decision authority in writing to the relevant Component Acquisition Executive for a major acquisition program that has a life cycle cost estimate of not less than $300,000,000 but not more than $1,000,000,000 if all of the following requirements are met:

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

(ii) The Component Acquisition Executive concerned has a well-trained and experienced workforce, commensurate with the size of the acquisition program and related activities delegated to the Component Acquisition Executive by the Under Secretary for Management.

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

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

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

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

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

(I) complete reviews of operational requirements to ensure the requirements are measurable, testable, and achievable within the constraints of cost and schedule;

(II) integrate applicable standards into development specifications;

(III) complete systems engineering reviews and technical assessments during development to inform production and deployment decisions;

(IV) complete independent testing and evaluation of technologies and systems;

(V) use independent verification and validation of operational testing and evaluation implementation and results; and

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

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

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

[(d)**]***(e)* * * *

[(e)**]***(f)* * * *

[(f)**]***(g)* * * *

SEC. 702. CHIEF FINANCIAL OFFICER.

(a) IN GENERAL.—**[**The Chief**]**

(1) FUNCTIONS.—The Chief Financial Officer shall perform functions as specified in chapter 9 of title 31, United States Code, and, with respect to all such functions and other responsibilities that may be assigned to the Chief Financial Officer from time to time, shall also report to the Under Secretary for Management.

(2) ACQUISITION AUTHORITIES.—The Chief Financial Officer, in coordination with the Under Secretary for Management, shall oversee the costs of acquisition programs and related activities to ensure that actual and planned costs are in accordance with budget estimates and are affordable, or can be adequately funded, over the life cycle of such programs and activities.

(b) RESPONSIBILITIES.—In carrying out the responsibilities, authorities, and functions specified in section 902 of title 31, United States Code, the Chief Financial Officer shall—

(1) oversee Department budget formulation and execution;

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

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

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

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

(6) lead financial system modernization efforts throughout the Department;

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

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

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

(10) participate in the selection, performance planning, and review of cost estimating positions with the Department;

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

(A) report to the Inspector General of the Department the expenditures by such component for each conference hosted for which the total expenditures of the Department exceed $100,000, within 15 days after the date of the conference; and

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

(i) the information described in subsections (a), (b), and (c) of section 739 of title VII of division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Public Law 113–235; 128 Stat. 2389); and

(ii) documentation of such expenditures; and

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

(A) report to the Inspector General of the Department the expenditures by such component for each conference hosted or attended by Department employees for which the total expenditures of the Department are more than $20,000 and less than $100,000, not later than 30 days after the date of the conference; and

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

(i) the information described in subsections (a), (b), and (c) of section 739 of title VII of division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Public Law 113–235; 128 Stat. 2389); and

(ii) documentation of such expenditures.

[(b)**]***(c)* PROGRAM ANALYSIS AND EVALUATION FUNCTION.—In addition to the responsibilities set forth in chapter 14 of title 5, United States Code, and other applicable law, the Chief Human Capital Officer of the Department shall—Department shall—

(1) ESTABLISHMENT OF THE OFFICE OF PROGRAM ANALYSIS AND EVALUATION.—Not later than 90 days after the date of enactment of this subsection, the Secretary shall establish an Office of Program Analysis and Evaluation within the Department (in this section referred to as the "Office").

(2) * * *

(3) * * *

[(4) REORGANIZATION.—

[(A) IN GENERAL.—The Secretary may allocate or reallocate the functions of the Office, or discontinue the Office, in accordance with section 872(a).

[(B) EXEMPTION FROM LIMITATIONS.—Section 872(b) shall not apply to any action by the Secretary under this paragraph.][149]

[(c)]*(d)* * * *

SECTION 703. CHIEF INFORMATION OFFICER.

(a) IN GENERAL.—The Chief Information Officer shall report to the Secretary[, or to another official of the Department, as the Secretary may direct]. In addition to the functions under section 3506(a)(2) of title 44, United States Code, and section 11319 of title 40, United States Code, the Chief Information Officer shall—

(1) serve as the lead technical authority for information technology programs of the Department and components of the Department; and

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

(b) STRATEGIC PLANS.—

(1) IN GENERAL.—The Chief Information Officer shall, in coordination with the Chief Financial Officer, develop an information technology strategic plan every 5 years and report to the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate on the extent to which—

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

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

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

(D) unnecessary duplicative information technology within and across the components of the Department has been eliminated;

(E) outcome-oriented goals, quantifiable performance measures, and strategies for achieving those goals and measures have succeeded; and

(F) internal control weaknesses and how the Department will address those weaknesses.

(2) INITIAL PLAN.—Not later than 1 year after the date of enactment of this subsection, the Chief Information Officer shall complete the first information technology strategic plan required under paragraph (1).

[(b)] *(c)* * * *

[149] The bill as reported by the Committee retained a provision in H.R. 2825 as passed by the House of Representatives that would have removed Section 872 of the Homeland Security Act of 2002. Retaining this provision of the House bill was a drafting error by the Committee that will be corrected before any action is taken by the full Senate on the bill on the floor. The Chairman favors DHS retaining its ability to reorganize under Section 872.

(d) ACQUISITION RESPONSIBILITIES.—The acquisition responsibilities of the Chief Information Officer shall include—

(1) overseeing the management of the Homeland Security Enterprise Architecture and ensuring that, before each acquisition decision event, approved information technology acquisitions comply with departmental information technology management processes, technical requirements, and the Homeland Security Enterprise Architecture, and in any case in which information technology acquisitions do not comply with the management directives of the Department, making recommendations to the Acquisition Review Board regarding that noncompliance; and

(2) being responsible for—

(A) providing recommendations to the Acquisition Review Board regarding information technology programs; and

(B) developing information technology acquisition strategic guidance.

SEC. 704. CHIEF HUMAN CAPITAL OFFICER.

(a) * * *

(b) * * *

(1) develop and implement strategic workforce planning policies that are consistent with Government-wide leading principles **[**and in line**]**, *in line* with Department strategic human capital goals and priorities, *and informed by successful practices within the Federal Government and the private sector* taking into account the special requirements of members of the Armed Forces serving in the Coast Guard;

(2) **[**develop performance measures to provide a basis for monitoring and evaluating**]** *develop performance measures to monitor and evaluate on an ongoing basis,* Department-wide strategic workforce planning efforts;

(3) *assess the need of administrative and mission support staff across the Department, to identify and eliminate the unnecessary use of mission-critical staff for administrative and mission support positions;*

[(3)**]***(4)* * * *

[(4)**]***(5)* identify methods for managing and overseeing human capital programs and initiatives, *including leader development and employee engagement programs* in coordination with the head of each component of the Department;

[(5)**]***(6)* develop a career path framework and create opportunities for leader development in coordination with all components of the Department *that is informed by appropriate workforce planning initiatives;*

[(6)**]***(7)* * * *

[(7)**]***(8)* * * *

[(8)**]***(9)* * * *

(10) maintain a catalogue of available employee development opportunities easily accessible to employees of the Department, including departmental leadership development programs, interagency development programs, and rotational programs;

(11) approve the selection and organizational placement of each senior human capital official of each component of the Department and participate in the periodic performance reviews of each such senior human capital official;

(12) assess the success of the Department and the components of the Department regarding efforts to recruit and retain employees in rural and remote areas, and make policy recommendations as appropriate to the Secretary and to Congress;

(13) develop performance measures to monitor and evaluate on an ongoing basis any significant contracts issued by the Department or a component of the Department to a private entity regarding the recruitment, hiring, or retention of employees;

[(9)**]***(14)* * * *

[(10)**]***(15)* * * *

SEC. 705. [ESTABLISHMENT OF OFFICER FOR] CIVIL RIGHTS AND CIVIL LIBERTIES.

(a) IN GENERAL.—The **[**Officer for Civil Rights and Civil Liberties**]** *Chief Civil Rights and Civil Liberties Officer,* who shall report directly to he Secretary, shall—

(1) * * *

(2) make public through the Internet, radio, television, or newspaper advertisements information on the responsibilities and functions of, and how to contact, the *Chief* Officer;

* * * * * * *

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

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

(2) Investigating complaints and information indicating possible abuses of civil rights or civil liberties, unless the Inspector General of the Department determines that any such complaint or information should be investigated by the Inspector General.

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

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

(5) Any other activities as assigned by the Chief Civil Rights and Civil Liberties Officer.

(c) COMPONENT CIVIL RIGHTS AND CIVIL LIBERTIES OFFICERS.—

(1) IN GENERAL.—In consultation with the Chief Civil Rights and Civil Liberties Officer, the head of each component of the Department shall appoint a senior-level Federal employee with experience and background in civil rights and civil liberties as the Civil Rights and Civil Liberties Officer for the component.

(2) RESPONSIBILITIES.—Each Civil Rights and Civil Liberties Officer appointed under paragraph (1) shall—

(A) serve as the main point of contact for the Chief Civil Rights and Civil Liberties Officer; and

(B) coordinate with the Chief Civil Rights and Civil Liberties Officer to oversee the integration of civil rights and civil liberties into the activities of the component.

[(b)**]** *(d)* * * *

[SEC. 706. CONSOLIDATION AND CO–LOCATION OF OFFICES.]

[SEC. 707.] *SEC. 706.* QUADRENNIAL HOMELAND SECURITY REVIEW.

(a) REQUIREMENT.—

(1) * * *

(2) * * *

(3) CONSULTATION.—The Secretary shall conduct each quadrennial homeland security review under this subsection in consultation with—

(A) * * *

(B) key officials of the Department, including the Under Secretary for Strategy, Policy, and Plans; **[**and**]**

(C) *representatives from appropriate advisory committees established pursuant to section 871, including the Homeland Security Advisory Council and the Homeland Security Science and Technology Advisory Committee, or otherwise established, including the Aviation Security Advisory Committee established pursuant to section 44946 of title 49, United States Code; and*

[(C)**]** *(D)* * * *

(b) CONTENTS OF REVIEW.—In each quadrennial homeland security review, the Secretary shall—

(1) delineate and update, as appropriate, the national homeland security strategy, consistent with appropriate national and Department strategies, strategic plans, and Homeland Security Presidential Directives, including the National Strategy for Homeland Security, the **[**National Response Plan**]** *National Response Framework*, and the Department Security Strategic Plan;

(2) outline and prioritize the full range of the critical homeland security mission areas of the Nation *based on the risk assessment required pursuant to subsection (c)(2)(B)*;

(3) describe *to the extent practicable* the interagency cooperation, preparedness of Federal response assets, infrastructure, **[**budget plan**]***resources required,* and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy, required to execute successfully the full range of missions called for in the national homeland security strategy described in paragraph (1) and the homeland security mission areas outlined under paragraph (2);

(4) identify*, to the extent practicable,* the **[**budget plan required to provide sufficient resources to successfully**]***resources required* to execute the full range of missions called for in the national homeland security strategy described in paragraph (1) and the homeland security mission areas outlined under paragraph (2)**[**;**]***, including any resources identified from redundant, wasteful, or unnecessary capabilities and capacities that can be redirected to better support other existing capabilities and capacities, as the case may be; and*

(5) include an assessment of the organizational alignment of the Department with the national homeland security strategy referred to in paragraph (1) and the homeland security mission areas outlined under paragraph (2)**[**; and**]**.

[(6) review and assess the effectiveness of the mechanisms of the Department for executing the process of turning the re-

quirements developed in the quadrennial homeland security review into an acquisition strategy and expenditure plan within the Department.]

(c) REPORTING.—

(1) IN GENERAL.—Not later than [December 31]*September 30* of the year in which a quadrennial homeland security review is conducted, the Secretary shall submit to Congress a report regarding that quadrennial homeland security review.

(2) CONTENTS OF REPORT.—Each report submitted under paragraph (1) shall include—

(A) * * *

(B) a [description of the threats to]*risk assessment of* the assumed or defined national homeland security interests of the Nation that were examined for the purposes of that review;

(C) the national homeland security strategy, including a prioritized list of the critical homeland security missions of the nation, *as required under subsection (b)(2)*;

(D) *to the extent practicable* a description of the interagency cooperation, preparedness of Federal response assets, infrastructure, [budget plan]*resources required*, and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy, required to execute successfully the full range of missions called for in the applicable national homeland security strategy referred to in subsection (b)(1) and the homeland security mission areas outlined under subsection (b)(2);

(E) * * *

(F) *to the extent practicable* a discussion of [the status of] cooperation among Federal agencies in the effort to promote national homeland security;

(G) *to the extent practicable* a discussion of [the status of] cooperation between the Federal Government and State, local, and tribal governments in preventing terrorist attacks and preparing for emergency response to threats *and risks* to national homeland security; *and*

[(H) an explanation of any underlying assumptions used in conducting the review; and]

[(I)] *(H)* any other matter the Secretary considers appropriate.

(3) DOCUMENTATION.—The Secretary shall retain, from each quadrennial homeland security review, all information regarding the risk assessment, as required under subsection (c)(2)(B), including—

(A) the risk model utilized to generate the risk assessment;

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

(C) sources of information, including other risk assessments, utilized to generate the risk assessment.

[(3)] *(4)* PUBLIC AVAILABILITY.—The Secretary shall, consistent with the protection of national security and other sensitive matters, make each report submitted under paragraph

(1) publicly available on the Internet website of the Department.

(d) REVIEW.—Not later than 90 days after the submission of each report required under subsection (c)(1), the Secretary shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the degree to which the findings and recommendations developed in the quadrennial homeland security review covered by the report were integrated into the acquisition strategy and expenditure plans for the Department.

[(d)**]** *(e)* AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out this section.

[SEC. 708] ***SEC. 707***. * * *

[SEC. 709] ***SEC. 708***. **OFFICE OF STRATEGY, POLICY, AND PLANS.**

(a) * * *

(b) * * *

(c) FUNCTIONS.—The Under Secretary for Strategy, Policy, and Plans shall—

(1) * * *

(2) * * *

(3) develop and coordinate strategic plans and long-term goals of the Department with risk-based analysis and planning to improve operational mission effectiveness, including consultation with the Secretary regarding the quadrennial homeland security review under **[**section 707**]** *section 706*;

(4) * * *

(5) * * *

(6) enter into agreements with governments of other countries, in consultation with the Secretary of State or the head of another agency, as appropriate, international organizations, and international nongovernmental organizations in order to achieve the missions of the Department;

[(6)**]** *(7)* review and incorporate, as appropriate, external stakeholder feedback, *including feedback from organizations representing the needs of children* into Department policy; and

[(7)**]** *(8)* * * *

SEC. 709. CHIEF PROCUREMENT OFFICER.

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

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

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

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

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

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

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

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

(7) approve the selection and organizational placement of each head of contracting activity within the Department and participate in the periodic performance reviews of each head of contracting activity of the Department;

(8) ensure that a fair proportion of the value of Federal contracts and subcontracts are awarded to small business concerns, as defined under section 3 of the Small Business Act (15 U.S.C. 632), (in accordance with the procurement contract goals under section 15(g) of the Small Business Act (15 U.S.C. 644(g)), maximize opportunities for small business participation in such contracts, and ensure, to the extent practicable, small business concerns that achieve qualified vendor status for security-related technologies are provided an opportunity to compete for contracts for such technology; and

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

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

SEC. 710. CHIEF SECURITY OFFICER.

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

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

(1) develop, implement, and oversee compliance with the security policies, programs, and standards of the Department;

(2) participate in—

(A) the selection and organizational placement of each senior security official of a component, and the deputy for each such official, and any other senior executives responsible for security-related matters; and

(B) the periodic performance planning and reviews;

(3) identify training requirements, standards, and oversight of education to Department personnel on security-related matters;

(4) develop security programmatic guidelines;

(5) review contracts and interagency agreements associated with major security investments within the Department; and

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

SEC. 711. ANNUAL SUBMITTAL TO CONGRESS OF INFORMATION ON REPROGRAMMING OR TRANSFERS OF FUNDS TO RESPOND TO OPERATIONAL SURGES.

For each fiscal year until fiscal year 2023, the Secretary shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, together with the annual budget request for the Department, information on—

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

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

SEC. 712. CHIEF FACILITIES AND LOGISTICS OFFICER.

(a) IN GENERAL.—There is a Chief Facilities and Logistics Officer of the Department who shall report directly to the Under Secretary for Management. The Chief Facilities and Logistics Officer shall be career reserved for a member of the senior executive service.

(b) RESPONSIBILITIES.—The Chief Facilities and Logistics Officer shall—

(1) develop policies and procedures and provide program oversight to manage real property, facilities, environmental and energy programs, personal property, mobile assets, equipment, and other material resources of the Department;

(2) manage and execute, in consultation with the component heads, mission support services within the National Capital Region for real property, facilities, environmental and energy programs, and other common headquarters and field activities for the Department; and

(3) provide tactical and transactional services for the Department in the National Capital Region, including transportation, facility operations, and maintenance.

SEC. 713. LONG TERM REAL PROPERTY STRATEGIES.

(a) IN GENERAL.—

(1) FIRST STRATEGY.—Not later than 180 days after the date of enactment of this section, the Under Secretary for Management, in consultation with the Administrator of General Services, shall develop an initial 5-year regional real property strategy for the Department that covers the 5-fiscal-year period immediately following such date of enactment. Such strategy shall be geographically organized, as designated by the Under Secretary for Management.

(2) SECOND STRATEGY.—Not later than the first day of the fourth fiscal year covered by the first strategy under paragraph (1), the Under Secretary for Management, in consultation with the Administrator of General Services, shall develop a second 5-year real property strategy for the Department that covers the 5 fiscal years immediately following the conclusion of the first strategy.

(b) REQUIREMENTS.—

(1) INITIAL STRATEGY.—The initial 5-year strategy developed in accordance with subsection (a)(1) shall—

(A) identify opportunities to consolidate real property, optimize the usage of Federal assets, and decrease the number of commercial leases and square footage within the Department's real property portfolio;

(B) provide alternate housing and consolidation plans to increase efficiency through joint use of Department spaces while decreasing the cost of leased space;

(C) concentrate on geographical areas with a significant Department presence, as identified by the Under Secretary for Management;

5 (D) examine the establishment of central Department locations in each such geographical region and the co-location of Department components based on the mission sets and responsibilities of such components;

(E) identify opportunities to reduce overhead costs through co-location or consolidation of real property interests or mission support activities, such as shared mail screening and processing, centralized transportation and shuttle services, regional transit benefit programs, common contracting for custodial and other services, and leveraging strategic sourcing contracts and sharing of specialized facilities, such as training facilities and resources;

(F) manage the current Department Workspace Standard for Office Space in accordance with the Department office workspace design process to develop the most efficient and effective spaces within the workspace standard usable square foot ranges for all leased for office space entered into on or after the date of the enactment of this section, including the renewal of any leases for office space existing as of such date;

(G) define, based on square footage, what constitutes a major real property acquisition;

(H) prioritize actions to be taken to improve the operations and management of the Department's real property inventory, based on life-cycle cost estimations, in consultation with component heads;

(I) include information on the headquarters consolidation project of the Department, including—

(i) an updated list of the components and offices to be included in the project;

(ii) a comprehensive assessment of the current and future real property required by the Department at the site; and

(iii) updated cost and schedule estimates; and

(J) include any additional information determined appropriate or relevant by the Under Secretary for Management.

(2) SECOND STRATEGY.—The second 5-year strategy developed in accordance with subsection (a)(2) shall include information required in subparagraphs (A), (B), (C), (E), (F), (G), (H), (I), and (J) of paragraph (1) and information on the effectiveness of implementation efforts pursuant to the Department-wide policy required in accordance with subsection (c), including—

(A) the impact of such implementation on departmental operations and costs; and

(B) the degree to which the Department established central Department locations and co-located Department components pursuant to the results of the examination required by paragraph (1)(D).

(c) IMPLEMENTATION POLICIES.—Not later than 90 days after the development of each of the regional real property strategies developed in accordance with subsection (a), the Under Secretary for Management shall develop or update, as applicable, a Department-wide policy implementing such strategies.

(d) CERTIFICATIONS.—Subject to subsection (g)(3), the implementation policies developed pursuant to subsection (c) shall require component heads to certify to the Under Secretary for Management that such heads have complied with the requirements specified in subsection (b) before making any major real property decision or recommendation, as defined by the Under Secretary, including matters related to new leased space, renewing any existing leases, or agreeing to extend or newly occupy any Federal space or new construction, in accordance with the applicable regional real property strategy developed in accordance with subsection (a).

(e) UNDERUTILIZED SPACE.—

(1) IN GENERAL.—The implementation policies developed pursuant to subsection (c) shall require component heads, acting through regional property managers under subsection (f), to annually report to the Under Secretary for Management on underutilized space and identify space that may be made available for use, as applicable, by other components or Federal agencies.

(2) EXCEPTION.—The Under Secretary for Management may grant an exception to the workspace standard usable square foot ranges described in subsection (b)(1)(F) for specific office locations at which a reduction or elimination of otherwise underutilized space would negatively impact a component's ability to execute its mission based on readiness performance measures or would increase the cost of such space.

(3) UNDERUTILIZED SPACE DEFINED.—In this subsection, the term "underutilized space" means any space with respect to which utilization is greater than the workplace standard usable square foot ranges described in subsection (b)(1)(F).

(f) COMPONENT RESPONSIBILITIES.—

(1) REGIONAL PROPERTY MANAGERS.—Each component head shall identify a senior career employee of each such component for each geographic region included in the regional real property strategies developed in accordance with subsection (a) to serve as each such component's regional property manager. Each such regional property manager shall serve as a single point of contact for Department headquarters and other Department components for all real property matters relating to each such component within the region in which each such component is located, and provide data and any other support necessary for the Department of Homeland Security Regional Mission Support Coordinator strategic asset and portfolio planning and execution.

(2) DATA.—Regional property managers under paragraph (1) shall provide annually to the Under Secretary for Management, via a standardized and centralized system, data on each component's real property holdings, as specified by the Undersecretary

for Management, including relating to underutilized space under subsection (e) (as such term is defined in such subsection), total square footage leased, annual cost, and total number of staff, for each geographic region included in the regional real property strategies developed in accordance with subsection (a).

(g) ONGOING OVERSIGHT.—

(1) IN GENERAL.—The Under Secretary for Management shall monitor components' adherence to the regional real property strategies developed in accordance with subsection (a) and the implementation policies developed pursuant to subsection (c).

(2) ANNUAL REVIEW.—The Under Secretary for Management shall annually review the data submitted pursuant to subsection (f)(2) to ensure all underutilized space (as such term is defined in subsection (e)) is properly identified.

(3) CERTIFICATION REVIEW.—The Under Secretary for Management shall review, and if appropriate, approve, component certifications under subsection (d) before such components may make any major real property decision, including matters related to new leased space, renewing any existing leases, or agreeing to extend or newly occupy any Federal space or new construction, in accordance with the applicable regional real property strategy developed in accordance with subsection (a).

(4) CONGRESSIONAL REPORTING.—The Under Secretary for Management shall annually provide information to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Inspector General of the Department on the real property portfolio of the Department, including information relating to the following:

(A) A summary of the Department's real property holdings in each region described in the regional strategies developed in accordance with subsection (a), and for each such property, information including the total square footage leased, the total cost, the total number of staff at each such property, and the square foot per person utilization rate for office space (and whether or not such conforms with the workspace standard usable square foot ranges established described in subsection (b)(1)(F)).

(B) An accounting of all underutilized space (as such term is defined in subsection (e)).

(C) An accounting of all instances in which the Department or its components consolidated their real property holdings or co-located with another entity within the Department.

(D) A list of all certifications provided pursuant to subsection (d) and all such certifications approved pursuant to paragraph (3) of this subsection.

(5) INSPECTOR GENERAL REVIEW.—Not later than 120 days after the last day of the fifth fiscal year covered in each of the initial and second regional real property strategies developed in accordance with subsection (a), the Inspector General of the Department shall review the information submitted pursuant to paragraph (4) and issue findings regarding the effectiveness of the implementation of the Department-wide policy and over-

sight efforts of the management of real property facilities, personal property, mobile assets, equipment and the Department's other material resources as required under this section.

SEC. 714. WORKFORCE HEALTH AND MEDICAL SUPPORT.

(a) IN GENERAL.—The Under Secretary for Management shall be responsible for workforce-focused health and medical activities of the Department. The Under Secretary for Management may further delegate these responsibilities as appropriate.

(b) RESPONSIBILITIES.—The Under Secretary for Management, in coordination with the Chief Medical Officer, shall—

(1) provide oversight and coordinate the medical and health activities of the Department for the human and animal personnel of the Department;

(2) establish medical, health, veterinary, and occupational health exposure policy, guidance, strategies, and initiatives for the human and animal personnel of the Department;

(3) as deemed appropriate by the Under Secretary, provide medical liaisons to the components of the Department, on a reimbursable basis, to provide subject matter expertise on occupational medical and public health issues;

(4) serve as the primary representative for the Department on agreements regarding the detail of Department of Health and Human Services Public Health Service Commissioned Corps Officers to the Department, except that components and offices of the Department shall retain authority for funding, determination of specific duties, and supervision of Commissioned Corps officers detailed to a Department component; and

(5) perform such other duties relating to such responsibilities as the Secretary may require.

SEC. 715. EMPLOYEE ENGAGEMENT AND RETENTION ACTION PLAN.

(a) IN GENERAL.—The Secretary shall—

(1) not later than 180 days after the date of enactment of this section, and not later than September 30 of each fiscal year thereafter, issue a Department-wide employee engagement and retention action plan to inform and execute strategies for improving employee engagement, employee retention, Department management and leadership, diversity and inclusion efforts, employee morale, training and development opportunities, and communications within the Department, which shall reflect—

(A) input from representatives from operational components, headquarters, and field personnel, including supervisory and non-supervisory personnel, and employee labor organizations that represent employees of the Department;

(B) employee feedback provided through annual employee surveys, questionnaires, and other communications; and

(C) performance measures, milestones, and objectives that reflect the priorities and strategies of the action plan to improve employee engagement and retention; and

(2) require the head of each operational component of the Department to—

(A) develop and implement a component-specific employee engagement and retention plan to advance the action plan required under paragraph (1) that includes performance measures and objectives, is informed by employee feedback

provided through annual employee surveys, questionnaires, and other communications, as appropriate, and sets forth how employees and, if applicable, their labor representatives are to be integrated in developing programs and initiatives;

(B) monitor progress on implementation of such action plan; and

(C) provide to the Chief Human Capital Officer quarterly reports on actions planned and progress made under this paragraph.

(b) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit the ability of the departmental or component leadership from developing innovative approaches and strategies to employee engagement or retention not specifically required under this section.

(c) REPEAL.—This section shall be repealed on the date that is 5 years after the date of enactment of this section.

SEC. 716. ACQUSITION AUTHORITIES FOR PROGRAM ACCOUNTABILITY AND RISK MANAGEMENT.

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

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

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

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

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

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

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

(4) Coordinate the acquisition life cycle review process for the Acquisition Review Board.

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

(6) Support the Chief Procurement Officer in developing strategies and specific plans for hiring, training, and professional

development in order to improve the acquisition workforce of the Department.

(7) In consultation with Component Acquisition Executives—

(A) develop standards for the designation of key acquisition positions with major acquisition program management offices and on the Component Acquisition Executive support staff; and

(B) provide requirements and support to the Chief Procurement Officer in the planning, development, and maintenance of the Acquisition Career Management Program of the Department.

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

(9) Provide technical support and assistance to Department acquisition programs and acquisition personnel and coordinate with the Chief Procurement Officer on workforce training and development activities.

(c) RESPONSIBILITIES OF COMPONENTS.—Each head of a component shall—

(1) comply with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives established by the Under Secretary for Management; and

(2) for each major acquisition program—

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

(B) develop a life cycle cost estimate that is consistent with best practices identified by the Comptroller General of the United States and establish a complete life cycle cost estimate with supporting documentation, including an acquisition program baseline;

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

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

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

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

SEC. 717. ACQUISITION DOCUMENTATION.

(a) IN GENERAL.—For each major acquisition program, the Secretary, acting through the Under Secretary for Management, shall require the head of a relevant component or office to—

(1) maintain acquisition documentation that is complete, accurate, timely, and valid, and that includes, at a minimum—

(A) operational requirements that are validated consistent with departmental policy and changes to those requirements, as appropriate;

(B) a complete life cycle cost estimate with supporting documentation;

(C) verification of the life cycle cost estimate against independent cost estimates, and reconciliation of any differences;

(D) a cost-benefit analysis with supporting documentation; and

(E) a schedule, including, as appropriate, an integrated master schedule;

(2) prepare cost estimates and schedules for major acquisition programs under subparagraphs (B) and (E) of paragraph (1) in a manner consistent with best practices as identified by the Comptroller General of the United States; and

(3) submit certain acquisition documentation to the Secretary to produce a semi-annual Acquisition Program Health Assessment of departmental acquisitions for submission to Congress.

(b) WAIVER.—The Secretary may waive the requirement under subsection (a)(3) on a case-by-case basis with respect to any major acquisition program under this section for a fiscal year if—

(1) the major acquisition program has not—

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

(B) had a reasonable cost estimate established; and

(C) had a system configuration defined fully; or

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

(c) CONGRESSIONAL OVERSIGHT.—At the same time the budget of the President is submitted for a fiscal year under section 1105(a) of title 31, United States Code, the Secretary shall make information available, as applicable, to the congressional homeland security committees regarding the requirement described in subsection (a) in the prior fiscal year that includes, with respect to each major acquisition program for which the Secretary has issued a waiver under subsection (b)—

(1) the grounds for granting a waiver for the program;

(2) the projected cost of the program;

(3) the proportion of the annual acquisition budget of each component or office attributed to the program, as available; and

(4) information on the significance of the program with respect to the operations and the execution of the mission of each component or office described in paragraph (3).

SEC. 718. ACQUISITION INNOVATION.

The Under Secretary for Management shall—

(1) encourage each of the officers under the direction of the Under Secretary for Management to promote innovation and shall designate an individual to promote innovation;

(2) establish an acquisition innovation lab or similar mechanism to improve the acquisition programs, acquisition workforce training, and existing practices of the Department through methods identified in this section;

(3) test emerging and established acquisition best practices for carrying out acquisitions, consistent with applicable laws, regulations, and Department directives, as appropriate;

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

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

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

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

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

(C) incorporating the feedback described in subparagraphs (A) and (B), as appropriate, into future acquisition innovation efforts of the Department.

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle B—Inspector General

* * * * * * *

[SEC. 812.] *SEC. 811.* LAW ENFORCEMENT POWERS OF INSPECTOR GENERAL AGENTS.

[(a)] * * *

[(b) PROMULGATION OF INITIAL GUIDELINES.—

[(1) DEFINITION.—In this subsection,]

(a) DEFINITION.—In this section the term "memoranda of understanding" means the agreements between the Department of Justice and the Inspector General offices described under section 6(e)(3) of the Inspector General Act of 1978 (5 U.S.C. App.) [(as added by subsection (a) of this section)] that—

[(A)]*(1)* are in effect on the date of enactment of this act; and

[(B)]*(2)* authorize such offices to exercise authority that is the same or similar to the authority under section 6(e)(1) of such Act.

[(2)]*(b)* [IN GENERAL] *IN GENERAL.*—Not later than 180 days after the date of enactment of this Act, the Attorney General shall promulgate guidelines under section 6(e)(4) of the Inspector General Act of 1978 (5 U.S.C. App.) [(as added by subsection (a) of this section)] applicable to the Inspector General offices described under section 6(e)(3) of that Act.

[(3)]*(c)* [MINIMUM REQUIREMENTS] *MINIMUM REQUIREMENTS.*—The guidelines promulgated under this subsection shall include, at a minimum, the operational and training requirements in the memoranda of understanding.

[(4)]*(d)* [NO LAPSE OF AUTHORITY] *NO LAPSE OF AUTHORITY.*—The memoranda of understanding in effect on the date of enactment of this Act shall remain in effect until the guidelines promulgated under this subsection take effect.

[(c) [5 U.S.C. app. 6 note] EFFECTIVE DATES.—

[(1) IN GENERAL.—Subsection (a) shall take effect 180 days after the date of enactment of this Act.

[(2) INITIAL GUIDELINES.—Subsection (b) shall take effect on the date of enactment of this Act.]

* * * * * * *

Subtitle D—Acquisitions

* * * * * * *

SEC. 831. RESEARCH AND DEVELOPMENT PROJECTS.

(a) AUTHORITY.—Until September 30, [2017] *2022*, and subject to subsection (d), the Secretary may carry out a pilot program under which the Secretary may exercise the following authorities:

(1) * * *

(2) PROTOTYPE PROJECTS.—The Secretary may, under the authority of paragraph (1), carry out prototype projects in accordance with the requirements and conditions provided for carrying out prototype projects [under section 845 of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103–160). In applying the authorities of that section 845, subsection (c) of that section shall apply with respect to prototype projects under this paragraph, and the Secretary shall perform the functions of the Secretary of Defense under subsection (d) thereof] *under section 2371b of title 10, United States Code, and the Secretary shall perform the functions of the Secretary of Defense as prescribed.*

(b) * * *

(c) ADDITIONAL REQUIREMENTS.

(1) IN GENERAL.—The authority of the Secretary under this section shall terminate September 30, [2017] *2022*, unless before that date the Secretary—

(A) * * *

(B) * * *

[(2) REPORT.—The Secretary shall provide an annual report to the Committees on Appropriations of the Senate and the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives detailing the projects for which the authority granted by subsection (a) was used, the rationale for its use, the funds spent using that authority, the outcome of each project for which that authority was used, and the results of any audits of such projects.]

(2) REPORT.—The Secretary shall annually submit to the Committee on Homeland Security and the Committee on

Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report detailing the projects for which the authority granted by subsection (a) was utilized, the rationale for such utilizations, the funds spent utilizing such authority, the extent of cost-sharing for such projects among Federal and non-Federal sources, the extent to which utilization of such authority has addressed a homeland security capability gap or threat to the homeland identified by the Department, the total amount of payments, if any, that were received by the Federal Government as a result of the utilization of such authority during the period covered by each such report, the outcome of each project for which such authority was utilized, and the results of any audits of such projects.

(d) DEFINITION OF NONTRADITIONAL GOVERNMENT CONTRACTOR.—In this section, the term "nontraditional Government contractor" has the same meaning as the term "nontraditional defense contractor" [as defined in section 845(e) of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103–160; 10 U.S.C. 2371 note)] *as defined in section 2371b(e) of title 10, United States Code.*

(e) TRAINING.—The Secretary shall develop a training program for acquisitions staff on the utilization of the authority provided under subsection (a) to ensure accountability and effective management of projects consistent with the Program Management Improvement Accountability Act (Public Law 114–264; 130 Stat. 1371) and the amendments made by such Act.

* * * * * * *

SEC. 836. ACQUISITION REVIEW BOARD.

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

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

(2) review major acquisition programs; and

(3) review the use of best practices.

(b) COMPOSITION.—

(1) CHAIRPERSON.—The Under Secretary for Management shall serve as chairperson of the board.

(2) OTHER MEMBERS.—The Secretary shall ensure participation by other relevant Department officials.

(c) MEETINGS.—

(1) REGULAR MEETINGS.—The Board shall meet regularly for purposes of ensuring all acquisition programs proceed in a timely fashion to achieve mission readiness.

(2) OTHER MEETINGS.—The Board shall convene—

(A) at the discretion of the Secretary; and

(B) at any time—

(i) a major acquisition program—

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

(II) is in breach of the approved acquisition program baseline of the major acquisition program; or

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

(ii) a non-major acquisition program requires review, as determined by the Under Secretary for management.

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

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

(2) Oversee whether the business strategy, resources, management, and accountability of a proposed acquisition are executable and are aligned to strategic initiatives.

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

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

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

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

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

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

(e) ACQUISITION PROGRAM BASELINE REPORT REQUIREMENT.—If the person exercising acquisition decision authority over a major acquisition program approves the major acquisition program to proceed before the major acquisition program has a Department-approved acquisition program baseline, as required by Department policy—

(1) the Under Secretary for Management shall create and approve an acquisition program baseline report regarding such approval; and

(2) the Secretary shall—

(A) not later than 7 days after the date on which the acquisition decision memorandum is signed, provide written notice of the decision to the appropriate committees of Congress; and

(B) not later than 60 days after the date on which the acquisition decision memorandum is signed, provide the

memorandum and a briefing to the appropriate committees of Congress.

(f) REPORT.—Not later than 1 year after the date of enactment of this section and every year thereafter through fiscal year 2022, the Under Secretary for Management shall provide information to the appropriate committees of Congress on the activities of the Board for the prior fiscal year that includes information relating to—

(1) for each meeting of the Board, any acquisition decision memoranda;

(2) the results of the systematic reviews conducted under subsection (d)(4);

(3) the results of acquisition document reviews required under subsection (d)(5); and

(4) activities to ensure that practices are adopted and implemented throughout the Department under subsection (d)(6).

SEC. 837. CONGRESSIONAL NOTIFICATION AND OTHER REQUIREMENTS FOR MAJOR ACQUISITION PROGRAM BREACH.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term "appropriate committees of Congress" means.—

(1) 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; and

(2) in the case of notice or a report relating to the Coast Guard or the Transportation Security Administration, the committees described in paragraph (1) and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

(b) REQUIREMENTS WITHIN DEPARTMENT IN EVENT OF BREACH.—

(1) NOTIFICATIONS.—

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

(B) NOTIFICATION TO SECRETARY.—If a breach occurs in a major acquisition program and the breach results in a cost overrun greater than 15 percent, a schedule delay greater than 180 days, or a failure to meet any of the performance thresholds from the cost, schedule, or performance parameters specified in the most recently approved acquisition program baseline for the program, the Component Acquisition Executive for the program shall notify the Secretary and the Inspector General of the Department not later than 5 business days after the date on which the Component Acquisition Executive for the program, the head of the component concerned, the Executive Director of the Program Accountability and Risk Management Division, the Under Secretary for Management, and the Deputy Secretary are notified of the breach under subparagraph (A).

(2) REMEDIATION PLAN AND ROOT CAUSE ANALYSIS.—

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

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

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

(ii) provide prior cost estimating information;

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

(I) unrealistic performance expectations;

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

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

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

(V) changes to the scope of the program;

(VI) inadequate program funding or changes in planned out-year funding from one 5-year funding plan to the next 5-year funding plan as outlined in the Future Years Homeland Security Program required under section 874;

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

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

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

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

(vi) in coordination with the Component Acquisition Executive for the program, discuss all options considered, including—

(I) the estimated impact on cost, schedule, or performance of the program if no changes are made to current requirements;

(II) the estimated cost of the program if requirements are modified; and

(III) the extent to which funding from other programs will need to be reduced to cover the cost growth of the program.

(3) REVIEW OF CORRECTIVE ACTIONS.—

(A) IN GENERAL.—The Under Secretary for Management—

(i) shall review each remediation plan required under paragraph (2); and

(ii) not later than 30 days after submission of a remediation plan under paragraph (2), may approve the plan or provide an alternative proposed corrective action.

(B) SUBMISSION TO CONGRESS.—Not later than 30 days after the date on which the Under Secretary for Management completes a review of a remediation plan under subparagraph (A), the Under Secretary for Management shall submit to the appropriate committees of Congress a copy of the remediation plan.

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

(1) NOTIFICATION TO CONGRESS.—If a notification to the Secretary is made under subsection (b)(1)(B) relating to a breach in a major acquisition program, the Under Secretary for Management shall notify the appropriate committees of Congress of the breach in the next semi-annual Acquisition Program Health Assessment described in section 717(a)(3) after receipt by the Under Secretary for Management of the notification under subsection (b)(1)(B).

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

(A) the program is essential to the accomplishment of the mission of the Department;

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

(C) the management structure for the program is adequate to manage and control cost, schedule, and performance; and

(D) includes the date on which the new acquisition schedule and estimates for total acquisition cost will be completed.

SEC. 838. MULTIYEAR ACQUISITION STRATEGY.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this section, the Under Secretary for Management shall brief the appropriate congressional committees on a multiyear acquisition strategy to—

(1) guide the overall direction of the acquisitions of the Department while allowing flexibility to deal with ever-changing threats and risks;

(2) keep pace with changes in technology that could impact deliverables; and

(3) help industry better understand, plan, and align resources to meet the future acquisition needs of the Department.

(b) UPDATES.—The strategy required under subsection (a) shall be updated and included in each Future Years Homeland Security Program required under section 874.

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

SEC. 839. ACQUISITION POLICIES AND GUIDANCE.

(a) PROGRAM ACCOUNTABILITY REPORT.—The Under Secretary for Management shall prepare and submit to the congressional homeland security committees a semi-annual program accountability report to meet the mandate of the Department to perform program health assessments and improve program execution and governance.

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

(1) IDENTIFICATION.—Not later than 60 days after the date of enactment of this section, component heads of the Department shall identify to the Under Secretary for Management all level 3 acquisition programs of each respective component.

(2) CERTIFICATION.—Not later than 30 days after receipt of the information under paragraph (1), the Under Secretary for Management shall certify in writing to the congressional homeland security committees whether the heads of the components of the Department have properly identified the programs described in that paragraph.

(3) METHODOLOGY.—To carry out this subsection, the Under Secretary shall establish a process with a repeatable methodology to continually identify level 3 acquisition programs.

(c) POLICIES AND GUIDANCE.—

(1) SUBMISSION.—Not later than 180 days after the date of enactment of this section, the Component Acquisition Executives shall submit to the Under Secretary for Management the policies and relevant guidance for the level 3 acquisition programs of each component.

(2) CERTIFICATION.—Not later than 90 days after receipt of the policies and guidance under subparagraph (A), the Under Secretary shall certify in writing to the congressional homeland security committees that the policies and guidance of each component adhere to Department-wide acquisition policies.

* * * * * * *

Subtitle E—Human Resource Management

* * * * * * *

SEC. 843. USE OF COUNTERNARCOTICS ENFORCEMENT ACTIVISTS IN CERTAIN EMPLOYEE PERFORMANCE APPRAISALS.

(a) * * *

(b) DEFINITIONS.—For the purposes of this section—

(1) the term "National Drug Control Program Agency" means—

(A) * * *

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

[(i) the counternarcotics officer, appointed under section 878; or

[(ii) if applicable, the counternarcotics officer's successor in function (as determined by the Secretary); and] *by the Secretary; and*

(2) * * *

SEC. 844. HOMELAND SECURITY ROTATION PROGRAM.

[(a) ESTABLISHMENT.—]

[(1)]*(a)* IN GENERAL.—[Not later than 180 days after the date of the enactment of this section, the]*The* Secretary shall establish the Homeland Security Rotation Program (in this section referred to as the Rotation Program) [for employees of the Department] *for certain personnel within the Department*. The Rotation Program shall use applicable best practices, including those from the Chief Human Capital Officers Council.

[(2)]*(b)* GOALS.—The Rotation Program established by the Secretary shall—

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

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

[(A)]*(3)* be established in accordance with the Human Capital Strategic Plan of the Department;

[(B)]*(4) provide* [middle and senior level] employees in the Department the opportunity to broaden their knowledge through exposure to other components of the Department

[(C)]*(5)* * * *

[(D)]*(6)* * * *

[(E)]*(7) seek to improve morale and retention throughout the Department and* invigorate the workforce with exciting and professionally rewarding opportunities;

[(F)]*(8)* * * *

[(G)]*(9)* * * *

[(3)]*(c)* ADMINISTRATION.—

[(A)]*(1)* * * *

[(B)]*(2)* RESPONSIBILITIES.—The Chief Human Capital Officer shall—

[(i)]*(A)* * * *

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

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

[(iv)]*(C)*

[(v)]*(D)*

[(vi)]*(E)*

[(vii)]*(F)*

[(viii)]*(G)*

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

(1) before selecting employees for participation in the Rotation Program, disseminate information broadly within the Department about the availability of the Rotation Program, qualifications for participation in the Rotation Program, including full-time employment within the employing component or office not

less than 1 year, and the general provisions of the Rotation Program;

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

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

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

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

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

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

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

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

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

[(5)**]**(*f*) REPORTING.—Not later than 180 days after the date of the establishment of the Rotation Program, the Secretary shall submit a report on the status of the Rotation Program, including a description of the Rotation Program, the number of employees participating, and how the Rotation Program is used in succession planning and leadership development to the appropriate committees of Congress.

(g) INTELLIGENCE ROTATIONAL ASSIGNMENT PROGRAM.—

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

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

(3) ELIGIBILITY.—The Intelligence Rotational Assignment Program established pursuant to paragraph (1) shall be open to employees serving in existing analyst positions within the Department's intelligence enterprise and other Department employ-

ees as determined appropriate by the Chief Human Capital Officer and the Chief Intelligence Officer.

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

(h) EVALUATION.—The Chief Human Capital Officer, acting through the Under Secretary for Management, shall—

(1) perform regular evaluations of the Homeland Security Rotation Program; and

(2) not later than 90 days after the end of each fiscal year, submit to the Secretary a report detailing the findings of the evaluations under paragraph (1) during that fiscal year, which shall include—

(A) an analysis of the extent to which the program meets the goals under subsection (b);

(B) feedback from participants in the program, including the extent to which rotations have enhanced their performance in their current role and opportunities to improve the program;

(C) aggregated information about program participants; and

(D) a discussion of how rotations can be aligned with the needs of the Department with respect to employee training and mission needs.

* * * * * * *

Subtitle F—Federal Emergency Procurement Flexibility

* * * * * * *

[SEC. 857. REVIEW AND REPORT BY COMPTROLLER GENERAL.]

[SEC. 858.] *SEC. 857. IDENTIFICATION OF NEW ENTRANTS INTO THE FEDERAL MARKETPLACE.*

* * * * * * *

Subtitle H—Miscellaneous Provisions

SEC. 871. ADVISORY COMMITTEES.

* * * * * * *

[SEC. 872. REORGANIZATION.] [150]

* * * * * * *

SEC. 874. FUTURE [YEAR] *YEARS* HOMELAND SECURITY PROGRAM.

[(a) IN GENERAL.—Each budget request submitted to Congress for the Department under section 1105 of title 32, United States Code, shall, at or about the same time, be accompanied by a Future Years Homeland Security Program.**]**

[150] The bill as reported by the Committee retained a provision in H.R. 2825 as passed by the House of Representatives that would have removed Section 872 of the Homeland Security Act of 2002. Retaining this provision of the House bill was a drafting error by the Committee that will be corrected before any action is taken by the full Senate on the bill on the floor. The Chairman favors DHS retaining its ability to reorganize under Section 872.

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

(b) * * *

[(c) EFFECTIVE DATE.—This section shall take effect with respect to the preparation and submission of the fiscal year 2005 budget request for the Department and for any subsequent fiscal year, except that the first Future Years Homeland Security Program shall be submitted not later than 90 days after the Department's fiscal year 2005 budget request is submitted to Congress.]

(c) PROJECTION OF ACQUISITION ESTIMATES.—On and after February 1, 2019 each Future Years Homeland Security Program shall project—

(1) acquisition estimates for the fiscal year for which the budget is submitted and the 4 succeeding fiscal years, with specified estimates for each fiscal year, for all major acquisitions by the Department and each component of the Department; and

(2) estimated annual deployment schedules for all physical asset major acquisitions over the 5-fiscal-year period described in paragraph (1), estimated costs and number of service contracts, and the full operating capability for all information technology major acquisitions.

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

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

* * * * * * *

[SEC. 878. COUNTERNARCOTICS OFFICER.]

[SEC. 879. OFFICE OF INTERNATIONAL AFFAIRS.]

* * * * * * *

[SEC. 881. REVIEW OF PAY AND BENEFIT PLANS]

* * * * * * *

SEC. 884. FEDERAL LAW ENFORCEMENT TRAINING CENTERS

(a) * * *

* * * * * * *

(d) TRAINING RESPONSIBILITIES.—

(1) * * *

(2) * * *

(3) * * *

(4) STRATEGIC PARTNERSHIPS.—

(A) IN GENERAL.—The Director may—

(i) * * *

(ii) coordinate with the [Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department] *Director of Cybersecurity and Infrastructure Security* and with private sector stakeholders, including critical infrastructure owners and operators, to provide training pertinent to improving coordination, security, and resiliency of critical infrastructure

* * * * * * *

SEC. 890B. DEPARTMENT LEADERSHIP COUNCILS.

(a) DEPARTMENT LEADERSHIP COUNCILS.—

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

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

(A) serve as a coordinating forum;

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

(C) establish policies to reduce duplication in acquisition programs; and

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

(3) RELATIONSHIP TO OTHER FORUMS.—The Secretary or Deputy Secretary may delegate the authority to direct the implementation of any decision or guidance resulting from the action of a Department leadership council to any office, component, coordinator, or other senior official of the Department

(b) JOINT REQUIREMENTS COUNCIL.—

(1) DEFINITION OF JOINT REQUIREMENT.—In this subsection, the term "joint requirement" means a condition or capability of multiple operating components of the Department that is required to be met or possessed by a system, product, service, result, or component to satisfy a contract, standard, specification, or other formally imposed document.

(2) ESTABLISHMENT.—The Secretary shall establish within the Department a Joint Requirements Council.

(3) MISSION.—In addition to other matters assigned to the Joint Requirements Council by the Secretary and Deputy Secretary, the Joint Requirements Council shall—

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

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

(C) make prioritized capability recommendations for the joint requirements validated under subparagraph (A) to the Secretary, the Deputy Secretary, or the chairperson of a De-

partment leadership council designated by the Secretary to review decisions of the Joint Requirements Council.

(4) CHAIRPERSON.—The Secretary shall appoint a chairperson of the Joint Requirements Council, for a term of not more than 2 years, from among senior officials of the Department as designated by the Secretary.

(5) COMPOSITION.—The Joint Requirements Council shall be composed of senior officials representing components of the Department and other senior officials as designated by the Secretary.

(6) RELATIONSHIP TO FUTURE YEARS HOMELAND SECURITY PROGRAM.—The Secretary shall ensure that the Future Years Homeland Security Program required under section 874 is consistent with the recommendations of the Joint Requirements Council required under paragraph (3)(C), as affirmed by the Secretary, the Deputy Secretary, or the chairperson of a Department leadership council designated by the Secretary under that paragraph.

* * * * * * *

Subtitle J—Secure Handling of Ammonium Nitrate

* * * * * * *

SEC. 899A. DEPARTMENT LEADERSHIP COUNCILS.

(a) IN GENERAL.—The Secretary shall regulate the sale and transfer of ammonium nitrate by an ammonium nitrate facility in accordance with this subtitle to prevent the misappropriation or use of ammonium nitrate in an act of terrorism. *Such regulations shall be carried out by the Cybersecurity and Infrastructure Security Agency.*

(b) AMMONIUM NITRATE MIXTURES.—Not later than 90 days after the date of the enactment of this subtitle, the Secretary, in consultation with the heads of appropriate Federal departments and agencies (including the Secretary of Agriculture), shall, after notice and an opportunity for comment, establish a threshold percentage for ammonium nitrate in a substance.

SEC. 899B. REGULATION OF THE SALE AND TRANSFER OF AMMONIUM NITRATE.

(a) IN GENERAL.—The Secretary shall regulate the sale and transfer of ammonium nitrate by an ammonium nitrate facility in accordance with this subtitle to prevent the misappropriation or use of ammonium nitrate in an act of terrorism. *Such regulations shall be carried out by the Cybersecurity and Infrastructure Security Agency.*

* * * * * * *

TITLE IX—NATIONAL HOMELAND SECURITY COUNCIL

* * * * * * *

SEC. 903. MEMBERSHIP.

(a) [MEMBERS—]*MEMBERS*.—The members of the Council shall be the following:

(1) The President.

(2) The Vice President.

(3) The Secretary of Homeland Security.

(4) The Attorney General.

(5) The Secretary of Defense.

(6) Such other individuals as may be designated by the President.

(b) * * *

* * * * * * *

TITLE XVI—TRANSPORTATION SECURITY

* * * * * * *

Subtitle B—Transportation Security Administration Acquisition Improvements

SEC. 1611. 5-YEAR TECHNOLOGY INVESTMENT PLAN.

(a) * * *

* * * * * * *

(d) CONTENTS OF PLAN.—The Plan shall include—

(1) an analysis of transportation security risks and the associated capability gaps that would be best addressed by security-related technology, including consideration of the most recent quadrennial homeland security review under [section 707] *section 706*;

* * * * * * *

TITLE XVIII—EMERGENCY COMMUNICATIONS

* * * * * * *

SEC. 1801. [OFFICE OF EMERGENCY COMMUNICATIONS] *EMERGENCY COMMUNICATIONS DIVISION.*

(a) IN GENERAL.—There is established in the Department an [Office of Emergency Communications] *Emergency Communications Division. The Division shall be located in the Cybersecurity and Infrastructure Security Agency.*

[(b) DIRECTOR.—The head of the office shall be the Director for Emergency Communications. The Director shall report to the Assistant Secretary for Cybersecurity and Communications.]

(b) ASSISTANT DIRECTOR.—The head of the Division shall be the Assistant [Director for Emergency Communications]. The Assistant Director shall report to the Director of Cybersecurity and Infrastructure Security. All decisions of the Assistant Director that entail the exercise of significant authority shall be subject to the approval of the Director of Cybersecurity and Infrastructure Security.

(c) RESPONSIBILITIES.—The *Assistant* Director for Emergency Communications shall—

(1) * * *

(2) * * *

[(3) administer the Department's responsibilities and authorities relating to the Integrated Wireless Network program;]

[(4)](3) * * *

[(5)](4) * * *

[(6)](5) * * *

[(7)](6) * * *

[(8)](7) * * *

[(9)](8) * * *

[(10)](9) * * *

[(11)](10) * * *

[(12)](11) review, in consultation with the [Assistant Secretary for Grants and Training] *Administrator of the Federal Emergency Management Agency*, all interoperable emergency communications plans of Federal, State, local, and tribal governments, including Statewide and tactical interoperability plans, developed pursuant to homeland security assistance administered by the Department, but excluding spectrum allocation and management related to such plans;

[(13)](12) * * *

[(14)](13) perform such other duties of the Department necessary to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; [and]

(14) administer the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) programs, or successor programs;

(15) assess the impact of emerging technologies on interoperable emergency communications; [and]

(16) fully participate in the mechanisms required under section 2202(c)(8); and

[(15)][(16)] *(17)* perform other duties of the Department necessary to achieve the goal of and maintain and enhance interoperable emergency communications capabilities.

(d) PERFORMANCE OF PREVIOUSLY TRANSFERRED FUNCTIONS.—The Secretary shall transfer to, and administer through, the *Assistant* Director for Emergency Communications the following programs and responsibilities:

(1) * * *

[(2) The responsibilities of the Chief Information Officer related to the implementation of the Integrated Wireless Network.]

[(3)](2) The Interoperable Communications Technical Assistance Program.

(e) COORDINATION.—The *Assistant* Director for Emergency Communications shall coordinate—

(1) * * *

(2) * * *

[(f) SUFFICIENCY OF RESOURCES PLAN.—

[(1) REPORT.—Not later than 120 days after the date of enactment of this section, the Secretary shall submit to Congress a report on the resources and staff necessary to carry out fully the responsibilities under this title.

[(2) COMPTROLLER GENERAL REVIEW.—The Comptroller General shall under paragraph (1). Not later than 60 days after the date on which such report is submitted, the Comptroller General shall submit to Congress a report containing the findings of such review.]

(f) *ANNUAL REPORTING OF DIVISION ACTIVITIES.—The Assistant [Director for Emergency Communications] shall, not later than 1 year after the date of the enactment of this subsection and annually thereafter for each of the next 4 years, report to the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on the activities and programs of the Emergency Communications Division, including specific information on efforts to carry out paragraphs (3), (4), and (5) of subsection (c).*

SEC. 1802. NATIONAL EMERGENCY COMMUNICATIONS PLAN.

(a) IN GENERAL.—The Secretary, acting through the [Director for Emergency Communications] *Assistant Director for Emergency Communications*[, and in cooperation with the Department of National Communications System (as appropriate),] shall, in cooperation with State, local, and tribal governments, Federal departments and agencies, emergency response providers, and the private sector, develop not later than 180 days after the completion of the baseline assessment under section 1803, and periodically, *but not less than once every 5 years*, update, a National Emergency Communications Plan to provide recommendations regarding how the United States should—

(1) * * *
(2) * * *

(b) * * *

(c) CONTENTS.—The National Emergency Communications Plan shall—

(1) * * *
(2) * * *
(3) consider the impact of emerging technologies on the attainment of interoperable emergency communications;
[(3)]*(4)* * * *
[(4)]*(5)* * * *
[(5)]*(6)* * * *
[(6)]*(7)* * * *
[(7)]*(8)* * * *
[(8)]*(9)* * * *
[(9)]*(10)* * * *
[(10)]*(11)* * * *

SEC. 1803. ASSESSMENTS AND REPORTS.

(a) BASELINE ASSESSMENT.—Not later than 1 year after the date of enactment of this section and not less than every 5 years thereafter, the Secretary, acting through the [Director for Emergency Communications] *Assistant Director for Emergency Communications*, shall conduct an assessment of Federal, State, local, and tribal governments that—

* * * * * * *

(d) PROGRESS REPORTS.—Not later than one year after the date of enactment of this section and biennially thereafter, the Sec-

retary, acting through the [Director for Emergency Communications] *Assistant Director for Emergency Communications*, shall submit to Congress a report on the progress of the Department in achieving the goals of, and carrying out its responsibilities its responsibilities under, this title, including—

* * * * * * *

SEC. 1804. COORDINATION OF DEPARTMENT EMERGENCY COMMUNICATIONS GRANT PROGRAMS.

(a) COORDINATION OF GRANTS AND STANDARDS PROGRAMS.—The Secretary, acting through the [Director for Emergency Communications] *Assistant Director for Emergency Communications*, shall ensure that grant guidelines for the use of homeland security assistance administered by the Department relating to interoperable emergency communications are coordinated and consistent with the goals and recommendations in the National Emergency Communications Plan under section 1802.

(b) DENIAL OF ELIGIBILITY FOR GRANTS.—

(1) IN GENERAL.—The Secretary, acting through the [Assistant Secretary for Grants and Planning]*Administrator of the Federal Emergency Management Agency*, and in consultation with the [[Director for Emergency Communications]] *Assistant [Director for Emergency Communications],* may prohibit any State, local, or tribal government from using homeland security assistance administered by the Department to achieve, maintain, or enhance emergency communications capabilities, if—

* * * * * * *

SEC. 1809. INTEROPERABLE EMERGENCY COMMUNICATIONS GRANT PROGRAM.

(a) * * *

(b) POLICY.—The [Director for Emergency Communications] *Assistant Director for Emergency Communications* shall ensure that a grant awarded to a State under this section is consistent with the policies established pursuant to the responsibilities and authorities of the [Office of Emergency Communications] *Emergency Communications Division* under this title, including ensuring that activities funded by the grant—

(1) * * *

(2) * * *

(c) ADMINISTRATION.—

(1) * * *

(2) GUIDANCE.—In administering the grant program, the Administrator shall ensure that the use of grants is consistent with guidance established by the [Director of Emergency Communications] *Assistant Director for Emergency Communications* pursuant to section 7303(a)(1)(H) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(a)(1)(H)).

(d) * * *

(e) APPROVAL OF PLANS.—

(1) APPROVAL AS CONDITION OF GRANT.—Before a State may receive a grant under this section, the [Director of Emergency Communications] *Assistant Director for Emergency Communications* shall approve the State's Statewide Interoperable

Communications Plan required under section 7303(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(f)).

(2) PLAN REQUIREMENTS.—In approving a plan under this subsection, [the Director of Emergency Communications] *the Assistant Director of Emergency Communications* shall ensure that the plan—(A) is designed to improve interoperability at the city, county, regional, State and interstate level; (B) considers any applicable local or regional plan; and (C) complies, to the maximum extent practicable, with the National Emergency Communications Plan under section 1802.

(3) APPROVAL OF REVISIONS.—The [Director] *Assistant Director* of Emergency Communications may approve revisions to a State's plan if [the Director] *the Assistant Director* determines that doing so is likely to further interoperability.

* * * * * * *

(m) REPORTS.—

(1) ANNUAL REPORTS BY STATE GRANT RECIPIENTS.—A State that receives a grant under this section shall annually submit to the [Director] *Assistant Director* of Emergency Communications a report on the progress of the State in implementing that State's Statewide Interoperable Communications Plans required under section 7303(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(f)) and achieving interoperability at the city, county, regional, State, and interstate levels. [The Director] *The Assistant Director* shall make the reports publicly available, including by making them available on the Internet website of the [Office of Emergency Communications] *Cybersecurity and Infrastructure Security Agency*, subject to any redactions that [the Director determines] *the Assistant Director determines* are necessary to protect classified or other sensitive information.

(2) ANNUAL REPORTS TO CONGRESS.—At least once each year, the [Director of Emergency Communications] *Assistant Director for Emergency Communications* shall submit to Congress a report on the use of grants awarded under this section and any progress in implementing Statewide Interoperable Communications Plans and improving interoperability at the city, county, regional, State, and interstate level, as a result of the award of such grants.

* * * * * * *

SEC. 1810. BORDER INTEROPERABILITY DEMONSTRATION PROJECT.

(a) IN GENERAL.—

(1) ESTABLISHMENT.—The Secretary acting through the [Director of the Office of Emergency Communications (referred to in this section as the "Director")] *Assistant Director for Emergency Communications (referred to in this section as the "Assistant Director")*, and in coordination with the Federal Communications Commission and the Secretary of Commerce, shall establish an International Border Community Interoperable Communications Demonstration Project (referred to in this section as the "demonstration project").

(2) MINIMUM NUMBER OF COMMUNITIES.—The [Director] *Assistant Director* shall select no fewer than 6 communities to participate in a demonstration project.

(3) * * *

(b) CONDITIONS.—[The Director] *The Assistant Director*, in coordination with the Federal Communications Commission and the Secretary of Commerce, shall ensure that the project is carried out as soon as adequate spectrum is available as a result of the 800 megahertz rebanding process in border areas, and shall ensure that the border projects do not impair or impede the rebanding process, but under no circumstances shall funds be distributed under this section unless the Federal Communications Commission and the Secretary of Commerce agree that these conditions have been met.

(c) PROGRAM REQUIREMENTS.—Consistent with the responsibilities of the [Office of Emergency Communications] *Emergency Communications Division* under section 1801, the [Director] *Assistant Director* shall foster local, tribal, State, and Federal interoperable emergency communications, as well as interoperable emergency communications with appropriate Canadian and Mexican authorities in the communities selected for the demonstration project. The [Director] *Assistant Director* shall—

(1) * * *

* * * * * * *

(6) take other actions or provide equipment as the [Director] *Assistant Director* deems appropriate to foster interoperable emergency communications.

(d) DISTRIBUTION OF FUNDS.—

(1) * * *

(2) * * *

(3) REPORT.—Not later than 90 days after a State receives funds under this subsection the State shall report to the [Director] *Director* on the status of the distribution of such funds to local and tribal governments.

(e) MAXIMUM PERIOD OF GRANTS.—The [Director] *Assistant Director* may not fund any participant under the demonstration project for more than 3 years.

(f) TRANSFER OF INFORMATION AND KNOWLEDGE.—The [Director] *Assistant Director* shall establish mechanisms to ensure that the information and knowledge gained by participants in the demonstration project are transferred among the participants and to other interested parties, including other communities that submitted applications to the participant in the project.

* * * * * * *

TITLE XIX—[DOMESTIC NUCLEAR DETECTION OFFICE] *COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE*

SEC. 1900. DEFINITIONS.

In this title:

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

(2) OFFICE.—The term "Office" means the Countering Weapons of Mass Destruction Office established under section 1901(a).

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

[SEC. 1901. DOMESTIC NUCLEAR DETECTION OFFICE.]

Subtitle A—Countering Weapons of Mass Destruction Office

SEC. 1901. COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE.

(a) ESTABLISHMENT.—There is established in the Department a Countering Weapons of Mass Destruction Office.

(b) ASSISTANT SECRETARY.—The Office shall be headed by an Assistant Secretary for the Countering Weapons of Mass Destruction Office, who shall be appointed by the President.

(c) RESPONSIBILITIES.—The Assistant Secretary shall serve as the Secretary's principal advisor on—

(1) weapons of mass destruction matters and strategies; and

(2) coordinating the efforts to counter weapons of mass destruction.

[SEC. 1905. RELATIONSHIP TO OTHER DEPARTMENT ENTITIES AND FEDERAL AGENCIES.]

Subtitle B—Mission of the Office

SEC. 1921. MISSION OF THE OFFICE.

The Office shall be responsible for coordinating with other Federal efforts and developing departmental strategy and policy to plan, detect, or protect against the importation, possession, storage, transportation, development, or use of unauthorized chemical, biological, radiological, or nuclear materials, devices, or agents, in the United States and to protect against an attack using such materials, devices, or agents against the people, territory, or interests of the United States.

SEC. 1922. RELATIONSHIP TO OTHER DEPARTMENT ENTITIES AND FEDERAL AGENCIES.

(a) IN GENERAL.—The authority of the Assistant Secretary under this title shall neither affect nor diminish the authority or the responsibility of any officer of the Department or of any officer of any other department or agency of the United States with respect to the command, control, or direction of the functions, personnel, funds, assets, and liabilities of any entity within the Department or any Federal department or agency.

(b) FEDERAL EMERGENCY MANAGEMENT AGENCY.—Nothing in this title or any other provision of law may be construed to affect or reduce the responsibilities of the Federal Emergency Management Agency or the Administrator of the Agency, including the diversion of any asset, function, or mission of the Agency or the Administrator of the Agency.

[SEC. 1902. MISSION OF OFFICE] ***SEC. 1923. RESPONSIBILITIES.***

(a) * * *

(1) * * *

* * * * * * *

(10) * * *

(11) establish, within the [Domestic Nuclear Detection Office] *Countering Weapons of Mass Destruction Office*, the National Technical Nuclear Forensics Center to provide centralized stewardship, planning, assessment, gap analysis, exercises, improvement, and integration for all Federal nuclear forensics and attribution activities—

* * * * * * *

[SEC. 1903.] ***SEC. 1924.*** **HIRING AUTHORITY.**

[SEC. 1904.] ***SEC. 1925.*** **TESTING AUTHORITY.**

(a) IN GENERAL.—The Director shall coordinate with the responsible Federal agency or other entity to facilitate the use by the Office, by its contractors, or by other persons or entities, of existing Government laboratories, centers, ranges, or other testing facilities for the testing of materials, equipment, models, computer software, and other items as may be related to the missions identified in [section 1902] *section 1923*. Any such use of Government facilities shall be carried out in accordance with all applicable laws, regulations, and contractual provisions, including those governing security, safety, and environmental protection, including, when applicable, the provisions of section 309. The Office may direct that private sector entities utilizing Government facilities in accordance with this section pay an appropriate fee to the agency that owns or operates those facilities to defray additional costs to the Government resulting from such use.

* * * * * * *

[SEC. 1906.] ***SEC. 1926.*** **CONTRACTING AND GRANT MAKING AUTHORITIES.**

The Secretary, acting through the [Director for Domestic Nuclear Detection] *Assistant Secretary for the Countering Weapons of Mass Destruction Office*, in carrying out the responsibilities under paragraphs (6) and (7) of section [1902(a)] *1923(a)* of this title, shall—

(1) operate extramural and intramural programs and distribute funds through grants, cooperative agreements, and other transactions and contracts;

(2) ensure that activities under paragraphs (6) and (7) of section [1902(a)] *1923(a)* of this title include investigations of radiation detection equipment in configurations suitable for deployment at seaports, which may include underwater or water surface detection equipment and detection equipment that can be mounted on cranes and straddle cars used to move shipping containers; and

(3) have the authority to establish or contract with 1 or more federally funded research and development centers to provide independent analysis of homeland security issues and carry out other responsibilities under this subchapter.

[SEC. 1907.] *SEC. 1927.* JOINT ANNUAL INTERAGENCY REVIEW OF GLOBAL NUCLEAR DETECTION ARCHITECTURE.

(a) ANNUAL REVIEW.—

(1) * * *

(A) * * *

(B) * * *

(C) the [Director of the Domestic Nuclear Detection Office] *Assistant Secretary for the Countering Weapons of Mass Destruction Office* and each of the relevant departments that are partners in the National Technical Forensics Center—

* * * * * * *

(c) DEFINITION.—In this section, the term global nuclear detection architecture means the global nuclear detection architecture developed under [section 1902] *section 1923* of this title.

* * * * * * *

SUBTITLE C—CHIEF MEDICAL OFFICER

SEC. 1931. CHIEF MEDICAL OFFICER.

(a) IN GENERAL.—There is in the Department a Chief Medical Officer, who shall be appointed by the Secretary. The Chief Medical Officer shall report to the Assistant Secretary.

(b) QUALIFICATIONS.—The individual appointed as Chief Medical Officer shall be a licensed physician possessing a demonstrated ability in and knowledge of medicine and public health.

(c) RESPONSIBILITIES.—The Chief Medical Officer shall have the responsibility within the Department for medical issues related to natural disasters, acts of terrorism, and other man-made disasters including—

(1) serving as the principal advisor to the Secretary, the Assistant Secretary, and other Department officials on medical and public health issues;

(2) providing operational medical support to all components of the Department;

(3) as appropriate provide medical liaisons to the components of the Department, on a reimbursable basis, to provide subject matter expertise on operational medical issues;

(4) coordinating with State, local, and tribal governments, the medical community, and others within and outside the Department, including the Department of Health and Human Services Centers for Disease Control, with respect to medical and public health matters; and

(5) performing such other duties relating to such responsibilities as the Secretary may require.

* * * * * * *

TITLE XX—HOMELAND SECURITY GRANTS

SEC. 2001. DEFINITIONS.

In this title, the following definitions shall apply:

(1) * * *

(2) * * *

(3) CORE CAPABILITIES.—The term "core capabilities" means the capabilities for Federal, State, local, and tribal government preparedness for which guidelines are required to be established under section 646(a) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 746(a)).

[(3)**]***(4)* CRITICAL INFRASTRUCTURE SECTORS.—The term "critical infrastructure sectors" means the following sectors, in both urban and rural areas:

* * * * * * *

[(4)**]***(5)* DIRECTLY ELIGIBLE TRIBE.—The term "directly eligible tribe means—

(A) any Indian tribe—

(i) * * *

(ii) * * *

(iii) * * *

(I) * * *

(II) that is located within 10 miles of a system or asset included on the prioritized critical infrastructure list established under **[**section 210E(a)(2)**]** *section 2214(a)(2)* or has such a system or asset within its territory;

(III) * * *

(IV) * * *

(iv) * * *

(B) * * *

[(5)**]***(6)* * * *

[(6)**]***(7)* * * *

[(7)**]***(8)* * * *

[(8)**]***(9)* * * *

[(9)**]***(10)* * * *

[(10)**]***(11)* * * *

[(11)**]***(12)* * * *

[(12)**]***(13)* * * *

[(13) TARGET CAPABILITIES.—The term "target capabilities" means the target capabilities for Federal, State, local, and tribal government preparedness for which guidelines are required to be established under section 646(a) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 746(a)).**]**

(14) TRIBAL GOVERNMENT.—The term "tribal government" means the government of an Indian tribe.

* * * * * * *

SUBTITLE A—GRANTS TO STATE AND HIGH-RISK URBAN AREAS

SEC. 2002. HOMELAND SECURITY GRANT PROGRAMS.

(a) GRANTS AUTHORIZED.—The Secretary, through the Administrator, may award grants under sections **[**2003 and 2004**]** *sections 2003, 2004, and 2010* to State, local, and tribal governments.

(b) * * *

(c) * * *

SEC. 2003. URBAN AREA SECURITY INITIATIVE.

(a) * * *

(b) ASSESSMENT AND DESIGNATION OF HIGH-RISK URBAN AREAS.—

(1) IN GENERAL.—The Administrator shall designate high-risk urban areas to receive grants under this section based on procedures under this subsection.

(2) INITIAL ASSESSMENT.—

(A) IN GENERAL.—For each fiscal year, the Administrator shall conduct an initial assessment *using the most up-to-date data available* of the relative threat, vulnerability, and consequences from acts of terrorism faced by each eligible metropolitan area, including consideration of—

* * * * * * *

(d) DISTRIBUTION OF AWARDS.—

(1) * * *

(2) * * *

(A) * * *

[(B) FUNDS RETAINED.—A State shall provide each relevant high-risk urban area with an accounting of the items, services, or activities on which any funds retained by the State under subparagraph (A) were expended.]

(B) FUNDS RETAINED.—To ensure transparency and avoid duplication, a State shall provide each relevant high-risk urban area with a detailed accounting of the items, services, or activities on which any funds retained by the State under subparagraph (A) are to be expended. Such accounting shall be provided not later than 90 days after the date on which such funds are retained.

(3) * * *

(4) * * *

[(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for grants under this section—

(1) $850,000,000 for fiscal year 2008;

(2) $950,000,000 for fiscal year 2009;

(3) $1,050,000,000 for fiscal year 2010;

(4) $1,150,000,000 for fiscal year 2011;

(5) $1,300,000,000 for fiscal year 2012; and

(6) such sums as are necessary for fiscal year 2013, and each fiscal year thereafter.]

(e) THREAT AND HAZARD IDENTIFICATION RISK ASSESSMENT AND CAPABILITY ASSESSMENT.—As a condition of receiving a grant under this section, each high-risk urban area shall submit to the Administrator a threat and hazard identification and risk assessment and capability assessment—

(1) at such time and in such form as is required by the Administrator; and

(2) consistent with the Federal Emergency Management Agency's Comprehensive Preparedness Guide 201, Second Edition, or such successor document or guidance as is issued by the Administrator.

(f) PERIOD OF PERFORMANCE.—The Administrator shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.

SEC. 2004. STATE HOMELAND SECURITY GRANT PROGRAM.

(a) * * *

* * * * * * *

[(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for grants under this section—

(1) $950,000,000 for each of fiscal years 2008 through 2012; and

(2) such sums as are necessary for fiscal year 2013, and each fiscal year thereafter.]

(f) THREAT AND HAZARD IDENTIFICATION AND RISK ASSESSMENT AND CAPABILITY ASSESSMENT.—

(1) IN GENERAL.—As a condition of receiving a grant under this section, each State shall submit to the Administrator a threat and hazard identification and risk assessment and capability assessment—

(A) at such time and in such form as is required by the Administrator; and

(B) consistent with the Federal Emergency Management Agency's Comprehensive Preparedness Guide 201, Second Edition, or such successor document or guidance as is issued by the Administrator.

(2) COLLABORATION.—In developing the threat and hazard identification and risk assessment under paragraph (1), a State shall solicit input from local and tribal governments, including first responders, and, as appropriate, nongovernmental and private sector stakeholders.

(3) FIRST RESPONDERS DEFINED.—In this subsection, the term "first responders"—

(A) means an emergency response provider; and

(B) includes representatives of local governmental and nongovernmental fire, law enforcement, emergency management, and emergency medical personnel.

(g) PERIOD OF PERFORMANCE.—The Administrator shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 month.

SEC. 2005. GRANTS TO DIRECTLY ELIGIBLE TRIBES.

(a) * * *

* * * * * * *

(h) PERIOD OF PERFORMANCE.—The Secretary shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.

[(h)]*(i)* * * *

[(i)]*(j)* * * *

[(j)]*(k)* STATE OBLIGATIONS.—

(1) IN GENERAL.—States shall be responsible for allocating grant funds received under section 2004 to tribal governments in order to help those tribal communities achieve [target] *core* capabilities not achieved through grants to directly eligible tribes.

(2) * * *

(3) * * *

[(k)]*(l)* * * *

SEC. 2006. TERRORISM PREVENTION.

(a) LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM.—

(1) IN GENERAL.—The Administrator shall ensure that *States and high-risk urban areas expend* not less than 25 percent of the total combined funds appropriated for grants under sections 2003 and 2004 **[**is used**]** for law enforcement terrorism prevention activities.

(2) * * *

(A) * * *

* * * * * * *

[(I) any other activity permitted under the Fiscal Year 2007 Program Guidance of the Department for the Law Enforcement Terrorism Prevention Program; and**]**

(I) activities as determined appropriate by the Administrator, in coordination with the Assistant Secretary for State and Local Law Enforcement within the Office of Partnership and Engagement of the Department, through outreach to relevant stakeholder organizations; and

(J) * * *

(3) * * *

(4) ANNUAL REPORT.—The Administrator, in coordination with the Assistant Secretary for State and Local Law Enforcement, shall report annually from fiscal year 2018 through fiscal year 2022 on the use of grants under sections 2003 and 2004 for law enforcement terrorism prevention activities authorized under this section, including the percentage and dollar amount of funds used for such activities and the types of projects funded.

(b) OFFICE FOR STATE AND LOCAL LAW ENFORCEMENT.—

(1) ESTABLISHMENT.—There is established in the **[**Policy Directorate**]** *Office of Partnership and Engagement* of the Department an Office for State and Local Law Enforcement, which shall be headed by an Assistant Secretary for State and Local Law Enforcement.

(2) * * *

(3) * * *

(4) RESPONSIBILITIES.—The Assistant Secretary for State and Local Law Enforcement shall—

(A) * * *

(B) serve as a liaison between State, local, and tribal law enforcement agencies and the Department, *including through consultation with such agencies regarding Department programs that may impact such agencies*;

(C) * * *

(D) work with the Administrator to **[**ensure**]** *verify* that law enforcement and terrorism-focused grants to State, local, and tribal government agencies, including grants under sections 2003 and 2004, the Commercial Equipment Direct Assistance Program, and other grants administered by the Department to support fusion centers and law enforcement-oriented programs, are appropriately focused on terrorism prevention activities;

(E) coordinate with the Science and Technology Directorate, the Federal Emergency Management Agency, the Department of Justice, the National Institute of Justice,

law enforcement organizations, and other appropriate entities to support the development, promulgation, and updating, as necessary, of national voluntary consensus standards for training and personal protective equipment to be used in a tactical environment by law enforcement officers; [and]

(F) conduct, jointly with the Administrator, a study to determine the efficacy and feasibility of establishing specialized law enforcement deployment teams to assist State, local, and tribal governments in responding to natural disasters, acts of terrorism, or other man-made disasters and report on the results of that study to the appropriate committees of Congress[.]*;*

(G) produce an annual catalog that summarizes opportunities for training, publications, programs, and services available to State, local, tribal, and territorial law enforcement agencies from the Department and from each component and office within the Department and, not later than 30 days after the date of such production, disseminate the catalog, including by—

(i) making such catalog available to State, local, tribal, and territorial law enforcement agencies, including by posting the catalog on the website of the Department and cooperating with national organizations that represent such agencies;

(ii) making such catalog available through the Homeland Security Information Network; and

(iii) submitting such catalog to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(H) in coordination with appropriate components and offices of the Department and other Federal agencies, develop, maintain, and make available information on Federal resources intended to support fusion center access to Federal information and resources.

(5) REPORT.—For each of fiscal years 2019 through 2023, the Assistant Secretary for State and Local Law Enforcement shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the activities of the Office for State and Local Law Enforcement. Each such report shall include, for the fiscal year covered by the report, a description of each of the following:

(A) Efforts to coordinate and share information regarding Department and component agency programs with State, local, and tribal law enforcement agencies.

(B) Efforts to improve information sharing through the Homeland Security Information Network by appropriate component agencies of the Department and by State, local, and tribal law enforcement agencies.

(C) The status of performance metrics within the Office for State and Local Law Enforcement to evaluate the effectiveness of efforts to carry out responsibilities set forth within this subsection.

(D) Any feedback from State, local, and tribal law enforcement agencies about the Office for State and Local Law Enforcement, including the mechanisms utilized to collect such feedback.

(E) Efforts to carry out all other responsibilities of the Office for State and Local Law Enforcement.

[(5)**]** *(6)* RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to diminish, supercede, or replace the responsibilities, authorities, or role of the Administrator.

SEC. 2007. PRIORITIZATION.

(a) IN GENERAL.—In allocating funds among States and high-risk urban areas applying for grants under section 2003 or 2004, the Administrator shall consider, for each State or high-risk urban area—

(1) its relative threat, vulnerability, and consequences from acts of terrorism, including consideration of—

[(A) its population, including appropriate consideration of military, tourist, and commuter populations;**]**

(A) its population, including consideration of domestic and international tourists, commuters, and military populations, including military populations residing in communities outside military installations;

* * * * * * *

(E) the most current threat assessments available to the Department, *including threat information from other relevant Federal agencies and field offices, as appropriate*;

* * * * * * *

(I) the extent to which it has unmet **[**target**]** *core* capabilities;

(J) * * *

(2) the anticipated effectiveness of the proposed use of the grant by the State or high-risk urban area in increasing the ability of that State or high-risk urban area to prevent, prepare for, protect against, and respond to acts of terrorism, to meet its **[**target**]** *core* capabilities, and to otherwise reduce the overall risk to the high-risk urban area, the State, or the Nation.

(b) * * *

SEC. 2008. USE OF FUNDS.

(a) PERMITTED USES.—The Administrator to use grant funds to achieve **[**target**]** *core* capabilities related to preventing, preparing for, protecting against, and responding to acts of terrorism, consistent with a State homeland security plan and relevant local, tribal, and regional homeland security plans, including by working in conjunction with a National Laboratory (as defined in section 2(3) of the Energy Policy Act of 2005 (42 U.S.C. 15801(3))), through—

(1) * * *

(2) * * *

(3) protecting a system or asset included on the prioritized critical infrastructure list established under **[**section 210E(a)(2)**]** *section 2214(a)(2)*;

(4) * * *

(5) ensuring operability and achieving interoperability of emergency communications*, provided such emergency communications align with the Statewide Communication Interoperability Plan and are coordinated with the Statewide Interoperability Coordinator or Statewide interoperability governance body of the State of the recipient*;

(6) enhancing medical preparedness, medical surge capacity, and mass prophylaxis capabilities, including the development and maintenance of an initial pharmaceutical stockpile, including medical kits and diagnostics sufficient to protect first responders (as defined in section 2004(f)), their families, immediate victims, and vulnerable populations from a chemical or biological event;

(7) enhancing cybersecurity, including preparing for and responding to cybersecurity risks and incidents (as such terms are defined in section 2209) and developing statewide cyber threat information analysis and dissemination activities;

[(6)**]***(8)* responding to an increase in the threat level under the **[**Homeland Security Advisory System**]** *National Terrorism Advisory System*, or to the needs resulting from a National Special Security Event;

[(7)**]***(9)* * * *

[(8)**]***(10)* * * *

[(9)**]***(11)* * * *

[(10)**]***(12)* * * *

[(11)**]***(13)* * * *

[(12)**]***(14)* paying expenses directly related to administration of the grant, except that such expenses may not exceed **[**3**]** *5* percent of the amount of the grant; *and*

[(13)**]***(15)* any activity permitted under the Fiscal Year 2007 Program Guidance of the Department for the State Homeland Security Grant Program, the Urban Area Security Initiative (including activities permitted under the full-time counterterrorism staffing pilot), or the Law Enforcement Terrorism Prevention Program**[**; and**]**.

[(14) any other appropriate activity, as determined by the Administrator.**]**

(b) LIMITATIONS ON USE OF FUNDS.—

(1) IN GENERAL.—Funds provided under section 2003 or 2004 may not be used—

(A) to supplant State or local funds, except that nothing in this paragraph shall prohibit the use of grant funds provided to a State or high-risk urban area for otherwise permissible uses under section (a) on the basis that a State or high-risk urban area has previously used State or local funds to support the same or similar uses; **[**or**]**

(B) for any State or local government cost-sharing contribution**[**.**]***; or*

(C) to support any organization or group which has knowingly or recklessly funded domestic terrorism or international terrorism (as those terms are defined in section 2331 of title 18, United States Code) or organization or group known to engage in or recruit to such activities, as determined by the Secretary in consultation with the Administrator, the Under Secretary for Intelligence and Anal-

ysis, and the heads of other appropriate Federal departments and agencies.

(2) * * *

(3) LIMITATIONS ON DISCRETION.—

(A) * * *

(B) ANALYSTS.—If amounts awarded to a grant recipient under section 2003 or 2004 are used for paying salary or benefits of a qualified intelligence analyst under subsection [(a)(10)] *(a)(12)*, the Administrator shall make such amounts available without time limitations placed on the period of time that the analyst can serve under the grant.

(4) CONSTRUCTION.—

(A) IN GENERAL.—A grant awarded under section 2003 or 2004 may not be used to acquire land or to construct buildings or other physical facilities.

(B) EXCEPTIONS.—

(i) IN GENERAL.—Notwithstanding subparagraph (A), nothing in this paragraph shall prohibit the use of a grant awarded under section 2003 or 2004 to achieve [target] *core* capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism, including through the alteration or remodeling of existing buildings for the purpose of making such buildings secure against acts of terrorism.

(ii) * * *

(iii) * * *

(c) MULTIPLE-PURPOSE FUNDS.—Nothing in this subtitle shall be construed to prohibit State, local, or tribal governments from using grant funds under sections 2003 and 2004 in a manner that enhances preparedness for disasters unrelated to acts of terrorism, if such use assists such governments in achieving [target] *core* capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism.

(d) * * *

(e) * * *

(f) EQUIPMENT STANDARDS.—[If an applicant]

(1) APPLICATION REQUIREMENT.—If an applicant for a grant under section 2003 or 2004 proposes to upgrade or purchase, with assistance provided under that grant, new equipment or systems that do not meet or exceed any applicable national voluntary consensus standards developed under section 647 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 747), the applicant shall include in its application an explanation of why such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed such standards.

(2) REVIEW PROCESS.—The Administrator shall implement a uniform process for reviewing applications that, in accordance with paragraph (1), contain explanations for a proposal to use grants provided under section 2003 or 2004 to purchase equipment or systems that do not meet or exceed any applicable national voluntary consensus standards developed under section 647 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 747).

(3) FACTORS.—In carrying out the review process under paragraph (2), the Administrator shall consider the following:

(A) Current or past use of proposed equipment or systems by Federal agencies or the Armed Forces.

(B) The absence of a national voluntary consensus standard for such equipment or systems.

(C) The existence of an international consensus standard for such equipment or systems, and whether such equipment or systems meets such standard.

(D) The nature of the capability gap identified by the applicant, and how such equipment or systems will address such gap.

(E) The degree to which such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed existing consensus standards.

(F) Any other factor determined appropriate by the Administrator.

(g) REVIEW PROCESS.—The Administrator shall implement a uniform process for reviewing applications to use grants provided under section 2003 or 2004 to purchase equipment or systems not included on the Authorized Equipment List maintained by the Administrator.

(h) MAINTENANCE OF EQUIPMENT.—Any applicant for a grant under section 2003 or 2004 seeking to use funds to purchase equipment, including pursuant to paragraphs (3), (4), (5), or (12) of subsection (a) of this section, shall by the time of the receipt of such grant develop a plan for the maintenance of such equipment over its life-cycle that includes information identifying which entity is responsible for such maintenance.

SEC. 2009. OPERATION STONEGARDEN.

(a) ESTABLISHMENT.—There is established in the Department a program to be known as 'Operation Stonegarden'. Under such program, the Secretary, acting through the Administrator, shall make grants to eligible law enforcement agencies, through the State Administrative Agency, to enhance border security in accordance with this section.

(b) ELIGIBLE RECIPIENTS.—To be eligible to receive a grant under this section, a law enforcement agency shall—

(1) be located in—

(A) a State bordering either Canada or Mexico; or

(B) a State or territory with a maritime border; and

(2) be involved in an active, ongoing U.S. Customs and Border Protection operation coordinated through a sector office.

(c) PERMITTED USES.—The recipient of a grant under this section may use such grant for any of the following:

(1) Equipment, including maintenance and sustainment costs.

(2) Personnel costs, including overtime and backfill, directly incurred in support of enhanced border law enforcement activities.

(3) Any activity permitted for Operation Stonegarden under the Department of Homeland Security's Fiscal Year 2016 Homeland Security Grant Program Notice of Funding Opportunity.

(4) Any other appropriate activity, as determined by the Administrator, in consultation with the Commissioner of U.S. Customs and Border Protection.

(d) PERIOD OF PERFORMANCE.—The Secretary shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.

(e) COLLECTION OF INFORMATION.—For any fiscal year beginning on or after the date that is 30 days after the date of enactment of this section for which grants are made under Operation Stonegarden, the Administrator shall separately collect and maintain financial information with respect to grants awarded under Operation Stonegarden, which shall include—

(1) the amount of the awards;

(2) the amount obligated for the awards;

(3) the amount of outlays under the awards;

(4) financial plans with respect to the use of the awards;

(5) any funding transfers or reallocations; and

(6) any adjustments to spending plans or reprogramming.

(f) OVERSIGHT BY THE ADMINISTRATOR.—

(1) IN GENERAL.—The Administrator shall establish and implement guidelines—

(A) to ensure that amounts made available under Operation Stonegarden are used in accordance with grant guidance and Federal laws;

(B) to improve program performance reporting and program performance measurements to facilitate designing, implementing, and enforcing procedures under Operation Stonegarden; and

(C) that require the recording of standardized performance data regarding program output.

(2) SUBMISSION.—Not later than 90 days after the date of enactment of this section, the Administrator shall submit to the Committee on Homeland Security and the Committee on Oversight and Government Reform of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the guidelines established under paragraph (1).

(g) FINANCIAL REVIEW GUIDELINES.—

(1) IN GENERAL.—The Administrator, in coordination with the Commissioner of U.S. Customs and Border Protection, shall develop and implement guidelines establishing procedures for implementing the auditing and reporting requirements under section 2022 with respect to Operation Stonegarden.

(2) SUBMISSION.—Not later than 90 days after the date of enactment of this section, the Administrator shall submit to the Committee on Homeland Security and the Committee on Oversight and Government Reform of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the guidelines established under paragraph (1).

(h) REPORT AND BRIEFING.—The Administrator, in coordination with the Commissioner of U.S. Customs and Border Protection, shall, at least annually during each of fiscal years 2018 through 2022, submit to the Committee on Homeland Security and the Committee on Oversight and Government Reform of the House of Rep-

resentatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report and briefing including—

(1) for the period covered by the report—

(A) information on how each recipient of a grant under Operation Stonegarden expended amounts received under the grant;

(B) a list of all operations carried out using amounts made available under Operation Stonegarden; and

(C) for each operation described in subparagraph (B)—

(i) whether the operation is active or completed;

(ii) the targeted purpose of the operation;

(iii) the location of the operation; and

(iv) the total number of hours worked by employees of the grant recipient and by employees of U.S. Customs and Border Protection with respect to the operation, including the number of hours for which such employees received basic pay and the number of hours for which such employees received premium pay, by type of premium pay; and

(2) in the first report submitted under this subsection—

(A) an examination of the effects changing the Operation Stonegarden Program to award multi-year grants would have on the mission of the program; and

(B) the findings and recommendations of the Administrator regarding what changes could improve the program to better serve the program mission, which may include feedback from grant recipients.

SEC. 2010. NON–PROFIT SECURITY GRANT PROGRAM.

(a) ESTABLISHMENT.—There is established in the Department a program to be known as the 'Non-Profit Security Grant Program' (in this section referred to as the "Program"). Under the Program, the Secretary, acting through the Administrator, shall make grants to eligible nonprofit organizations described in subsection (b), through the State in which such organizations are located, for target hardening and other security enhancements to protect against terrorist attacks.

(b) ELIGIBLE RECIPIENTS.—Eligible nonprofit organizations described in this subsection (a) are organizations that are—

(1) described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such Code; and

(2) determined to be at risk of a terrorist attack by the Administrator.

(c) PERMITTED USES.—The recipient of a grant under this section may use such grant for any of the following:

(1) described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such Code; and

(2) determined to be at risk of a terrorist attack by the Administrator.

(d) ALLOCATION.—The Administrator shall ensure that not less than an amount equal to 30 percent of the total funds appropriated for grants under the Program for each fiscal year is used for grants to eligible nonprofit organizations described in subsection (b) that

are located in jurisdictions not receiving funding under section 2003.

(e) PERIOD OF PERFORMANCE.—The Administrator shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.

* * * * * * *

SUBTITLE B—GRANT ADMINISTRATION

SEC. 2021. ADMINISTRATION AND COORDINATION.

(a) * * *

(b) * * *

[(c) INTERAGENCY COORDINATION.—

[(1) IN GENERAL.—Not later than 12 months after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the Secretary (acting through the Administrator), the Attorney General, the Secretary of Health and Human Services, and the heads of other agencies providing assistance to State, local, and tribal governments for preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other man-made disasters, shall jointly—

[(A) compile a comprehensive list of Federal grant programs for State, local, and tribal governments for preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other manmade disasters;

[(B) compile the planning, reporting, application, and other requirements and guidance for the grant programs described in subparagraph (A);

[(C) develop recommendations, as appropriate, to—(i) eliminate redundant and duplicative requirements for State, local, and tribal governments, including onerous application and ongoing reporting requirements; (ii) ensure accountability of the programs to the intended purposes of such programs; (iii) coordinate allocation of grant funds to avoid duplicative or inconsistent purchases by the recipients; (iv) make the programs more accessible and user friendly to applicants; and (v) ensure the programs are coordinated to enhance the overall preparedness of the Nation;

[(D) submit the information and recommendations under subparagraphs (A), (B), and (C) to the appropriate committees of Congress; and

[(E) provide the appropriate committees of Congress, the Comptroller General, and any officer or employee of the Government Accountability Office with full access to any information collected or reviewed in preparing the submission under subparagraph (D).

[(2) SCOPE OF TASK.—Nothing in this subsection shall authorize the elimination, or the alteration of the purposes, as delineated by statute, regulation, or guidance, of any grant program that exists on the date of the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, nor authorize the review or preparation of proposals on the

elimination, or the alteration of such purposes, of any such grant program.]

[(d)](c) * * *

(1) * * *

(2) * * *

(3) with respect to terrorism-focused grants, it is necessary to ensure both that the [target] *core* capabilities of the highest risk areas are achieved quickly and that basic levels of preparedness, as measured by the attainment of [target] *core* capabilities, are achieved nationwide.

* * * * * * *

SEC. 2022. ACCOUNTABILITY.

(a) AUDITS OF GRANT PROGRAMS.—

(1) COMPLIANCE REQUIREMENTS.—

(A) * * *

(B) ACCESS TO INFORMATION.—[The Department]

(i) IN GENERAL.—The Department and each recipient of a grant administered by the Department shall provide the Comptroller General and any officer or employee of the Government Accountability Office with full access to information regarding the activities carried out related to any grant administered by the Department.

(ii) INSPECTOR GENERAL REVIEW.—With respect to each grant awarded, the Inspector General of the Department may—

(I) examine any records of the contractor or grantee, any of its subcontractors or subgrantees, or any State or local agency or other entity in receipt of or administering any grant awarded, that pertain to, and involve transactions relating to the contract, subcontract, grant, or subgrant; and

(II) interview any officer or employee of the contractor or grantee, any of its subcontractors or subgrantees, or any State or local agency or other entity in receipt of or administering any grant awarded, regarding transactions relating to the contract, subcontract, grant, or subgrant.

(iii) RULE OF CONSTRUCTION.—Nothing in clause (ii) may be construed to limit or restrict the authority of the Inspector General of the Department.

* * * * * * *

(b) REPORTS BY GRANT RECIPIENTS.—

(1) QUARTERLY REPORTS ON HOMELAND SECURITY SPENDING.—

(A) IN GENERAL.—As a condition of receiving [a grant under section 2003 or 2004] *a covered grant, any recipient, including,* a State, high-risk urban area, or directly eligible tribe, shall, not later than 30 days after the end of each Federal fiscal quarter, submit to the Administrator *or the Secretary, as appropriate under the covered grant,* a report on activities performed using grant funds during that fiscal quarter.

(B) CONTENTS.—Each report submitted under subparagraph (A) shall at a minimum include, for the applicable *recipient, including any* State, high-risk urban area, or directly eligible tribe, and each subgrantee thereof—

(i) the amount obligated to that recipient under [section 2003 or 2004] *the covered grant* in that quarter;

(ii) the amount of funds received and expended under [section 2003 or 2004] *the covered grant* by that recipient in that quarter; [and]

(iii) a [summary] *detailed* description of expenditures made by that recipient using [such funds, and the purposes for which such expenditures were made.] *such funds, including—*

(I) the name of the recipient and the project or activity;

(II) a detailed description of the project or activity;

(III) an evaluation of the completion status of the project or activity;

(IV) in the case of an infrastructure investment—

(aa) the purpose, total expected cost, and rationale for funding the infrastructure investment with funds made available; and

(bb) the name of the point of contact for the recipient if there are questions concerning the infrastructure investment; and

(V) detailed information from each subgrantee, including the information described in subparagraphs (I) through (IV), on any subgrant awarded by the recipient; and

(iv) the total amount of funds received to date under each covered grant.

(C) END-OF-YEAR REPORT.—The report submitted under subparagraph (A) by *any recipient, including any* a State, high-risk urban area, or directly eligible tribe, relating to the last quarter of any fiscal year shall include, *in addition to the contents required under subparagraph (B)—*

(i) the amount and date of receipt of all funds received under the grant during that fiscal year

(ii) the identity of, and *total* amount provided to, any subgrantee for that grant during that fiscal year; *and*

(iii) the amount and the dates of disbursements of all such funds expended in compliance with section 2021(a)(1) or under mutual aid agreements or other sharing arrangements that [apply within] *apply to or within any recipient, including* the State, high-risk urban area, or directly eligible tribe, as applicable, during that fiscal year[; and].

[(iv) how the funds were used by each recipient or subgrantee during that fiscal year.]

(2) * * *

(3) REQUIRED REPORTING FOR PRIOR AWARDED GRANTS.—Not later than 180 days after the end of the quarter following the date of enactment of this paragraph, each recipient of a covered

grant awarded before the date of enactment of this paragraph shall provide the information required under this subsection and thereafter comply with the requirements of this subsection.

(4) ASSISTANCE IN REPORTING.—The Administrator or the Secretary, as appropriate under the covered grant, in coordination with the Director of the Office of Management and Budget, shall provide for user-friendly means for grant recipients to comply with the reporting requirements of this subsection.

(5) SUBGRANTEE REPORTING.—Each grant recipient required to report information under paragraph (1)(B)(iii)(V) shall register with the System for Award Management database or complete other registration requirements as determined necessary by the Director of the Office of Management and Budget.

(6) PUBLICATION OF INFORMATION.—Not later than 7 days after the date on which the Administrator or the Secretary, as the case may be, receives the reports required to be submitted under this subsection, the Administrator and the Secretary shall make the information in the reports publicly available, in a searchable database, on the website of the Federal Emergency Management Agency or Department, as appropriate.

(7) COVERED GRANT DEFINED.—In this subsection, the term "covered grant" means a grant awarded under—

(A) this Act; or

(B) a program described in paragraphs (1) through (6) of section 2002(b) that is administered by the Department.

(c) * * *

(d) SUNSET AND DISPOSITION OF UNEXPENDED GRANT AMOUNTS.—

(1) IN GENERAL.—Except as may be otherwise provided in the authorizing statute of a grant program, effective on the date that is 5 years after the date on which grant funds are distributed by the Administrator or the Secretary, as appropriate, under a covered grant (as defined in subsection (b)(7)), the authority of a covered grant recipient, including any grantee or subgrantee, to obligate, provide, make available, or otherwise expend those funds is terminated.

(2) RETURN OF UNEXPENDED GRANT AMOUNTS.—Upon the termination of authority under paragraph (1), any grant amounts that have not been expended shall be returned to the Administrator or the Secretary, as the case may be. The Administrator or the Secretary, as the case may be, shall deposit any grant amounts returned under this paragraph in the General Fund of the Treasury in accordance with section 3302 of title 31, United States Code.

(3) AWARDS TO RECIPIENTS RETURNING GRANT FUNDS.—On and after the date on which the authority of a covered grant recipient is terminated under paragraph (1) with respect to a grant under a covered grant program, the Administrator or the Secretary, as appropriate, may award a grant under the covered grant program to the covered grant recipient, only pursuant to the submission of a new grant application, in accordance with the requirements of the grant program.

(4) APPLICABILITY.—This subsection shall apply to any grant awarded under a covered grant program on or after the date of enactment of this subsection.

* * * * * * *

SEC. 2024. MEMORANDA OF UNDERSTANDING WITH DEPARTMENTAL COMPONENTS AND OFFICES REGARDING THE POLICY AND GUIDANCE.

The Administrator shall enter into memoranda of understanding with the heads of the following departmental components and offices delineating the roles and responsibilities of such components and offices regarding the policy and guidance for grants under section 1406 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1135), sections 2003 and 2004 of this Act, and section 70107 of title 46, United States Code, as appropriate:

(1) The Commissioner of U.S. Customs and Border Protection.

(2) The Administrator of the Transportation Security Administration.

(3) The Commandant of the Coast Guard.

(4) The Under Secretary for Intelligence and Analysis.

(5) The Assistant [Director for Emergency Communications].

(6) The Assistant Secretary for State and Local Law Enforcement.

(7) The Countering Violent Extremism Coordinator.

(8) The Officer for Civil Rights and Civil Liberties.

(9) The Chief Medical Officer.

(10) The heads of other components or offices of the Department, as determined by the Secretary.

TITLE XXI—CHEMICAL FACILITY ANTI-TERRORISM STANDARDS

* * * * * * *

SEC. 2102. CHEMICAL FACILITY ANTI-TERRORISM STANDARDS PROGRAM.

(a) PROGRAM ESTABLISHED.—There is in the Department a Chemical Facility Anti-Terrorism Standards Program.

(1) IN GENERAL.—There is in the Department a Chemical Facility Anti-Terrorism Standards Program, *which shall be located in the Cybersecurity and Infrastructure Security Agency.*

* * * * * * *

SEC. 2103. PROTECTION AND SHARING OF INFORMATION.

(a) * * *

(b) * * *

(c) SHARING OF INFORMATION WITH FIRST RESPONDERS.—

(1) REQUIREMENT.—The Secretary shall provide to State, local, and regional fusion centers (as that term is defined in section ⟦210A(j)(1)⟧ *210A(j)*) and State and local government officials, as the Secretary determines appropriate, such information as is necessary to help ensure that first responders are properly prepared and provided with the situational awareness

needed to respond to security incidents at covered chemical facilities.

SEC. 2104. CIVIL ENFORCEMENT.

(a) * * *

(b) * * *

(c) EMERGENCY OPERATIONS.—

(1) * * *

(2) LIMITATION ON DELEGATION.—The Secretary may not delegate the authority under paragraph (1) to any official other than the [Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department appointed under section 103(a)(1)(H)] *Director of Cybersecurity and Infrastructure Security.*

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle A—Cybersecurity and Infrastructure Security

SEC. 2201. DEFINITIONS.

In this subtitle:

(1) CRITICAL INFRASTRUCTURE INFORMATION.—The term "critical infrastructure information" has the meaning given the term in section 2222.

(2) CYBERSECURITY RISK.—The term "cybersecurity risk" has the meaning given the term in section 2209.

(3) CYBERSECURITY THREAT.—The term "cybersecurity threat" has the meaning given the term in section 102(5) of the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

(4) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term "national cybersecurity asset response activities" means—

(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

(D) facilitating information sharing and operational coordination with threat response; and

(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

(5) SECTOR-SPECIFIC AGENCY.—The term "Sector-Specific Agency" means a Federal department or agency, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

(6) SHARING.—The term "sharing" has the meaning given the term in section 2209.

SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) REDESIGNATION.—

(1) IN GENERAL.—The National Protection and Programs Directorate of the Department shall, on and after the date of the enactment of this subtitle, be known as the "Cybersecurity and Infrastructure Security Agency" (in this subtitle referred to as the "Agency").

(2) REFERENCES.—Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department.

(b) DIRECTOR.—

(1) IN GENERAL.—The Agency shall be headed by a Director of Cybersecurity and Infrastructure Security (in this subtitle referred to as the "Director"), who shall report to the Secretary.

(2) REFERENCE.—Any reference to an Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and any other related program of the Department as described in section 103(a)(1)(H) as in effect on the day before the date of enactment of this subtitle in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Director of Cybersecurity and Infrastructure Security of the Department.

(c) RESPONSIBILITIES.—The Director shall—

(1) lead cybersecurity and critical infrastructure security programs, operations, and associated policy for the Agency, including national cybersecurity asset response activities;

(2) coordinate with Federal entities, including Sector-Specific Agencies, and non-Federal entities, including international entities, to carry out the cybersecurity and critical infrastructure activities of the Agency, as appropriate;

(3) carry out the responsibilities of the Secretary to secure Federal information and information systems consistent with law, including subchapter II of chapter 35 of title 44, United States Code, and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113));

(4) coordinate a national effort to secure and protect against critical infrastructure risks, consistent with subsection (e)(1)(E);

(5) oversee the EMP and GMD planning and protection and preparedness activities of the Agency;

(6) upon request, provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators

and, where appropriate, provide those analyses, expertise, and other technical assistance in coordination with Sector-Specific Agencies and other Federal departments and agencies;

(7) develop and utilize mechanisms for active and frequent collaboration between the Agency and Sector-Specific Agencies to ensure appropriate coordination, situational awareness, and communications with Sector-Specific Agencies;

(8) maintain and utilize mechanisms for the regular and ongoing consultation and collaboration among the Divisions of the Agency to further operational coordination, integrated situational awareness, and improved integration across the Agency in accordance with this Act;

(9) develop, coordinate, and implement—

(A) comprehensive strategic plans for the activities of the Agency; and

(B) risk assessments by and for the Agency;

(10) carry out emergency communications responsibilities, in accordance with title XVIII;

(11) carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate that outreach and engagement with critical infrastructure Sector-Specific Agencies, as appropriate;

(12) oversee an integrated analytical approach to physical and cyber infrastructure analysis; and

(13) carry out such other duties and powers prescribed by law or delegated by the Secretary.

(d) DEPUTY DIRECTOR.—There shall be in the Agency a Deputy Director of Cybersecurity and Infrastructure Security who shall—

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

(2) report to the Director.

(e) CYBERSECURITY AND INFRASTRUCTURE SECURITY AUTHORITIES OF THE SECRETARY.—

(1) IN GENERAL.—The responsibilities of the Secretary relating to cybersecurity and infrastructure security shall include the following:

(A) To access, receive, and analyze law enforcement information, intelligence information, and other information from Federal Government agencies, State, local, tribal, and territorial government agencies, including law enforcement agencies, and private sector entities, and to integrate that information, in support of the mission responsibilities of the Department, in order to—

(i) identify and assess the nature and scope of terrorist threats to the homeland;

(ii) detect and identify threats of terrorism against the United States; and

(iii) understand those threats in light of actual and potential vulnerabilities of the homeland.

(B) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States, including an assessment of the probability of success of those attacks and the feasibility and potential efficacy of various

countermeasures to those attacks. At the discretion of the Secretary, such assessments may be carried out in coordination with Sector-Specific Agencies.

(C) To integrate relevant information, analysis, and vulnerability assessments, regardless of whether the information, analysis, or assessments are provided or produced by the Department, in order to make recommendations, including prioritization, for protective and support measures by the Department, other Federal Government agencies, State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities regarding terrorist and other threats to homeland security.

(D) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this title, including obtaining that information from other Federal Government agencies.

(E) To develop, in coordination with the Sector-Specific Agencies with available expertise, a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency communications systems, and the physical and technological assets that support those systems.

(F) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government agencies, including Sector-Specific Agencies, and in cooperation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities.

(G) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information relating to homeland security within the Federal Government and between Federal Government agencies and State, local, tribal, and territorial government agencies and authorities.

(H) To disseminate, as appropriate, information analyzed by the Department within the Department, to other Federal Government agencies with responsibilities relating to homeland security, and to State, local, tribal, and territorial government agencies and private sector entities with those responsibilities in order to assist in the deterrence, prevention, or preemption of, or response to, terrorist attacks against the United States.

(I) To consult with State, local, tribal, and territorial government agencies and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(J) To ensure that any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties.

(K) To request additional information from other Federal Government agencies, State, local, tribal, and territorial government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain that information.

(L) To establish and utilize, in conjunction with the Chief Information Officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(M) To coordinate training and other support to the elements and personnel of the Department, other Federal Government agencies, and State, local, tribal, and territorial government agencies that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

(N) To coordinate with Federal, State, local, tribal, and territorial law enforcement agencies, and the private sector, as appropriate.

(O) To exercise the authorities and oversight of the functions, personnel, assets, and liabilities of those components transferred to the Department pursuant to section 201(g).

(P) To carry out the functions of the national cybersecurity and communications integration center under section 2209.

(Q) To carry out the requirements of the Chemical Facility Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate program established under subtitle J of title VIII, or any successor programs.

(2) REALLOCATION.—The Secretary may reallocate within the Agency the functions specified in sections 2203(b) and 2204(b), consistent with the responsibilities provided in paragraph (1), upon certifying to and briefing the appropriate congressional committees, and making available to the public, not less than 60 days before the reallocation that the reallocation is necessary for carrying out the activities of the Agency.

(3) STAFF.—

(A) IN GENERAL.—The Secretary shall provide the Agency with a staff of analysts having appropriate expertise and experience to assist the Agency in discharging the responsibilities of the Agency under this section.

(B) PRIVATE SECTOR ANALYSTS.—Analysts under this subsection may include analysts from the private sector.

(C) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(4) DETAIL OF PERSONNEL.—

(A) IN GENERAL.—In order to assist the Agency in discharging the responsibilities of the Agency under this section, personnel of the Federal agencies described in subparagraph (B) may be detailed to the Agency for the performance of analytic functions and related duties.

(B) AGENCIES.—The Federal agencies described in this subparagraph are—

(i) the Department of State;

(ii) the Central Intelligence Agency;

(iii) the Federal Bureau of Investigation;

(iv) the National Security Agency;

(v) the National Geospatial-Intelligence Agency;

(vi) the Defense Intelligence Agency;

(vii) Sector-Specific Agencies; and

(viii) any other agency of the Federal Government that the President considers appropriate.

(C) INTERAGENCY AGREEMENTS.—The Secretary and the head of a Federal agency described in subparagraph (B) may enter into agreements for the purpose of detailing personnel under this paragraph.

(D) BASIS.—The detail of personnel under this paragraph may be on a reimbursable or non-reimbursable basis.

(f) COMPOSITION.—The Agency shall be composed of the following divisions:

(1) The Cybersecurity Division, headed by an Assistant Director.

(2) The Infrastructure Security Division, headed by an Assistant Director.

(3) The Emergency Communications Division under title XVIII, headed by an Assistant Director.

(g) CO-LOCATION.—

(1) IN GENERAL.—To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence.

(2) COORDINATION.—When establishing the central locations described in paragraph (1), the Director shall coordinate with component heads and the Under Secretary for Management to co-locate or partner on any new real property leases, renewing any occupancy agreements for existing leases, or agreeing to extend or newly occupy any Federal space or new construction.

(h) PRIVACY.—

(1) IN GENERAL.—There shall be a Privacy Officer of the Agency with primary responsibility for privacy policy and compliance for the Agency.

(2) RESPONSIBILITIES.—The responsibilities of the Privacy Officer of the Agency shall include—

(A) ensuring that the use of technologies by the Agency sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(B) ensuring that personal information contained in systems of records of the Agency is handled in full compliance as specified in section 552a of title 5, United States Code (commonly known as the "Privacy Act of 1974");

(C) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Agency; and

(D) conducting a privacy impact assessment of proposed rules of the Agency on the privacy of personal information, including the type of personal information collected and the number of people affected.

(i) SAVINGS.—Nothing in this title may be construed as affecting in any manner the authority, existing on the day before the date of enactment of this title, of any other component of the Department or any other Federal department or agency.

SEC. 2203. CYBERSECURITY DIVISION.

(a) ESTABLISHMENT.—

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

(2) ASSISTANT DIRECTOR.—The Cybersecurity Division shall be headed by an Assistant Director for Cybersecurity (in this section referred to as the "Assistant Director"), who shall—

(A) be at the level of Assistant Secretary within the Department;

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

(C) report to the Director.

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

(b) FUNCTIONS.—The Assistant Director shall—

(1) direct the cybersecurity efforts of the Agency;

(2) carry out activities, at the direction of the Director, related to the security of Federal information and Federal information systems consistent with law, including subchapter II of chapter 35 of title 44, United States Code, and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113));

(3) fully participate in the mechanisms required under section 2202(c)(7); and

(4) carry out such other duties and powers as prescribed by the Director.

SEC. 2204. INFRASTRUCTURE SECURITY DIVISION.

(a) ESTABLISHMENT.—

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

(2) ASSISTANT DIRECTOR.—The Infrastructure Security Division shall be headed by an Assistant Director for Infrastructure Security (in this section referred to as the "Assistant Director"), who shall—

(A) be at the level of Assistant Secretary within the Department;

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

(C) report to the Director.

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

(b) FUNCTIONS.—The Assistant Director shall—

(1) direct the critical infrastructure security efforts of the Agency;

(2) carry out, at the direction of the Director, the Chemical Facilities Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate program established under subtitle J of title VIII, or any successor programs;

(3) fully participate in the mechanisms required under section 2202(c)(7); and

(4) carry out such other duties and powers as prescribed by the Director.

[SEC. 223]*SEC. 2205.* ENHANCEMENT OF FEDERAL AND NON-FEDERAL CYBERSECURITY.

In carrying out the responsibilities under [section 201] *section 2022*, the [Under Secretary appointed under section 103(a)(1)(H)] *Director of Cybersecurity and Infrastructure Security shall—*

(1) * * *

(A) * * *

(B) in coordination with the Under Secretary for Emergency Preparedness and Response, crisis management support in response to threats to, or attacks on, critical information systems; [and]

(2) * * *

(3) * * *

[SEC. 224]*SEC. 2206.* NET GUARD.

The [Assistant Secretary for Infrastructure Protection] *Director of Cybersecurity and Infrastructure Security* may establish a national technology guard, to be known as "NET Guard", comprised of local teams of volunteers with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks.

[SEC. 225]*SEC. 2207.* CYBER SECURITY ENHANCEMENT ACT OF 2002.

* * * * * * *

[SEC. 226]*SEC. 2208.* CYBERSECURITY RECRUITMENT AND RETENTION.

* * * * * * *

[SEC. 227]*SEC. 2209.* NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITIONS.—In this section.—

(1) * * *

(2) * * *

(3) * * *

(4) the term "information sharing and analysis organization" has the meaning given that term in [section 212(5)] *section 2222(5)*;

(5) * * *

(6) * * *

(b) CENTER.—There is in the Department a national cybersecurity and communications integration center (referred to in this section as the "Center") to carry out certain responsibilities of the [Under Secretary appointed under section 103(a)(1)(H)] *Director. The Center shall be located in the Cybersecurity and Infrastructure Security Agency. The head of the Center shall report to the Assistant Director for Cybersecurity.*

(c) FUNCTIONS.—The cybersecurity functions of the Center shall include—

(1) * * *

* * * * * * *

(5) * * *

(A) * * *

(B) sharing the analysis conducted under subparagraph (A) with Federal and non-Federal entities*, including the National Network of Fusion Centers (as defined in section 210A), as appropriate;*

(6) * * *

(7) providing [information and recommendations] *information, recommendations, and best practices* on security and resilience measures to Federal and non-Federal entities, including [information and recommendations] *information, recommendations, and best practices* to—

* * * * * * *

(9) sharing cyber threat indicators, defensive measures *best practices*, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;

(10) * * *

(11) in coordination with the [Office of Emergency Communications] *Emergency Communications Division* of the Department, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications.

(d) COMPOSITION.—

(1) IN GENERAL.—The Center shall be composed of—

(A) * * *

(B) appropriate representatives of non-Federal entities, such as—

(i) State, local, and tribal governments;

(ii) information sharing and analysis organizations, including information sharing and analysis centers *and State, local, and regional fusion centers (as defined in section 201A), as appropriate*;

(iii) owners and operators of critical information systems; and

(iv) private entities;

* * * * * * *

(f) NO RIGHT OR BENEFIT.—

(1) IN GENERAL.—The provision of assistance or information to, and inclusion in the Center of, governmental or private entities under this section shall be at the sole and unreviewable discretion of the [Under Secretary appointed under section 103(a)(1)(H)] *Director*.

(2) * * *

(g) AUTOMATED INFORMATION SHARING.—

(1) IN GENERAL.—The [Under Secretary appointed under section 103(a)(1)(H)] *Director*, in coordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the sharing of cyber threat indicators and defensive measures in accordance with title I of the Cybersecurity Act of 2015.

(2) ANNUAL REPORT.—The [Under Secretary appointed under section 103(a)(1)(H)] *Director* shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives an annual report on the status and progress of the development of the capabilities described in paragraph (1). Such reports shall be required until such capabilities are fully implemented.

(h) VOLUNTARY INFORMATION SHARING PROCEDURES.—

(1) PROCEDURES.—

(A) IN GENERAL.—The Center may enter into a voluntary information sharing relationship with any consenting non-Federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes in accordance with this section. Nothing in this subsection may be construed to require any non-Federal entity to enter into any such information sharing relationship with the Center or any other entity. The Center may terminate a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the [Under Secretary appointed under section 103(a)(1)(H)] *Director*, for any reason, including if the Center determines that the non-Federal entity with which the Center has entered into such a relationship has violated the terms of this subsection.

(B) NATIONAL SECURITY.—The Secretary may decline to enter into a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the [Under Secretary appointed under section 103(a)(1)(H)] *Director*, for any reason, including if the Secretary determines that such is appropriate for national security.

(2) * * *

(A) * * *

(B) NEGOTIATED AGREEMENT.—At the request of a non-Federal entity, and if determined appropriate by the Center, at the sole and unreviewable discretion of the Secretary, acting through the [Under Secretary appointed under section 103(a)(1)(H)] *Director*, the Department shall

negotiate a non-standard agreement, consistent with this section.

(C) * * *

(i) * * *

(j) * * *

(k) OUTREACH.—Not later than 60 days after the date of enactment of this subsection, the Secretary, acting through the [Under Secretary appointed under section 103(a)(1)(H)] *Director*, shall—

* * * * * * *

[SEC. 228]*SEC. 2210*. CYBERSECURITY PLANS.

(a) DEFINITIONS.—In this section—

(1) * * *

(2) the terms "cybersecurity risk" and "information system" have the meanings given those terms in [section 227] *section 2209*;

* * * * * * *

(c) CYBER INCIDENT RESPONSE PLAN.—The [Under Secretary appointed under section 103(a)(1)(H)] *Director of Cybersecurity and Infrastructure Security* shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in [section 212(5)] *section 2222(5)*), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in [section 227] *section 2209*) to critical infrastructure.

(d) * * *

[SEC. 228A.]*SEC. 2211*. CYBERSECURITY STRATEGY.

(a) * * *

(b) CONTENTS.—The strategy required under subsection (a) shall include the following:

(1) * * *

(2) * * *

(A) Cybersecurity functions set forth in [the section 227] *section 2209* (relating to the national cybersecurity and communications integration center).

(B) * * *

(C) * * *

(D) * * *

(c) CONSIDERATIONS.—In developing the strategy required under subsection (a), the Secretary shall—

(1) CONSIDER—

(A) * * *

(B) * * *

(C) the most recent Quadrennial Homeland Security Review issued pursuant to [section 707] *section 706*; and

* * * * * * *

[SEC. 229.]*SEC. 2212*. CLEARANCES.

The Secretary shall make available the process of application for security clearances under Executive Order 13549 (75 Fed. Reg. 162; relating to a classified national security information program) or

any successor Executive Order to appropriate representatives of sector coordinating councils, sector information sharing and analysis organizations (as defined in [section 212(5)] *section 2222(5)*), owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.

[SEC. 230.]*SEC. 2213.* FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.

(a) DEFINITIONS.—In this section—

(1) * * *

(2) * * *

(3) the term "agency information system" has the meaning given the term in [section 228] *section 2210*; and

(4) the terms "cybersecurity risk" and "information system" have the meanings given those terms in [section 227] *section 2209*.

* * * * * * *

[SEC. 210E.] *SEC. 2214.* NATIONAL ASSET DATABASE.

(a) * * *

* * * * * * *

[(e) INSPECTOR GENERAL STUDY.—By not later than two years after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the Inspector General of the Department shall conduct a study of the implementation of this section.]

[(f)]*(e)* * * *

* * * * * * *

Subtitle B—Critical Infrastructure Information

* * * * * * *

[SEC. 211.]*SEC. 2221.* SHORT TITLE.

* * * * * * *

[SEC. 212.] *SEC. 2222.* DEFINITIONS.

In this subtitle:

(1) * * *

* * * * * * *

(8) CYBERSECURITY RISK; INCIDENT.—The terms "cybersecurity risk" and "incident" have the meanings given those terms in [section 227] *section 2209*.

[SEC. 213.] *SEC. 2223.* DESIGNATION OF CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.

* * * * * * *

[SEC. 214.] *SEC. 2224.* PROTECTION OF VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.

(a) * * *

* * * * * * *

(h) AUTHORITY TO DELEGATE.—The President may delegate authority to a critical infrastructure protection program, designated under [section 213] *section 2223*, to enter into a voluntary agree-

ment to promote critical infrastructure security, including with any Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 708 of the Defense Production Act of 1950 (50 U.S.C. App. 2158).

[SEC. 215.] *SEC. 2225.* NO PRIVATE RIGHT OF ACTION.

* * * * * * *

CONSOLIDATED APPROPRIATIONS ACT OF 2016

* * * * * * *

DIVISION N—CYBERSECURITY ACT OF 2015

* * * * * * *

TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT

* * * * * * *

Subtitle A—National Cybersecurity and Communications Integration Center

* * * * * * *

SEC. 202. DEFINITIONS.

In this subtitle:

(1) * * *

(2) CYBERSECURITY RISK; INCIDENT.—The terms "cybersecurity risk" and "incident" have the meanings given those terms in section [227] 2209 of the Homeland Security Act of 2002 (6 U.S.C. 148)**[**, as so redesignated by section 223(a)(3) of this division**]**.

* * * * * * *

SEC. 207. ASSESSMENT.

Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the appropriate congressional committees a report that includes—

(1) * * *

(2) to the extent practicable, findings regarding increases in the sharing of cyber threat indicators, defensive measures, and information relating to cybersecurity risks and incidents at the center established under **[**section 227**]** of the Homeland Security Act of 2002**[**, as redesignated by section 223(a) of this division,**]** and throughout the United States.

SEC. 208. MULTIPLE SIMULTANEOUS CYBER INCIDENTS AT CRITICAL INFRASTRUCTURE.

Not later than 1 year after the date of enactment of this Act, the **[**Under Secretary appointed under section 103(a)(1)(H) of the

Homeland Security Act of 2002 (6 U.S.C. 113(a)(1)(H))] *Director of Cybersecurity and Infrastructure Security of the Department* shall provide information to the appropriate congressional committees on the feasibility of producing a risk-informed plan to address the risk of multiple simultaneous cyber incidents affecting critical infrastructure, including cyber incidents that may have a cascading effect on other critical infrastructure.

* * * * * * *

Subtitle B—Federal Cybersecurity Enhancement

* * * * * * *

SEC. 222. DEFINITIONS.

In this subtitle:

(1) * * *

(2) AGENCY INFORMATION SYSTEM.—The term "agency information system" has the meaning given the term in [section 228] *section 2210* of the Homeland Security Act of 2002[, as added by section 223(a)(4) of this division].

(3) * * *

(4) CYBERSECURITY RISK; INFORMATION SYSTEM.—The terms "cybersecurity risk" and "information system" have the meanings given those terms in [section 227]*section 2209* of the Homeland Security Act of 2002[, as so redesignated by section 223(a)(3) of this division].

* * * * * * *

SEC. 223. IMPROVED FEDERAL NETWORK SECURITY.

(a) * * *

(b) AGENCY RESPONSIBILITIES.—

(1) IN GENERAL.—Except as provided in paragraph (2)—

(A) not later than 1 year after the date of enactment of this Act or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under [section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a)]*section 2213(b)(1) of the Homeland Security Act of 2002*, whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to [section 230(b)(2) of the Homeland Security Act of 2002 (6 U.S.C. 151(b)(2)), as added by subsection (a)] *section 2213(b)(2) of the Homeland Security Act of 2002*, the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

(2) * * *

(3) * * *

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit an agency from applying the intrusion detection and prevention capabilities to an information

system other than an agency information system under [section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a)]*section 2213(b)(1) of the Homeland Security Act of 2002*, at the discretion of the head of the agency or as provided in relevant policies, directives, and guidelines.

* * * * * * *

SEC. 226. ASSESSMENT; REPORTS.

(a) DEFINITIONS.—In this section:

(1) AGENCY INFORMATION.—The term "agency information has the meaning given the term in [section 230] *section 2213* of the Homeland Security Act of 2002[, as added by section 223(a)(6) of this division].

(2) * * *

(3) * * *

(4) INTRUSION ASSESSMENT PLAN.—The term "intrusion detection and prevention capabilities means the plan required under [section 228(b)(1)] *section 2210(b)(1)* of the Homeland Security Act of 2002[, as added by section 223(a)(4) of this division].

(5) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—The term "intrusion detection and prevention capabilities' means the capabilities required under [section 230(b)] section *2213(b)* of the Homeland Security Act of 2002[, as added by section 223(a)(6) of this division].

(b) * * *

(c) REPORTS TO CONGRESS.—

(1) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—

(A) Secretary of Homeland Security report. Not later than 6 months after December 18, 2015, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

* * * * * * *

(vi) a description of the pilot established under [section 230(c)(5)] *section 2213(c)(5)* of the Homeland Security Act of 2002[, as added by section 223(a)(6) of this division], including the number of new technologies tested and the number of participating agencies.

* * * * * * *

SEC. 227. TERMINATION.

(a) IN GENERAL.—The authority provided under [section 230] *section 2213* of the Homeland Security Act of 2002[, as added by section 223(a)(6) of this division], and the reporting requirements under section 226(c) of this division shall terminate on the date that is 7 years after the date of enactment of this Act.

(b) RULE OF CONSTRUCTION.—Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under [section 230(d)(2)]*section 2213(d)(2)* of the Homeland Security Act of 2002[, as added by section 223(a)(6) of this division], if such assistance

was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

* * * * * * *

TITLE IV—OTHER CYBER MATTERS

* * * * * * *

SEC. 404. ENHANCEMENT OF EMERGENCY SERVICES.

(a) COLLECTION OF DATA.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the center established under [section 227]*section 2209* of the Homeland Security Act of 2002[, as redesignated by section 223(a)(3) of this division,] in coordination with appropriate Federal entities and the [Director for Emergency Communications]*Assistant Director for Emergency Communications*, shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers (as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)) within the State.

(b) ANALYSIS OF DATA.—Not later than 1 year after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Director of the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the [Director for Emergency Communications] *Assistant Director for Emergency Communications*, and in consultation with the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology, shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations on security and resilience measures for any information system or network used by State emergency response providers.

* * * * * * *

INTEGRATED PUBLIC ALERT AND WARNING SYSTEM MODERNIZATION ACT OF 2015

* * * * * * *

SEC. 2. INTEGRATED PUBLIC AERT AND WARNING SYSTEM MODERNIZATION.

(a) * * *

(b) INTEGRATED PUBLIC ALERT AND WARNING SYSTEM SUBCOMMITTEE.—

(1) * * *

* * * * * * *

(6) RECOMMENDATIONS.—The Subcommittee shall—

(A) * * *

(B) * * *

(i) recommendations for common alerting and warning protocols, standards, terminology, and operating

procedures for the public alert and warning system; [and]

(ii) * * *

(I) * * *

* * * * * * *

(VII) provides redundant alert mechanisms, if practicable, to reach the greatest number of people regardless of whether they have access to, or use, any specified medium of communication or any particular device[.]*;*

(iii) recommendations for best practices of State, tribal, and local governments to follow to maintain the integrity of the public alert and warning system, including—

(I) The procedures for State, tribal, and local government officials to authenticate civil emergencies and initiate, modify, and cancel alerts transmitted through the public alert and warning system, including protocols and technology capabilities for—

(aa) the initiation, or prohibition on the initiation, of alerts by a single authorized or unauthorized individual; and

(bb) testing a State, tribal, or local government incident management and warning tool without accidentally initiating an alert through the public alert and warning system;

(II) the standardization, functionality, and interoperability of incident management and warning tools used by State, tribal, and local governments to notify the public of an emergency through the public alert and warning system;

(III) the training and recertification of emergency management personnel on best practices for originating and transmitting an alert through the public alert and warning system; and

(IV) the procedures, protocols, and guidance concerning the protective action plans that State, tribal, and local governments should issue to the public following an alert issued under the public alert and warning system.

(7) REPORT.—

(A) SUBCOMMITTEE SUBMISSION.—[Not later than]

(i) INITIAL REPORT.—Not later than 1 year after the date of enactment of this Act, the Subcommittee shall submit to the National Advisory Council a report containing any recommendations required to be developed under [paragraph (6)] *clauses (i) and (ii) of paragraphs (6)(B)* for approval by the National Advisory Council.

(ii) SECOND REPORT.—Not later than 18 months after the date of enactment of the Department of Homeland Security Authorization Act, the Subcommittee shall submit to the National Advisory Council a report containing any recommendations

required to be developed under paragraph (6)(B)(iii) for approval by the National Advisory Council.

(B) SUBMISSION BY NATIONAL ADVISORY COUNCIL.—If the National Advisory Council approves the recommendations contained in the [report] *reports* submitted under subparagraph (A), the National Advisory Council shall submit the [report] *reports* to—

* * * * * * *

(8) TERMINATION.—The Subcommittee shall terminate not later than [3] *5* years after the date of enactment of this Act.

(c) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this Act and the amendments made by this Act such sums as may be necessary for each of fiscal years 2016, 2017, and [2018] *2018, 2019, 2020,* and *2021*.

* * * * * * *

POST-KATRINA EMERGENCY MANAGEMENT REFORM ACT

* * * * * * *

TITLE VI—NATIONAL EMERGENCY MANAGEMENT

* * * * * * *

SEC. 602. DEFINITIONS.

In this title—

(1) the term "Administrator" means the Administrator of the Agency;

* * * * * * *

(13) the term "[National Response Plan] *National Response Framework"* means the [National Response Plan] *National Response Framework* or any successor plan prepared under section [502(a)(6)] *504(a)(6)* of the Homeland Security Act of 2002 (as amended by this Act);

* * * * * * *

Subtitle C—Comprehensive Preparedness System

* * * * * * *

CHAPTER 1—NATIONAL PREPAREDNESS SYSTEM

* * * * * * *

SEC. 643. NATIONAL PREPAREDNESS GOAL.

(a) * * *

(b) NATIONAL INCIDENT MANAGEMENT SYSTEM AND [NATIONAL RESPONSE PLAN] *NATIONAL RESPONSE FRAMEWORK.*—The national preparedness goal, to the greatest extent practicable, shall be con-

sistent with the National Incident Management System and the [National Response Plan] *National Response Framework*.

* * * * * * *

SEC. 648. TRAINING AND EXERCISES.

(a) NATIONAL TRAINING PROGRAM.—

(1) IN GENERAL.—Beginning not later than 180 days after the date of enactment of this Act, the Administrator, in coordination with the heads of appropriate Federal agencies, the National Council on Disability, and the National Advisory Council, shall carry out a national training program to implement the national preparedness goal, National Incident Management System, [National Response Plan] *National Response Framework*, and other related plans and strategies.

(2) * * *

(b) NATIONAL EXERCISE PROGRAM.—

(1) IN GENERAL.—Beginning not later than 180 days after the date of enactment of this Act, the Administrator, in coordination with the heads of appropriate Federal agencies, the National Council on Disability, and the National Advisory Council, shall carry out a national exercise program to test and evaluate the national preparedness goal, National Incident Management System, [National Response Plan] *National Response Framework*, and other related plans and strategies.

(2) REQUIREMENTS.—The national exercise program—

(A) shall be—

(i) * * *

* * * * * * *

(v) designed to address the unique requirements of populations with special needs; [and]

(vi) * * *

(vii) designed, to the extent practicable, to include exercises addressing emerging terrorist threats, such as scenarios involving United States citizens departing the United States to enlist with or provide material support or resources to terrorist organizations abroad or terrorist infiltration into the United States, including United States citizens and foreign nationals; and

* * * * * * *

SEC. 649. COMPREHENSIVE ASSESSMENT SYSTEM.

(a) * * *

(b) PERFORMANCE METRICS AND MEASURES.—The Administrator shall ensure that each component of the national preparedness system, National Incident Management System, [National Response Plan] *National Response Framework*, and other related plans and strategies, and the reports required under section 652 is developed, revised, and updated with clear and quantifiable performance metrics, measures, and outcomes.

(c) CONTENTS.—The assessment system established under subsection (a) shall assess—

(1) compliance with the national preparedness system, National Incident Management System, [National Response

Plan] *National Response Framework*, and other related plans and strategies;

* * * * * * *

[SEC. 650. REMEDIAL ACTION MANAGEMENT PROGRAM.

[The Administrator, in coordination with the National Council on Disability and the National Advisory Council, shall establish a remedial action management program to—

[(1) analyze training, exercises, and real-world events to identify and disseminate lessons learned and best practices;

[(2) generate and disseminate, as appropriate, after action reports to participants in exercises and real-world events; and

[(3) conduct remedial action tracking and long-term trend analysis.]

SEC. 650. REMEDIAL ACTION MANAGEMENT PROGRAM.

(a) IN GENERAL.—The Administrator, in coordination with the National Council on Disability and the National Advisory Council, shall establish a remedial action management program to—

(1) analyze training, exercises, and real world events to identify lessons learned, corrective actions, and best practices;

(2) generate and disseminate, as appropriate, the lessons learned, corrective actions, and best practices described in paragraph (1); and

(3) conduct remedial action tracking and long-term trend analysis.

(b) FEDERAL CORRECTIVE ACTIONS.—The Administrator, in coordination with the heads of appropriate Federal departments and agencies, shall—

(1) utilize the program established under subsection (a) to collect information on corrective actions identified by such Federal departments and agencies during exercises and the response to natural disasters, acts of terrorism, and other man-made disasters; and

(2) not later than 1 year after the date of the enactment of the FEMA Reauthorization Act of 2018 and annually thereafter for each of the next 4 years, submit to Congress a report on the status of those corrective actions.

(c) DISSEMINATION OF AFTER ACTION REPORTS.—The Administrator shall provide electronically, to the maximum extent practicable, to Congress and Federal, State, local, tribal, and private sector officials after-action reports and information on lessons learned and best practices from responses to acts of terrorism, natural disasters, capstone exercises conducted under the national exercise program under section 648(b), and other emergencies or exercises.

SEC. 651. FEDERAL RESPONSE CAPABILITY INVENTORY.

(a) * * *

(b) * * *

(c) DEPARTMENT OF DEFENSE.—The Administrator, in coordination with the Secretary of Defense, shall develop a list of organizations and functions within the Department of Defense that may be used, pursuant to the authority provided under the [National Response Plan] *National Response Framework* and sections 402, 403, and 502 of the Robert T. Stafford Disaster Relief and Emergency

Assistance Act (42 U.S.C. 5170a, 5170b, 5192), to provide support to civil authorities during natural disasters, acts of terrorism, and other man-made disasters.

(d) * * *

SEC. 652. REPORTING REQUIREMENTS.

(a) * * *

(b) CATASTROPHIC RESOURCE REPORT.—

(1) * * *

(2) CONTENTS.—Each estimate under paragraph (1) shall include the resources both necessary for and devoted to—

(A) * * *

* * * * * * *

(F) other responsibilities under the catastrophic incident annex and the catastrophic incident supplement of the [National Response Plan] *National Response Framework*;

(G) * * *

(H) * * *

(c) STATE PREPAREDNESS REPORT.—

(1) * * *

(2) CONTENTS.—Each report shall include—

(A) an assessment of State compliance with the national preparedness system, National Incident Management System, [National Response Plan] *National Response Framework*, and other related plans and strategies;

(B) * * *

(C) * * *

SEC. 653. FEDERAL PREPAREDNESS.

(a) AGENCY RESPONSIBILITY.—In support of the national preparedness system, the President shall ensure that each Federal agency with coordinating, primary, or supporting responsibilities under the [National Response Plan] *National Response Framework*—

(1) * * *

* * * * * * *

(4) develops deliberate operational plans and the corresponding capabilities, including crisis planning, to respond effectively to natural disasters, acts of terrorism, and other man-made disasters in support of the [National Response Plan] *National Response Framework* to ensure a coordinated Federal response.

(b) * * *

(c) MISSION ASSIGNMENTS.—To expedite the provision of assistance under the [National Response Plan] *National Response Framework*, the President shall ensure that the Administrator, in coordination with Federal agencies with responsibilities under the [National Response Plan] *National Response Framework*, develops prescripted mission assignments, including logistics, communications, mass care, health services, and public safety.

(d) COORDINATION.—The President, acting through the Administrator, shall develop and provide to Federal departments and agencies with coordinating, primary, or supporting responsibilities under the National Response Framework performance metrics to ensure

readiness to execute responsibilities under the emergency support functions of the National Response Framework.

[(d)]*(e)* CERTIFICATION.—The President shall certify on an annual basis that each Federal agency with coordinating, primary, or supporting responsibilities under the [National Response Plan] *National Response Framework* complies with subsections (a) and (b).

[(e)]*(f)* * * *

SEC. 654. USE OF EXISTING RESOURCES.

In establishing the national preparedness goal and national preparedness system, the Administrator shall use existing preparedness documents, planning tools, and guidelines to the extent practicable and consistent with this Act.

* * * * * * *

Subtitle G—Authorization of Appropriations

* * * * * * *

SEC. 699. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to carry out this title and the amendments made by this title for the [administration and operations] *management and administration* of the Agency—

(1) for fiscal year 2008, an amount equal to the amount appropriated for fiscal year 2007 for [administration and operations] *management and administration* of the Agency, multiplied by 1.1;

(2) for fiscal year 2009, an amount equal to the amount described in paragraph (1), multiplied by 1.1; [and]

(3) for fiscal year 2010, an amount equal to the amount described in paragraph (2), multiplied by 1.1[.]*; and*

(4) for fiscal year 2018, $1,049,000,000;

(5) for fiscal year 2019, $1,065,784,000; and

(6) for fiscal year 2020, $1,082,836,544.

* * * * * * *

ROBERT T. STAFFORD DISASTER RELIEF AND EMERGENCY ASSISTANCE ACT

* * * * * * *

TITLE II—DISASTER PREPAREDNESS AND MITIGATION ASSISTANCE

* * * * * * *

SEC. 203. PREDISASTER HAZARD MITIGATION.

(a) * * *

(b) * * *

(c) APPROVAL BY PRESIDENT.—If the President determines that a State or local government has identified natural disaster hazards in areas under its jurisdiction and has demonstrated the ability to

form effective public-private natural disaster hazard mitigation partnerships, the President, using amounts in the National *Public Infrastructure* Predisaster Mitigation Fund established under subsection (i) of this section (referred to in this section as the "Fund"), may provide technical and financial assistance to the State or local government to be used in accordance with subsection (e) of this section.

(d) * * *

(e) USES OF TECHNICAL AND FINANCIAL ASSISTANCE.—

(1) IN GENERAL.—Technical and financial assistance provided under this section—

(A) * * *

(B) may be used—

(i) to support effective public-private natural disaster hazard mitigation partnerships;

(ii) to improve the assessment of a community's vulnerability to natural hazards; **[**or**]**

(iii) to establish hazard mitigation priorities, and an appropriate hazard mitigation plan, for a community**[**.**]***; or*

(iv) to establish and carry out enforcement activities to implement the latest published editions of relevant consensus-based codes, specifications, and standards that incorporate the latest hazard-resistant designs and establish minimum acceptable criteria for the design, construction, and maintenance of residential structures and facilities that may be eligible for assistance under this Act for the purpose of protecting the health, safety, and general welfare of the buildings' users against disasters.

(2) * * *

(f) ALLOCATION OF FUNDS.—

(1) IN GENERAL—The President shall award financial assistance under this section on a competitive basis *for mitigation activities that are cost effective* and in accordance with the criteria in subsection (g).

(2) * * *

(3) REDISTRIBUTION OF UNOBLIGATED AMOUNTS.—The President may—

(A) withdraw amounts of financial assistance made available to a State (including amounts made available to local governments of a State) under this subsection that remain unobligated by the end of the third fiscal year after the fiscal year for which the amounts were allocated; and

(B) in the fiscal year following a fiscal year in which amounts were withdrawn under subparagraph (A), add the amounts to any other amounts available to be awarded on a competitive basis pursuant to paragraph (1).

(g) CRITERIA FOR ASSISTANCE AWARDS—In determining whether to provide technical and financial assistance to a State or local government under this section, the President shall *provide financial assistance only in States that have received a major disaster declaration during the previous 7-year period and* take into account—

* * * * * * *

(h) * * *

[(i) NATIONAL PREDISASTER MITIGATION FUND—

[(1) ESTABLISHMENT.—The President may establish in the Treasury of the United States a fund to be known as the "National Predisaster Mitigation Fund", to be used in carrying out this section.

[(2) TRANSFERS TO FUND.—There shall be deposited in the Fund—

[(A) amounts appropriated to carry out this section, which shall remain available until expended; and

[(B) sums available from gifts, bequests, or donations of services or property received by the President for the purpose of predisaster hazard mitigation.

[(3) EXPENDITURES FROM FUND.—Upon request by the President, the Secretary of the Treasury shall transfer from the Fund to the President such amounts as the President determines are necessary to provide technical and financial assistance under this section.

[(4) INVESTMENT OF AMOUNTS.—

[(A) IN GENERAL.—The Secretary of the Treasury shall invest such portion of the Fund as is not, in the judgment of the Secretary of the Treasury, required to meet current withdrawals. Investments may be made only in interest-bearing obligations of the United States.

[(B) ACQUISITION OF OBLIGATIONS.—For the purpose of investments under subparagraph (A), obligations may be acquired—

[(i) on original issue at the issue price; or

[(ii) by purchase of outstanding obligations at the market price.

[(C) SALE OF OBLIGATIONS.—Any obligation acquired by the Fund may be sold by the Secretary of the Treasury at the market price.

[(D) CREDITS TO FUND.—The interest on, and the proceeds from the sale or redemption of, any obligations held in the Fund shall be credited to and form a part of the Fund.

[(E) TRANSFERS OF AMOUNTS.—

[(i) IN GENERAL.—The amounts required to be transferred to the Fund under this subsection shall be transferred at least monthly from the general fund of the Treasury to the Fund on the basis of estimates made by the Secretary of the Treasury.

[(ii) ADJUSTMENTS.—Proper adjustment shall be made in amounts subsequently transferred to the extent prior estimates were in excess of or less than the amounts required to be transferred.]

(i) NATIONAL PUBLIC INFRASTRUCTURE PREDISASTER MITIGATION ASSISTANCE.—

(1) IN GENERAL.—The President may set aside from the Disaster Relief Fund, with respect to each major disaster, an amount equal to 6 percent of the estimated aggregate amount of the grants to be made pursuant to sections 403, 406, 407, 408, 410, and 416 for the major disaster in order to provide technical and financial assistance under this section.

(2) ESTIMATED AGGREGATE AMOUNT.—Not later than 180 days after each major disaster declaration pursuant to this Act, the estimated aggregate amount of grants for purposes of paragraph (1) shall be determined by the President and such estimated amount need not be reduced, increased, or changed due to variations in estimates.

(3) NO REDUCTION IN AMOUNTS.—The amount set aside pursuant to paragraph (1) shall not reduce the amounts otherwise made available for sections 403, 404, 406, 407, 408, 410, and 416 under this Act.

[(j) LIMITATION ON TOTAL AMOUNT OF FINANCIAL ASSISTANCE.—The President shall not provide financial assistance under this section in an amount greater than the amount available in the Fund.]

[(k)]*(j)* * * *

[(l)]*(k)* * * *

[(m) AUTHORIZATION OF APPROPRIATIONS—There are authorized to be appropriated to carry out this section—

[(1) $180,000,000 for fiscal year 2011;

[(2) $200,000,000 for fiscal year 2012;

[(3) $200,000,000 for fiscal year 2013.]

[(n)]*(l)* * * *

* * * * * * *

TITLE III—MAJOR DISASTER AND EMERGENCY ASSISTANCE ADMINISTRATION

* * * * * * *

SEC. 306. PERFORMANCE OF SERVICES.

(a) * * *

(b) * * *

(c) The Administrator of the Federal Emergency Management Agency may appoint temporary personnel, after serving continuously for 3 years, to positions in the Federal Emergency Management Agency in the same manner that competitive service employees with competitive status are considered for transfer, reassignment, or promotion to such positions. An individual appointed under this subsection shall become a career-conditional employee, unless the employee has already completed the service requirements for career tenure.

* * * * * * *

SEC. 324. MANAGEMENT COSTS.

(a) DEFINITION OF MANAGEMENT COST.—In this section, the term "management cost" includes any indirect cost, [any administrative expense, and any other expense not directly chargeable to] *direct administrative cost, and any other administrative expense associated with* a specific project under a major disaster, emergency, or disaster preparedness or mitigation activity or measure.

(b) ESTABLISHMENT OF MANAGEMENT COST RATES.—[Notwithstanding]

(1) IN GENERAL.—Notwithstanding any other provision of law (including any administrative rule or guidance), the President shall by regulation [establish] *implement* management cost

rates, for grantees and subgrantees, that shall be used to determine contributions under this Act for management costs.

(2) SPECIFIC MANAGEMENT COSTS.—The Administrator shall provide for management costs, in addition to the eligible project costs, to cover direct and indirect costs of administering the following programs:

(A) HAZARD MITIGATION.—A grantee under section 404 may be reimbursed for direct and indirect administrative costs in a total amount of not more than 15 percent of the total amount of the grant award under such section of which not more than 10 percent may be used by the grantee and 5 percent by the subgrantee for such costs.

(B) PUBLIC ASSISTANCE.—A grantee under sections 403, 406, 407, and 502 may be reimbursed direct and indirect administrative costs in a total amount of not more than 12 percent of the total award amount under such sections, of which not more than 7 percent may be used by the grantee and 5 percent by the subgrantee for such costs.

(c) REVIEW.—The President shall review the management cost rates established under subsection (b) not later than 3 years after the date of establishment of the rates and periodically thereafter.

* * * * * * *

TITLE IV—MAJOR DISASTER ASSISTANCE PROGRAMS

* * * * * * *

SEC. 430. AGENCY ACCOUNTABILITY.

(a) PUBLIC ASSISTANCE.—Not later than 5 days after the date on which an award of a public assistance grant is made under section 406 that is in excess of $1,000,000, the Administrator of the Federal Emergency Management Agency (referred to in this section as the 'Administrator') shall publish on the website of the Federal Emergency Management Agency (referred to in this section as the 'Agency') the specifics of each such grant award, including identifying—

(1) the Federal Emergency Management Agency Region;

(2) the major disaster or emergency declaration number;

(3) the State, county, and applicant name;

(4) if the applicant is a private nonprofit organization;

(5) the damage category code;

(6) the amount of the Federal share obligated; and

(7) the date of the award.

(b) MISSION ASSIGNMENTS.—

(1) IN GENERAL.—Not later than 5 days after the date on which a mission assignment or mission assignment task order is issued under section 402(1) or section 502(a)(1), the Administrator shall publish on the website of the Agency any mission assignment or mission assignment task order to another Federal department or agency regarding a major disaster in excess of $1,000,000, including—

(A) the name of the impacted State or Indian tribe;

(B) the major disaster declaration for such State or Indian tribe;

(C) the assigned agency;

(D) the assistance requested;

(E) a description of the major disaster;

(F) the total cost estimate;

(G) the amount obligated;

(H) the State or tribal cost share, if applicable;

(I) the authority under which the mission assignment or mission assignment task order was directed; and

(J) if applicable, the date on which a State or Indian tribe requested the mission assignment.

(2) RECORDING CHANGES.—Not later than 10 days after the last day of each month until a mission assignment or mission assignment task order described in paragraph (1) is completed and closed out, the Administrator shall update any changes to the total cost estimate and the amount obligated.

(c) DISASTER RELIEF MONTHLY REPORT.—Not later than 10 days after the first day of each month, the Administrator shall publish reports on the website of the Agency, including a specific description of the methodology and the source data used in developing such reports, including—

(1) an estimate of the amounts for the fiscal year covered by the President's most recent budget pursuant to section 1105(a) of title 31, United States Code, including—

(A) the unobligated balance of funds to be carried over from the prior fiscal year to the budget year;

(B) the unobligated balance of funds to be carried over from the budget year to the year after the budget year;

(C) the amount of obligations for noncatastrophic events for the budget year;

(D) the amount of obligations for the budget year for catastrophic events, as defined under the National Response Framework, delineated by event and by State;

(E) the total amount that has been previously obligated or will be required for catastrophic events delineated by event and by State for all prior years, the current fiscal year, the budget year, and each fiscal year thereafter;

(F) the amount of previously obligated funds that will be recovered for the budget year;

(G) the amount that will be required for obligations for emergencies, major disasters, fire management assistance grants, as described in section 420, surge activities, and disaster readiness and support activities; and

(H) the amount required for activities not covered under section 251(b)(2)(D)(iii) of the Balanced Budget and Emergency Deficit Control Act of 1985 (2 U.S.C. 901(b)(2)(D)(iii));

(2) a summary of the amount for disaster relief of—

(A) appropriations made available by source;

(B) the transfers executed;

(C) the previously allocated funds recovered; and

(D) the commitments, allocations, and obligations made;

(3) a table of disaster relief activity delineated by month, including—

(A) the beginning and ending balances;

(B) the total obligations to include amounts obligated for fire assistance, emergencies, surge, and disaster support activities;

(C) the obligations for catastrophic events delineated by event and by State; and

(D) the amount of previously obligated funds that are recovered;

(4) a summary of allocations, obligations, and expenditures for catastrophic events delineated by event;

(5) the cost with respect to—

(A) public assistance;

(B) individual assistance;

(C) mitigation;

(D) administrative activities;

(E) operations; and

(F) any other relevant category (including emergency measures and disaster resources) delineated by major disaster; and

(6) the date on which funds appropriated will be exhausted.

(d) CONTRACTS.—

(1) INFORMATION.—

(A) IN GENERAL.—Not later than 10 days after the first day of each month, the Administrator shall publish on the website of the Agency the specifics of each contract in excess of $1,000,000 that the Agency enters into during the previous month, including—

(i) the name of the party;

(ii) the date the contract was awarded;

(iii) the amount and scope of the contract;

(iv) if the contract was awarded through competitive bidding process;

(v) if no competitive bidding process was used, the reason why competitive bidding was not used; and

(vi) the authority used to bypass the competitive bidding process.

(B) REQUIREMENT.—The information required to be published under subparagraph (A) shall be delineated by major disaster, if applicable, and specify the damage category code, if applicable.

(2) REPORT.—Not later than 10 days after the last day of the fiscal year, the Administrator shall provide a report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives summarizing the following information for the preceding fiscal year:

(A) The number of contracts awarded without competitive bidding.

(B) The reasons why a competitive bidding process was not used.

(C) The total amount of contracts awarded with no competitive bidding.

(D) The damage category codes, if applicable, for contracts awarded without competitive bidding.

* * * * * * *

UNITED STATES CODE

* * * * * * *

TITLE 5—GOVERNMENT ORGANIZATION AND EMPLOYEES

* * * * * * *

PART III—EMPLOYEES

* * * * * * *

Subpart C—Employee Performance

* * * * * * *

CHAPTER 45—INCENTIVE AWARDS

* * * * * * *

Table of Sections

* * * * * * *

4512. Agency Awards for cost savings disclosures.
4512A. Department of Homeland Security awards for cost savings disclosures.

* * * * * * *

Subchapter I—Awards for Superior Accomplishments

* * * * * * *

SEC. 4509. PROHIBITION OF CASH AWARD TO EXECUTIVE SCHEDULE OFFICERS.

(a) No officer may receive a cash award under the provisions of this subchapter, if such officer—

(1) * * *

(2) was appointed to such position by the President, by and with the advice and consent of the Senate.

(b) The Secretary of Homeland Security may not receive a cash award under this subchapter.

* * * * * * *

SEC. 4512. * * *

SEC. 4512A. DEPARTMENT OF HOMELAND SECURITY AWARDS FOR COST SAVINGS DISCLOSURES.

(a) In this section, the term 'surplus operations and support funds' means amounts made available for the operations and support account, or equivalent account, of the Department of Homeland Security, or a component thereof—

(1) that are identified by an employee of the Department of Homeland Security under subsection (b) as unnecessary;

(2) that the Inspector General of the Department of Homeland Security determines are not required for the purpose for which the amounts were made available;

(3) that the Chief Financial Officer of the Department of Homeland Security determines are not required for the purpose for which the amounts were made available; and

(4) the rescission of which would not be detrimental to the full execution of the purposes for which the amounts were made available.

(b) The Inspector General of the Department of Homeland Security may pay a cash award to any employee of the Department of Homeland Security whose disclosure of fraud, waste, or mismanagement or identification of surplus operations and support funds to the Inspector General of the Department of Homeland Security has resulted in cost savings for the Department of Homeland Security. The amount of an award under this section may not exceed the lesser of—

(1) $10,000; or

(2) an amount equal to 1 percent of the Department of Homeland Security's cost savings which the Inspector General determines to be the total savings attributable to the employee's disclosure or identification.

For purposes of paragraph (2), the Inspector General may take into account Department of Homeland Security cost savings projected for subsequent fiscal years which will be attributable to such disclosure or identification.

(c)

(1) The Inspector General of the Department of Homeland Security shall refer to the Chief Financial Officer of the Department of Homeland Security any potential surplus operations and support funds identified by an employee that the Inspector General determines meets the requirements under paragraphs (2) and (4) of subsection (a), along with any recommendations of the Inspector General.

(2)

(A) If the Chief Financial Officer of the Department of Homeland Security determines that potential surplus operations and support funds referred under paragraph (1) meet the requirements under subsection (a), except as provided in subsection (d), the Secretary of Homeland Security shall transfer the amount of the surplus operations and support funds from the applicable appropriations account to the general fund of the Treasury.

(B) Any amounts transferred under subparagraph (A) shall be deposited in the Treasury and used for deficit reduction, except that in the case of a fiscal year for which there is no Federal budget deficit, such amounts shall be used to reduce the Federal debt (in such manner as the Secretary of the Treasury considers appropriate).

(3) The Inspector General of the Department of Homeland Security and the Chief Financial Officer of the Department of Homeland Security shall issue standards and definitions for purposes of making determinations relating to potential surplus operations and support funds identified by an employee under this subsection.

(d)

(1) The Secretary of Homeland Security may retain not more than 10 percent of amounts to be transferred to the general fund of the Treasury under subsection (c)(2).

(2) Amounts retained by the Secretary of Homeland Security under paragraph (1) may be—

(A) used for the purpose of paying a cash award under subsection (b) to one or more employees who identified the surplus operations and support funds; and

(B) to the extent amounts remain after paying cash awards under subsection (b), transferred or reprogrammed for use by the Department of Homeland Security, in accordance with any limitation on such a transfer or reprogramming under any other provision of law.

(e)

(1) Not later than October 1 of each fiscal year, the Secretary of Homeland Security shall submit to the Secretary of the Treasury a report identifying the total savings achieved during the previous fiscal year through disclosures of possible fraud, waste, or mismanagement and identifications of surplus operations and support funds by an employee.

(2) Not later than September 30 of each fiscal year, the Secretary of Homeland Security shall submit to the Secretary of the Treasury a report that, for the previous fiscal year—

(A) describes each disclosure of possible fraud, waste, or mismanagement or identification of potentially surplus operations and support funds by an employee of the Department of Homeland Security determined by the Department of Homeland Security to have merit; and

(B) provides the number and amount of cash awards by the Department of Homeland Security under subsection (b).

(3) The Secretary of Homeland Security shall include the information described in paragraphs (1) and (2) in each budget request of the Department of Homeland Security submitted to the Office of Management and Budget as part of the preparation of the budget of the President submitted to Congress under section 1105(a) of title 31.

(4) The Secretary of the Treasury shall submit to the Committee on Appropriations of the Senate, the Committee on Appropriations of the House of Representatives, and the Government Accountability Office an annual report on Federal cost saving and awards based on the reports submitted under paragraphs (1) and (2).

(f) The Director of the Office of Personnel Management shall—

(1) ensure that the cash award program of the Department of Homeland Security complies with this section; and

(2) submit to Congress an annual certification indicating whether the cash award program of the Department of Homeland Security complies with this section.

(g) Not later than 3 years after the date of enactment of this section, and every 3 years thereafter, the Comptroller General of the United States shall submit to Congress a report on the operation of the cost savings and awards program under this section, including any recommendations for legislative changes.

* * * * * * *

Subpart D—Pay and Allowances

* * * * * * *

CHAPTER 53—PAY AND RATES SYSTEM

* * * * * * *

Subchapter II—Executive Schedule Pay Rates

* * * * * * *

SEC. 5314. POSITIONS AT LEVEL III.

Level III of the Executive Schedule applies to the following positions, for which the annual rate of basic pay shall be the rate determined with respect to such level under chapter 11 of title 2, as adjusted by section 5318 of this title:

* * * * * * *

Under Secretaries, Department of Homeland Security.

Director, Cybersecurity and Infrastructure Security Agency.

* * * * * * *

SEC. 5315 POSITIONS AT LEVEL IV.

Level IV of the Executive Schedule applies to the following positions, for which the annual rate of basic pay shall be the rate determined with respect to such level under chapter 11 of title 2, as adjusted by section 5318 of this title:

* * * * * * *

Assistant Secretaries, Department of Homeland Security.

Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency

Assistant Director for Infrastructure Security, Cybersecurity and Infrastructure Security Agency.

* * * * * * *

SEC. 10102. STRATEGIC HUMAN CAPITAL PLAN.

(a) * * *

(b) * * *

(c) ANNUAL UPDATES.—Not later than May 1, **[**2007**]** *2018*, and May 1st of each of the next 5 succeeding years, the Administrator shall submit to the appropriate committees of Congress an update on the strategic human capital plan, including an assessment by the Administrator, using results-oriented performance measures, of the progress of the Department and the Agency in implementing the strategic human capital plan.

* * * * * * *

TITLE 6—DOMESTIC SECURITY

* * * * * * *

CHAPTER 4—TRANSPORTATION SECURITY

* * * * * * *

Subchapter I—Transportation Security Planning and Information Sharing

* * * * * * *

SEC. 1102. NATIONAL PREPAREDNESS CONSORTIUM.

(a) * * *

(b) MEMBERS.—Members of the National Domestic Preparedness Consortium shall consist of—

(1) * * *

* * * * * * *

(4) the National Emergency Response and [Rescue] *Recovery* Training Center, Texas A&M University;

* * * * * * *

(c) DUTIES.—The National Domestic Preparedness Consortium shall identify, develop, test, and deliver training to State, local, and tribal emergency response providers, provide on-site and mobile training at the performance and management and planning levels *to the extent practicable, provide training in settings that simulate eal response environments, such as urban areas*, and facilitate the delivery of training by the training partners of the Department.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary—

[(1) for the Center for Domestic Preparedness—

[(A) $57,000,000 for fiscal year 2008;

[(B) $60,000,000 for fiscal year 2009;

[(C) $63,000,000 for fiscal year 2010; and

[(D) $66,000,000 for fiscal year 2011; and]

[(2) for the National Energetic Materials Research and Testing Center, the National Center for Biomedical Research and Training, the National Emergency Response and [Rescue]*Recovery* Training Center, the National Exercise Test, and Training Center, the Transportation Technology Center, Incorporated, and the National Disaster Preparedness Training Center each—

[(A) $22,000,000 for fiscal year 2008;

[(B) $23,000,000 for fiscal year 2009;

[(C) $24,000,000 for fiscal year 2010; and

[(D) $25,000,000 for fiscal year 2011.]

(1) for the Center for Domestic Preparedness—

(A) $63,939,000 for fiscal year 2018;

(B) $64,962,024 for fiscal year 2019; and

(C) $66,001,416 for fiscal year 2020; and

(2) for the members of the National Domestic Preparedness Consortium described in paragraphs (2) through (7) of subsection (b)—

(A) $101,000,000 for fiscal year 2018;

(B) $102,606,000 for fiscal year 2019; and

(C) $104,247,856 for fiscal year 2020.

(e) SAVINGS PROVISION.—From the amounts appropriated pursuant to this section, the Secretary shall ensure that future amounts provided to [each of the following entities] *members of the National Domestic Preparedness Consortium enumerated in subsection (b)* are not less than the amounts provided to each such entity for participation in the Consortium in fiscal year [2007—]*2005*.

[(1) the Center for Domestic Preparedness;

(2) the National Energetic Materials Research and Testing Center, New Mexico Institute of Mining and Technology;

(3) the National Center for Biomedical Research and Training, Louisiana State University;

(4) the National Emergency Response and [Rescue] *Recovery* Training Center, Texas A&M University; and

(5) the National Exercise, Test, and Training Center, Nevada Test Site.]

* * * * * * *

Subchapter III—Public Transportation Security

* * * * * * *

SEC. 1135. PUBLIC TRANSPORTATION SECURITY ASSISTANCE.

(a) * * *

(b) USE OF FUNDS.—A recipient of a grant under subsection (a) shall use the grant funds for one or more of the following:

(1) * * *

(2) Operating uses of funds, including—

(A) security training *and costs associated with filling the positions of employees receiving training during their absense*, including training under section 1137 of this title and training developed by institutions of higher education and by nonprofit employee labor organizations, for public transportation employees, including frontline employees;

* * * * * * *

[(m) AUTHORIZATION OF APPROPRIATIONS.—

[(1) There are authorized to be appropriated to the Secretary to make grants under this section—

[(A) such sums as are necessary for fiscal year 2007;

[(B) $650,000,000 for fiscal year 2008, except that not more than 50 percent of such funds may be used for operational costs under subsection (b)(2);

[(C) $750,000,000 for fiscal year 2009, except that not more than 30 percent of such funds may be used for operational costs under subsection (b)(2);

[(D) $900,000,000 for fiscal year 2010, except that not more than 20 percent of such funds may be used for operational costs under subsection (b)(2); and

[(E) $1,100,000,000 for fiscal year 2011, except that not more than 10 percent of such funds may be used for operational costs under subsection (b)(2).

[(2) PERIOD OF AVAILABILITY.—Sums appropriated to carry out this section shall remain available until expended.

[(3) WAIVER.—The Secretary may waive the limitation on operational costs specified in subparagraphs (B) through (E) of paragraph (1) if the Secretary determines that such a waiver is required in the interest of national security, and if the Secretary provides a written justification to the appropriate congressional committees prior to any such action.

[(4) EFFECTIVE DATE.—Funds provided for fiscal year 2007 transit security grants under Public Law 110–28 shall be allocated based on security assessments that are in existence as of August 3, 2007.]

(m) PERIODS OF PERFORMANCE.—Funds provided pursuant to a grant awarded under this section for a use specified in subsection

(b) shall remain available for use by a grant recipient for a period of not fewer than 36 months.

* * * * * * *

TITLE 15—COMMERCE AND TRADE

* * * * * * *

CHAPTER 14A—AID TO SMALL BUSINESS

* * * * * * *

SEC. 648. SMALL BUSINESS DEVELOPMENT CENTER PROGRAM AUTHORIZATION.

(a) * * *

(1) * * *

* * * * * * *

(8) CYBERSECURITY ASSISTANCE.—

(A) IN GENERAL.—The Department of Homeland Security, and any other Federal department or agency in coordination with the Department of Homeland Security, may leverage small business development centers to provide assistance to small business concerns by disseminating information relating to cybersecurity risks and other homeland security matters to help small business concerns in developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees.

(B) DEFINITIONS.—In this paragraph, the terms "cybersecurity risk" and "cyber threat indicator" have the meanings given such terms, respectively, under **[**section 227(a) of the Homeland Security Act of 2002 (6 U.S.C. 148(a))**]** *section 2209(a) of the Homeland Security Act of 2002*.

* * * * * * *

TITLE 19—CUSTOMS DUTIES

* * * * * * *

CHAPTER 4—THE TARIFF ACT OF 1930

* * * * * * *

Subtitle III—Administrative Provisions

* * * * * * *

PART II—REPORT, ENTRY, AND UNLOADING OF VESSELS AND VEHICLES

* * * * * * *

SEC. 1431. MANIFESTS.

(a) * * *

(b) * * *

(c) * * *

(1) * * *

[(2) The information listed in paragraph (1) shall not be available for public disclosure if—

[(A) the Secretary of the Treasury makes an affirmative finding on a shipment-by-shipment basis that disclosure is likely to pose a threat of personal injury or property damage; or

[(B) the information is exempt under the provisions of section 552(b)(1) of title 5.]

(A) The information listed in paragraph (1) shall not be available for public disclosure if—

(i) the Secretary of the Treasury makes an affirmative finding on a shipment-by-shipment basis that disclosure is likely to pose a threat of personal injury or property damage; or

(ii) the information is exempt under the provisions of section 552(b)(1) of title 5, United States Code.

(B) The Commissioner of U.S. Customs and Border Protection shall ensure that any personally identifiable information, including social security numbers, passport numbers, and residential addresses, is removed from any manifest signed, produced, delivered, or transmitted under this section before the manifest is disclosed to the public.

* * * * * * *

TITLE 42—THE PUBLIC HEALTH AND WELFARE

* * * * * * *

CHAPTER 6A—PUBLIC HEALTH SERVICE

* * * * * * *

Subchapter XXVI—National All–Hazards Preparedness for Public Health Emergencies

* * * * * * *

PART A—NATIONAL ALL–HAZARDS PREPAREDNESS AND RESPONSE PLANNING, COORDINATION, AND REPORTING

* * * * * * *

SEC. 300hh. PUBLIC HEALTH AND MEDICAL PREPAREDNESS AND RESPONSE FUNCTIONS.

(a) IN GENERAL.—The Secretary of Health and Human Services shall lead all Federal public health and medical response to public health emergencies and incidents covered by [the National Response Plan developed pursuant to section 502(6) of the Homeland Security Act of 2002] *the National Response Framework developed pursuant to section 504(a)(6) of the Homeland Security Act of 2002 (2 U.S.C. 314(a)(6))*, or any successor plan.

* * * * * * *

TITLE 46—SHIPPING

* * * * * * *

Subtitle VII—Security and Drug Enforcement

* * * * * * *

CHAPTER 701—PORT SECURITY

* * * * * * *

Subchapter I—General

* * * * * * *

SEC. 70107. GRANTS.

(a) * * *

* * * * * * *

[(l) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $400,000,000 for each of the fiscal years 2007 through 2013 to carry out this section.**]**

[(m)](*l*) * * *

(m) PERIOD OF PERFORMANCE.—The Secretary shall make funds under this section available for use by a recipient of a grant for a period of not less than 36 months.

* * * * * * *

TITLE 50—WAR AND NATIONAL DEFENSE

* * * * * * *

CHAPTER 40—DEFENSE AGAINST WEAPONS OF MASS DESTRUCTION ACT OF 1996

* * * * * * *

Subchapter I—Domestic Preparedness

* * * * * * *

SEC. 2314. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND HIGH–YIELD EXPLOSIVES RESPONSE TEAM.

(a) * * *

(b) ADDITION TO FEDERAL RESPONSE PLANS.—The Secretary of Homeland Security shall incorporate into the **[**National Response Plan prepared pursuant to section 502(6)[1] of the Homeland Security Act of 2002 (6 U.S.C. 312(6))**]** *National Response Framework prepared pursuant to section 504(a)(6) of the Homeland Security Act of 2002 (6 U.S.C. 314(a)(6)),* other existing Federal emergency response plans, and programs prepared under section 5196(b) of title 42 guidance on the use and deployment of the rapid response teams established under this section to respond to emergencies involving weapons of mass destruction. The Secretary of Homeland Security shall carry out this subsection in coordination with the

Secretary of Defense and the heads of other Federal agencies involved with the emergency response plans.

* * * * * * *

○