115TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 115–454
Part 1

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY ACT OF 2017

DECEMBER 11, 2017.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

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

R E P O R T

[To accompany H.R. 3359]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3359) to amend the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

79–006

PURPOSE AND SUMMARY

The purpose of H.R. 3359 is to amend the Homeland Security Act of 2002 (Pub. L. 107–296) to authorize a cybersecurity and infrastructure security agency within the Department of Homeland Security (DHS), and for other purposes. H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act of 2017, redesignates the existing National Protection and Programs Directorate (NPPD) as such Agency.

The agency will be led by a Director with responsibilities that include: leading cybersecurity and infrastructure security programs, operations, and associated policy for the Agency; maintaining and utilizing coordination mechanisms for ongoing consultation and collaboration among Agency divisions; and developing, coordinating and implementing comprehensive strategic plans and risk assessments. The bill also delineates cybersecurity and infrastructure security authorities for the Secretary.

H.R. 3359 establishes the Cybersecurity Division, headed by an Assistant Director, and the Infrastructure Security Division, headed by an Assistant Director, within the Agency. This legislation establishes the current Office of Emergency Communications (OEC) as a Division in the Agency with an Assistant Director reporting directly to the head of the Agency and maintains all of the current OEC functions. The bill includes a number of conforming amendments to ensure current authorities remain within the new agency. Finally, the legislation transfers the Office of Biometric Identity Management to the Management Directorate in DHS and provides the Secretary flexibility to move the Federal Protective Service.

BACKGROUND AND NEED FOR LEGISLATION

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace is an essential homeland security mission. This bill provides the necessary overarching structure for DHS to carry out its cybersecurity mission while also providing intradepartmental flexibility to best allow DHS to execute its mission in the cybersecurity and infrastructure security space. The redesignation and elevation of these missions within DHS will better allow DHS to carry out its operational mission and recruit the best work force to achieve this mission.

The bill realigns the current NPPD structure so it can more effectively carryout the existing authorities provided in law, including those provided in the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016, Pub.L. 114–113). The Cybersecurity and Infrastructure Security Agency will be structured to best work with partners at all levels of government, and from the private and non-profit sectors, to share information and build greater trust in order to make our cyber and physical infrastructure more secure.

HEARINGS

No hearings were held on H.R. 3359 in the 115th Congress. However the Committee held the following oversight hearings which informed the legislation:

114th Congress

On February 12, 2015, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Emerging Threats and Technologies to Protect the Homeland." The Subcommittee received testimony from Dr. Andy Ozment, Assistant Secretary, Office of Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security; Dr. Huban Gowadia, Director, Domestic Nuclear Detection Office, U.S. Department of Homeland Security; Mr. Joseph Martin, Acting Director, Homeland Security Enterprise and First Responders Group, Science and Technology Directorate, U.S. Department of Homeland Security; Mr. William Noonan, Deputy Special Agent in Charge, Criminal Investigative Division, Cyber Operations Branch, United States Secret Service, U.S. Department of Homeland Security; and Mr. William Painter, Analyst, Government and Finance Division, Congressional Research Service, Library of Congress.

On February 25, 2015, the Full Committee held a hearing entitled "Examining the President's Cybersecurity Information Sharing Proposal." The Committee received testimony from Hon. Suzanne Spaulding, Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security; Dr. Phyllis Schneck, Deputy Under Secretary, Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security; and Dr. Eric Fischer, Senior Specialist, Science and Technology, Congressional Research Service, Library of Congress.

On June 24, 2015, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "DHS' Efforts to Secure .Gov." The Subcommittee received testimony from Dr. Andy Ozment, Assistant Secretary, Office of Cybersecurity and Communications, National Programs and Protections Directorate, U.S. Department of Homeland Security; Mr. Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office; and Dr. Daniel M. Gerstein, The RAND Corporation.

On October 7, 2015, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Examining the Mission, Structure, and Reorganization Effort of the National Protection and Programs Directorate." The Subcommittee received testimony from Hon. Suzanne Spaulding, Under Secretary, National Programs and Protection Directorate, U.S. Department of Homeland Security; Dr. Phyllis Schneck, Deputy Under Secretary, Cybersecurity and Communications, National Programs and Protections Directorate, U.S. Department of Homeland Security; Dr. Ronald J. Clark, Deputy Under Secretary, National Programs and Protections Directorate, U.S. Department of Homeland Security; and Mr. Chris P. Currie, Director, Emergency Management National Preparedness and Critical Infrastructure

Protection Homeland Security and Justice Team, U.S. Government Accountability Office.

On February 25, 2016, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Emerging Cyber Threats to the United States." The Subcommittee received testimony from Mr. Frank Cillufo, Associate Vice President and Director, Center for Cyber and Homeland Security, The George Washington University; Ms. Jennifer Kolde, Lead Technical Director, FireEye Threat Intelligence; Mr. Adam Bromwich, Vice President, Security Technology and Response, Symantec, *testifying on behalf of the Cyber Threat Alliance*; and Dr. Isaac Porche, Associate Director, Forces and Logistics Program, The RAND Army Research Division, The RAND Corporation.

On April 7, 2016, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a field hearing in Sherman, Texas, entitled "Cyber Preparedness and Response at the Local Level." The Subcommittee received testimony from Mr. Alphonse G. Davis, Deputy Director/Chief Operations Officer, Texas A&M Engineering Extension Service; Mr. Sam Greif, Chief, Plano Fire–Rescue Department, Plano, Texas, *testifying on behalf of the International Association of Fire Chiefs*; Mr. Richard F. Wilson, Lieutenant, Dallas Police Department, Dallas, Texas; and Mr. Don Waddle, Detective (Ret.), Greenville Police Department, Greenville, Texas.

The Subcommittee on Emergency Preparedness, Response, and Communications and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a joint hearing on May 24, 2016, entitled "Enhancing Preparedness and Response Capabilities to Address Cyber Threats." The Subcommittees received testimony from Mr. Mark Ghilarducci, Director, Emergency Services, Office of the Governor, State of California; Lt. Col. Daniel J. Cooney, Assistant Deputy Superintendent, Office of Counter Terrorism, New York State Police; Brig. Gen. Steven Spano (Ret.—USAF), President and Chief Operating Officer, Center for Internet Security; Mr. Mark Raymond, Vice President, National Association of State Chief Information Officers; and Mr. Robert Galvin, Chief Technology Officer, Port Authority of New York and New Jersey.

On July 12, 2016, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Value of DHS' Vulnerability Assessments in Protecting our Nation's Critical Infrastructure." The Subcommittee received testimony from Mr. Chris P. Currie, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office; Dr. Andy Ozment, Assistant Secretary, Office of Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security; Ms. Caitlin Durkovich, Assistant Secretary, Office of Infrastructure Protection, National Protection and Programs Directorate, U.S. Department of Homeland Security; and Mr. Marcus L. Brown, Homeland Security Advisor, Director of the Office of Homeland Security, Commonwealth of Pennsylvania.

115th Congress

On March 9, 2017, the Subcommittee on Cybersecurity and Infrastructure Protection held a hearing entitled "The Current State of

DHS Private Sector Engagement for Cybersecurity." The Subcommittee received testimony from Mr. Daniel Nutkis, Chief Execurive Officer, HITRUST Alliance; Mr. Scott Montgomery, Vice President and Chief Technical Strategist, Intel Security Group, Intel Corporation; Mr. Jeffrey Greene, Senior Director, Global Government Affairs and Policy Symantec; Mr. Ryan M Gillis, Vice President of Cybersecurity Strategy and Global Policy, Palo Alto Networks; and Ms. Robyn Greene, Policy Counsel and Government Affairs Lead, Open Technology Institute, New America.

On March 22, 2017, the Full Committee held a hearing entitled "A Borderless Battle: Defending Against Cyber Threats." The Committee received testimony from GEN Keith B. Alexander (Ret. USA), President and Chief Executive Officer, IronNet Cybersecurity; Mr. Michael Daniel, President, Cyber Threat Alliance; Mr. Frank J. Cilluffo, Director, Center for Cyber and Homeland Security, George Washington University; and Mr. Bruce W. McConnell, Global Vice President, EastWest Institute.

On March 28, 2017, the Subcommittee on Cybersecurity and Infrastructure Protection held a hearing entitled "The Current State of DHS Efforts to Secure the Federal Networks." The Subcommittee received testimony from Ms. Jeanette Manfra, Acting Deputy Undersecretary for Cybersecurity, National Protection and Programs Directorate, U.S. Department of Homeland Security; Mr. Gregory C. Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office; and Mr. Chris A. Jaikaran, Analyst, Cybersecurity Policy, Congressional Research Service, Library of Congress.

On September 7, 2017, the Subcommittee on Cybersecurity and Infrastructure Protection held a hearing entitled "Challenges of Recruiting and Retaining a Cybersecurity Workforce." The Subcommittee received testimony from Dr. Frederick R. Chang, Executive Director, Darwin Deason Institute for Cyber Security, Southern Methodist University; Mr. Scott Montgomery, Vice President and Chief Technical Strategist, McAfee; Dr. Michael Papay, Vice President and Chief Information Security Officer, Northrop Grumman; and Ms. Juliet "Jules" Okafor, Vice President, Global Business Development, Fortress Information Security.

On October 3, 2017, the Subcommittee on Cybersecurity and Infrastructure Protection held a hearing entitled "Examining DHS's Cybersecurity Mission." The Subcommittee received testimony from Mr. Christopher Krebs, Senior Official Performing the Duties of the Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security; Ms. Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security; and Ms. Patricia Hoffman, Acting Assistant Secretary, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy.

COMMITTEE CONSIDERATION

The Committee met on July 26, 2017, to consider H.R. 3359, and ordered the measure to be reported to the House with a favorable recommendation, without amendment, by voice vote.

COMMITTEE VOTES

Clause 3(b) of Rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 3359.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of Rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of Rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act of 2017, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, September 5, 2017.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act of 2017.

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

Sincerely,

KEITH HALL,
Director.

Enclosure.

H.R. 3359—Cybersecurity and Infrastructure Security Agency Act of 2017

H.R. 3359 would rename the National Protection and Programs Directorate (NPPD) of the Department of Homeland Security (DHS) as the Cybersecurity and Infrastructure Security Agency. The bill also would consolidate certain missions of NPPD under two divisions: the Cybersecurity Division and the Infrastructure Security Division. Based on information from DHS, CBO has concluded that the requirements in the bill would not impose any new operating requirements on the agency. On that basis, CBO estimates that implementing H.R. 3359 would have a negligible effect on the federal budget.

Enacting H.R. 3359 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

CBO estimates that enacting H.R. 3359 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2028.

H.R. 3359 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would impose no costs on state, local, or tribal governments.

The CBO staff contact for this estimate is William Ma. The estimate was approved by Theresa Gullo, Assistant Director for Budget Analysis.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 3359 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

H.R. 3359 requires the Director of the Cybersecurity and Infrastructure Security Agency to provide Congress with information on the mechanisms for regular consultation and collaboration, including information on compositions, authorities, frequency of meetings, and visibility within the Agency within 90 days of enactment. This Act also requires the Director of the Cybersecurity and Infrastructure Security Agency to submit to Congress a report detailing how the Agency is meeting legislative requirements under the Cybersecurity Workforce Assessment Act and the Homeland Security Cybersecurity Workforce Assessment Act to address cyber work force needs not later than 90 days after the date of the enactment. Also, this Act requires the Director of the Cybersecurity and Infrastructure Security Agency, not later than 180 days after the date of the enactment of this Act, to report to Congress on the most efficient and effective methods of consolidating Agency facilities, personnel, and programs to most effectively carry out the Agency's mission.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 21626 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of the rule XXI.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

PREEMPTION CLARIFICATION

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 3359 does not preempt any State, local, or Tribal law.

DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 3359 would require no directed rule makings.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section provides that this bill may be cited as the "Cybersecurity and Infrastructure Security Agency Act of 2017".

Sec. 2. Cybersecurity and Infrastructure Security Agency

Section 2(a) amends the Homeland Security Act of 2002 by adding title 22, Cybersecurity and Infrastructure Security Agency, at the end. This includes creating the following new sections in the Homeland Security Act:

Section 2201 defines terms used in this subtitle including: "critical infrastructure information"; "critical infrastructure risk"; "cybersecurity risk"; "cybersecurity threat"; "Federal entity"; "non-Federal entity"; "sharing"; and "national cybersecurity asset response activities".

Section 2202 redesignates the National Protection and Programs Directorate of the Department as the 'Cybersecurity and Infrastructure Security Agency' and updates all current legal references accordingly. This section names the head of the Agency as Director and updates all current legal references accordingly. The Committee intends to strengthen the current efforts of NPPD by redesignating the Directorate to a standalone operational agency. These actions will provide the codification of essential existing activities and provide a vehicle for robust congressional oversight.

Section 2202 establishes the responsibilities of the Director, including: leading cybersecurity and critical infrastructure security programs, operations, and associated policy for the Agency; coordinating with Federal and non-Federal entities, including international entities to carry out the cybersecurity and critical infrastructure security activities of the Agency; carrying out the Sec-

retary's responsibilities to secure Federal information and information systems; maintaining and utilizing mechanisms for the regular and ongoing consultation and collaboration among the Agency's Divisions; carrying out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement; and developing, coordinating, and implementing comprehensive strategic plans and risk assessments.

The Committee intends to ensure the mechanisms for regular and ongoing consultation and collaboration are used to further operational coordination of the Agency, integrated situational awareness of the Agency and improved integration across the Agency.

The Committee also intends for experts with programmatic and operational expertise in cybersecurity conduct cybersecurity stakeholder outreach and engagement, experts with programmatic and operational expertise in infrastructure security to conduct infrastructure security stakeholder outreach and engagement and experts with programmatic and operational expertise in emergency communications to conduct emergency communications stakeholder outreach and engagement in order to maintain and strengthen relationships with stakeholders.

Section 2202 establishes a Deputy Director of Cybersecurity and Infrastructure Security to assist the Director in the management of the Agency who shall report to the Director.

Section 2202 includes the cybersecurity and infrastructure security authorities of the Secretary (including those currently authorized in section 201 of the Homeland Security Act for infrastructure protection), including: accessing, receiving and analyzing law enforcement and intelligence information to integrate such information in support of the mission of the Department; developing a comprehensive national plan for securing key resources and critical infrastructure of the United States; and carrying out the functions of the National Cybersecurity and Communications Integration Center and the requirements of the Chemical Facilities Anti-Terrorism Standards program. This section allows the Secretary to modify the functions of the Assistant Directors of Cybersecurity and Infrastructure Security, upon certifying to Congress 60 days prior to such modification, that such modification is necessary for carrying out the activities of the Agency. This section allows the Secretary to provide the Agency with a staff of analysts with appropriate expertise and experience. This section allows the Secretary to detail personnel to the Agency for the performance of analytic functions and related duties.

Section 2202 establishes the composition of the Agency to include the following Divisions, each headed by an Assistant Director: the Cybersecurity Division, the Infrastructure Security Division, and the Emergency Communications Division under title XVIII.

Section 2202 requires the Director to examine, to the maximum extent practicable, the establishment of central locations in geographical regions with significant Agency presence.

Section 2202 authorizes a Privacy Officer for the Agency, with responsibilities that include assuring that the use of technologies sustains privacy protections and that personal information is handled in full compliance with the fair information practices specified in the Privacy Act of 1974. The Committee expects the Privacy Officer

for the Agency to, in the course of their responsibilities, coordinate activities with the Chief Privacy Officer of the Department.

Section 2202 ensures nothing in this title may be construed as affecting the authority, existing the day before enactment of this title, of any other component of the Department or any other Federal department or agency.

Section 2203 establishes the Cybersecurity Division headed by an Assistant Director for Cybersecurity who is equivalent to an Assistant Secretary within the Department and will report to the Director. This section identifies the functions of the Assistant Director for the Cybersecurity Division, including: directing the cybersecurity efforts of the Agency; carrying out the Department's activities related to the security of information and information systems for Federal entities, consistent with law; fully participating in the coordinating and collaboration mechanisms required in section 2202; and carrying out such other duties and powers as prescribed by the Director.

Section 2204 establishes the Infrastructure Security Division headed by an Assistant Director who is equivalent to an Assistant Secretary within the Department and will report to the Director. This section identifies the functions of the Assistant Director for the Infrastructure Security Division to include: directing the critical infrastructure security efforts of the Agency; carrying out the efforts of the Department to secure the United States' high-risk chemical facilities, including the Chemical Facilities Anti-Terrorism Standards established under title XXI; fully participating in the coordinating and collaboration mechanisms required in section 2202; and carrying out such other duties and powers as prescribed by the Director.

Section 2(b) and (c) realign current positions in the Department for the Agency.

Section 2(d) requires the Director to provide Congress with information on the mechanisms for regular consultation and collaboration within the Agency in 90 days. The Director must also provide Congress information on the activities of the Agency's consultation and collaboration mechanisms and how such mechanisms have impacted operational coordination, situational awareness, and integration across the Agency within 1 year.

The Committee intends to require extensive coordination and collaboration efforts across the Agency. The cybersecurity, infrastructure security, and emergency communications missions of the Agency are inextricably linked. The Director must ensure no single division is operating without consideration of the other divisions' goals. Establishing and implementing mechanisms for regular consultation and coordination is essential for the Agency to strengthen its efforts and activities.

Section 2(e) requires the Director to submit to Congress a report detailing how the Agency is meeting legislative requirements under current law to address cyber work force needs not later than 90 days after the date of the enactment.

Section 2(f) requires the Director, not later than 180 days after the date of the enactment of this Act, to report to Congress on the most efficient and effective methods of consolidating Agency facilities, personnel, and programs to most effectively carry out the Agency's mission.

Section 2(g) includes conforming amendments to redesignate current functions and authorities of the Department to the Cybersecurity and Infrastructure Security Agency.

Sec. 3. Transfer of other entities

This section transfers the Office of Biometric Identity Management to the Management Directorate of the Department. This section also authorizes the Secretary of Homeland Security to transfer the Federal Protective Service to any component, directorate, or other office at DHS.

Sec. 4. Rule of construction

This section ensures nothing in this Act may be construed: to confer new authorities to the Secretary of Homeland Security, including programmatic and regulatory authorities, outside of the authorities that existed on the day before the date of the enactment of this Act; to reduce or limit the programmatic, regulatory, or enforcement authority vested in any other Federal agency by statute; or affect in any manner the authority, existing the day before enactment of the Act, of any other Federal agency or component of the Department.

Sec. 5. Prohibition on additional funding

This section States that no additional funds are authorized to be appropriated to carry out this Act or the amendments made by this Act. This Act and such amendment shall be carried out using amounts otherwise authorized.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black 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

SECTION 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:

* * * * * * *

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].

* * * * * * *

[Sec. 210E. National Asset Database.]

* * * * * * *

* * * * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

SEC. 103. OTHER OFFICERS.

(a) DEPUTY SECRETARY; UNDER SECRETARIES.—

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

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

(B) An Under Secretary for Science and Technology.

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

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

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

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

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

[(H) 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.

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

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

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

(b) INSPECTOR GENERAL.—There shall be in the Department an Office of Inspector General and an Inspector General at the head of such office, as provided in the Inspector General Act of 1978 (5 U.S.C. App.).

(c) COMMANDANT OF THE COAST GUARD.—To assist the Secretary in the performance of the Secretary's functions, there is a Commandant of the Coast Guard, who shall be appointed as provided in section 44 of title 14, United States Code, and who shall report directly to the Secretary. In addition to such duties as may be provided in this Act and as assigned to the Commandant by the Secretary, the duties of the Commandant shall include those required by section 2 of title 14, United States Code.

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

(1) A Director of the Secret Service.

(2) A Chief Information Officer.

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

(4) A Director for Domestic Nuclear Detection.

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

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

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

(g) VACANCIES.—

(1) ABSENCE, DISABILITY, OR VACANCY OF SECRETARY OR DEPUTY SECRETARY.—Notwithstanding chapter 33 of title 5, United States Code, the Under Secretary for Management shall serve as the Acting Secretary if by reason of absence, disability, or vacancy in office, neither the Secretary nor Deputy Secretary is available to exercise the duties of the Office of the Secretary.

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

(3) NOTIFICATION OF VACANCIES.—The Secretary shall notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of any vacancies that require notification under sections 3345 through 3349d of title 5, United States Code (commonly known as the "Federal Vacancies Reform Act of 1998").

* * * * * * *

TITLE II—INFORMATION ANALYSIS [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 INTELLIGENCE AND ANALYSIS [AND ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION].—

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

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

[(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) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information, in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 (50 U.S.C. 404o), in order to—

(A) identify and assess the nature and scope of terrorist threats to the homeland;

(B) detect and identify threats of terrorism against the United States; and

(C) understand such threats in light of actual and potential vulnerabilities of the homeland.

(2) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

(3) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether such information, analysis or assessments are provided by or produced by the Department) in order to—

(A) identify priorities for protective and support measures regarding terrorist and other threats to homeland security by the Department, other agencies of the Federal Government, State, and local government agencies and authorities, the private sector, and other entities; and

(B) prepare finished intelligence and information products in both classified and unclassified formats, as appropriate, whenever reasonably expected to be of benefit to a State, local, or tribal government (including a State, local, or tribal law enforcement agency) or a private sector entity.

(4) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such information from other agencies of the Federal Government.

[(5) To 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 relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

[(9)] *(7)* To consult with the Director of National Intelligence and other appropriate intelligence, law enforcement, or other elements of the Federal Government to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism against the United States through such means as the representation of the Department in discussions regarding requirements and priorities in the collection of such information.

[(10)] *(8)* To consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

[(11)] *(9)* To ensure that—

(A) any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties; and

(B) any intelligence information under this Act is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods under the National Security Act of 1947 (50 U.S.C. 401 et seq.) and related procedures and, as appropriate, similar authorities of the Attorney General concerning sensitive law enforcement information.

[(12)] *(10)* To request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

[(13)] *(11)* To establish and utilize, in conjunction with the chief information officer of the Department, a secure commu-

nications 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.

[(14)] *(12)* To ensure, in conjunction with the chief information officer of the Department, that any information databases and analytical tools developed or utilized by the Department—

(A) are compatible with one another and with relevant information databases of other agencies of the Federal Government; and

(B) treat information in such databases in a manner that complies with applicable Federal law on privacy.

[(15)] *(13)* To coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

[(16)] *(14)* To coordinate with elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.

[(17)] *(15)* To provide intelligence and information analysis and support to other elements of the Department.

[(18)] *(16)* To coordinate and enhance integration among the intelligence components of the Department, including through strategic oversight of the intelligence activities of such components.

[(19)] *(17)* To establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department, consistent with any directions from the President and, as applicable, the Director of National Intelligence.

[(20)] *(18)* To establish a structure and process to support the missions and goals of the intelligence components of the Department.

[(21)] *(19)* To ensure that, whenever possible, the Department—

(A) produces and disseminates unclassified reports and analytic products based on open-source information; and

(B) produces and disseminates such reports and analytic products contemporaneously with reports or analytic products concerning the same or similar information that the Department produced and disseminated in a classified format.

[(22)] *(20)* To establish within the Office of Intelligence and Analysis an internal continuity of operations plan.

[(23)] *(21)* Based on intelligence priorities set by the President, and guidance from the Secretary and, as appropriate, the Director of National Intelligence—

(A) to provide to the heads of each intelligence component of the Department guidance for developing the budget pertaining to the activities of such component; and

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

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

[(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) Not later than six months after the date of the enactment of this paragraph, to conduct an intelligence-based review and comparison of the risks and consequences of EMP and GMD facing critical infrastructure, and submit to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate—

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

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

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

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

(ii) be developed in consultation with the relevant Federal sector-specific agencies (as defined under Presidential Policy Directive-21) for critical infrastructure;

(iii) be developed in consultation with the relevant sector coordinating councils for critical infrastructure;

(iv) be informed, to the extent practicable, by the findings of the intelligence-based review and compari-

son of the risks and consequences of EMP and GMD facing critical infrastructure conducted under subparagraph (A); and

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

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

(e) STAFF.—

(1) IN GENERAL.—The Secretary shall provide the Office of Intelligence and Analysis [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.

(2) PRIVATE SECTOR ANALYSTS.—Analysts under this subsection may include analysts from the private sector.

(3) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(f) DETAIL OF PERSONNEL.—

(1) IN GENERAL.—In order to assist the Office of Intelligence and Analysis [and the Office of Infrastructure Protection] in discharging responsibilities under this section, personnel of the agencies referred to in paragraph (2) may be detailed to the Department for the performance of analytic functions and related duties.

(2) COVERED AGENCIES.—The agencies referred to in this paragraph are as follows:

(A) The Department of State.

(B) The Central Intelligence Agency.

(C) The Federal Bureau of Investigation.

(D) The National Security Agency.

(E) The National Geospatial-Intelligence Agency.

(F) The Defense Intelligence Agency.

(G) Any other agency of the Federal Government that the President considers appropriate.

(3) COOPERATIVE AGREEMENTS.—The Secretary and the head of the agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

(4) BASIS.—The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

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

(1) The National Infrastructure Protection Center of the Federal Bureau of Investigation (other than the Computer Investigations and Operations Section), including the functions of the Attorney General relating thereto.

(2) The National Communications System of the Department of Defense, including the functions of the Secretary of Defense relating thereto.

(3) The Critical Infrastructure Assurance Office of the Department of Commerce, including the functions of the Secretary of Commerce relating thereto.

(4) The National Infrastructure Simulation and Analysis Center of the Department of Energy and the energy security and assurance program and activities of the Department, including the functions of the Secretary of Energy relating thereto.

(5) The Federal Computer Incident Response Center of the General Services Administration, including the functions of the Administrator of General Services relating thereto.

* * * * * * *

SEC. 204. HOMELAND SECURITY INFORMATION SHARING.

(a) INFORMATION SHARING.—Consistent with section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), the Secretary, acting through the Under Secretary for Intelligence and Analysis, shall integrate the information and standardize the format of the products of the intelligence components of the Department containing homeland security information, terrorism information, weapons of mass destruction information, or national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))) except for any internal security protocols or personnel information of such intelligence components, or other administrative processes that are administered by any chief security officer of the Department.

(b) INFORMATION SHARING AND KNOWLEDGE MANAGEMENT OFFICERS.—For each intelligence component of the Department, the Secretary shall designate an information sharing and knowledge management officer who shall report to the Under Secretary for Intelligence and Analysis regarding coordinating the different systems used in the Department to gather and disseminate homeland security information or national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))).

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

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

(A) establish Department-wide procedures for the review and analysis of information provided by State, local, and tribal governments and the private sector;

(B) as appropriate, integrate such information into the information gathered by the Department and other departments and agencies of the Federal Government; and

(C) make available such information, as appropriate, within the Department and to other departments and agencies of the Federal Government.

(2) FEEDBACK.—The Secretary shall develop mechanisms to provide feedback regarding the analysis and utility of informa-

tion provided by any entity of State, local, or tribal government or the private sector that provides such information to the Department.

(d) TRAINING AND EVALUATION OF EMPLOYEES.—

(1) TRAINING.—The Secretary, acting through the Under Secretary for Intelligence and Analysis or the [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—

(A) the definitions of homeland security information and national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))); and

(B) how information available to such employees as part of their duties—

(i) might qualify as homeland security information or national intelligence; and

(ii) might be relevant to the Office of Intelligence and Analysis and the intelligence components of the Department.

(2) EVALUATIONS.—The Under Secretary for Intelligence and Analysis shall—

(A) on an ongoing basis, evaluate how employees of the Office of Intelligence and Analysis and the intelligence components of the Department are utilizing homeland security information or national intelligence, sharing information within the Department, as described in this title, and participating in the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485); and

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

* * * * * * *

SEC. 210A. DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL, AND REGIONAL FUSION CENTER INITIATIVE.

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

(b) DEPARTMENT SUPPORT AND COORDINATION.—Through the Department of Homeland Security State, Local, and Regional Fusion Center Initiative, and in coordination with the principal officials of participating State, local, or regional fusion centers and the officers designated as the Homeland Security Advisors of the States, the Secretary shall—

(1) provide operational and intelligence advice and assistance to State, local, and regional fusion centers;

(2) support efforts to include State, local, and regional fusion centers into efforts to establish an information sharing environment;

(3) conduct tabletop and live training exercises to regularly assess the capability of individual and regional networks of State, local, and regional fusion centers to integrate the efforts of such networks with the efforts of the Department;

(4) coordinate with other relevant Federal entities engaged in homeland security-related activities;

(5) provide analytic and reporting advice and assistance to State, local, and regional fusion centers;

(6) review information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is gathered by State, local, and regional fusion centers, and to incorporate such information, as appropriate, into the Department's own such information;

(7) provide management assistance to State, local, and regional fusion centers;

(8) serve as a point of contact to ensure the dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(9) facilitate close communication and coordination between State, local, and regional fusion centers and the Department;

(10) provide State, local, and regional fusion centers with expertise on Department resources and operations;

(11) provide training to State, local, and regional fusion centers and encourage such fusion centers to participate in terrorism threat-related exercises conducted by the Department; and

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

(c) PERSONNEL ASSIGNMENT.—

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

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

(A) Office of Intelligence and Analysis.

(B) [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.

(3) QUALIFYING CRITERIA.—

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

(B) CRITERIA.—Any criteria developed under subparagraph (A) may include—

(i) whether the fusion center, through its mission and governance structure, focuses on a broad counterterrorism approach, and whether that broad approach is pervasive through all levels of the organization;

(ii) whether the fusion center has sufficient numbers of adequately trained personnel to support a broad counterterrorism mission;

(iii) whether the fusion center has—

(I) access to relevant law enforcement, emergency response, private sector, open source, and national security data; and

(II) the ability to share and analytically utilize that data for lawful purposes;

(iv) whether the fusion center is adequately funded by the State, local, or regional government to support its counterterrorism mission; and

(v) the relevancy of the mission of the fusion center to the particular source component of Department officers or intelligence analysts.

(4) PREREQUISITE.—

(A) INTELLIGENCE ANALYSIS, PRIVACY, AND CIVIL LIBERTIES TRAINING.—Before being assigned to a fusion center under this section, an officer or intelligence analyst shall undergo—

(i) appropriate intelligence analysis or information sharing training using an intelligence-led policing curriculum that is consistent with—

(I) standard training and education programs offered to Department law enforcement and intelligence personnel; and

(II) the Criminal Intelligence Systems Operating Policies under part 23 of title 28, Code of Federal Regulations (or any corresponding similar rule or regulation);

(ii) appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer appointed under section 222 and the Officer for Civil Rights and Civil Liberties of the Department, in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note); and

(iii) such other training prescribed by the Under Secretary for Intelligence and Analysis.

(B) PRIOR WORK EXPERIENCE IN AREA.—In determining the eligibility of an officer or intelligence analyst to be assigned to a fusion center under this section, the Under Secretary for Intelligence and Analysis shall consider the familiarity of the officer or intelligence analyst with the

State, locality, or region, as determined by such factors as whether the officer or intelligence analyst—

(i) has been previously assigned in the geographic area; or

(ii) has previously worked with intelligence officials or law enforcement or other emergency response providers from that State, locality, or region.

(5) EXPEDITED SECURITY CLEARANCE PROCESSING.—The Under Secretary for Intelligence and Analysis—

(A) shall ensure that each officer or intelligence analyst assigned to a fusion center under this section has the appropriate security clearance to contribute effectively to the mission of the fusion center; and

(B) may request that security clearance processing be expedited for each such officer or intelligence analyst and may use available funds for such purpose.

(6) FURTHER QUALIFICATIONS.—Each officer or intelligence analyst assigned to a fusion center under this section shall satisfy any other qualifications the Under Secretary for Intelligence and Analysis may prescribe.

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

(1) assist law enforcement agencies and other emergency response providers of State, local, and tribal governments and fusion center personnel in using information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to develop a comprehensive and accurate threat picture;

(2) review homeland security-relevant information from law enforcement agencies and other emergency response providers of State, local, and tribal government;

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

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

(e) BORDER INTELLIGENCE PRIORITY.—

(1) IN GENERAL.—The Secretary shall make it a priority to assign officers and intelligence analysts under this section from United States Customs and Border Protection, United States Immigration and Customs Enforcement, and the Coast Guard to participating State, local, and regional fusion centers located in jurisdictions along land or maritime borders of the United States in order to enhance the integrity of and security at such borders by helping Federal, State, local, and tribal law enforcement authorities to identify, investigate, and otherwise interdict persons, weapons, and related contraband that pose a threat to homeland security.

(2) BORDER INTELLIGENCE PRODUCTS.—When performing the responsibilities described in subsection (d), officers and intelligence analysts assigned to participating State, local, and re-

gional fusion centers under this section shall have, as a primary responsibility, the creation of border intelligence products that—

(A) assist State, local, and tribal law enforcement agencies in deploying their resources most efficiently to help detect and interdict terrorists, weapons of mass destruction, and related contraband at land or maritime borders of the United States;

(B) promote more consistent and timely sharing of border security-relevant information among jurisdictions along land or maritime borders of the United States; and

(C) enhance the Department's situational awareness of the threat of acts of terrorism at or involving the land or maritime borders of the United States.

(f) DATABASE ACCESS.—In order to fulfill the objectives described under subsection (d), each officer or intelligence analyst assigned to a fusion center under this section shall have appropriate access to all relevant Federal databases and information systems, consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment for the implementation and management of that environment.

(g) CONSUMER FEEDBACK.—

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

(2) REPORT.—Not later than one year after the date of the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that includes a description of the consumer feedback obtained under paragraph (1) and, if applicable, how the Department has adjusted its production of intelligence products in response to that consumer feedback.

(h) RULE OF CONSTRUCTION.—

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

(2) PARTICIPATION.—Nothing in this section shall be construed to require a State, local, or regional government or entity to accept the assignment of officers or intelligence analysts of the Department into the fusion center of that State, locality, or region.

(i) GUIDELINES.—The Secretary, in consultation with the Attorney General, shall establish guidelines for fusion centers created and operated by State and local governments, to include standards that any such fusion center shall—

(1) collaboratively develop a mission statement, identify expectations and goals, measure performance, and determine effectiveness for that fusion center;

(2) create a representative governance structure that includes law enforcement officers and other emergency response providers and, as appropriate, the private sector;

(3) create a collaborative environment for the sharing of intelligence and information among Federal, State, local, and tribal government agencies (including law enforcement officers and other emergency response providers), the private sector, and the public, consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment;

(4) leverage the databases, systems, and networks available from public and private sector entities, in accordance with all applicable laws, to maximize information sharing;

(5) develop, publish, and adhere to a privacy and civil liberties policy consistent with Federal, State, and local law;

(6) provide, in coordination with the Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department, appropriate privacy and civil liberties training for all State, local, tribal, and private sector representatives at the fusion center;

(7) ensure appropriate security measures are in place for the facility, data, and personnel;

(8) select and train personnel based on the needs, mission, goals, and functions of that fusion center;

(9) offer a variety of intelligence and information services and products to recipients of fusion center intelligence and information; and

(10) incorporate law enforcement officers, other emergency response providers, and, as appropriate, the private sector, into all relevant phases of the intelligence and fusion process, consistent with the mission statement developed under paragraph (1), either through full time representatives or liaison relationships with the fusion center to enable the receipt and sharing of information and intelligence.

(j) DEFINITIONS.—In this section—

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

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

(3) the term "intelligence analyst" means an individual who regularly advises, administers, supervises, or performs work in the collection, gathering, analysis, evaluation, reporting, production, or dissemination of information on political, economic, social, cultural, physical, geographical, scientific, or military

conditions, trends, or forces in foreign or domestic areas that directly or indirectly affect national security;

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

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

(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.

* * * * * * *

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 Secretary for Science and Technology, shall have the responsibility for—

(1) advising the Secretary regarding research and development efforts and priorities in support of the Department's missions;

(2) developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for, identifying priorities, goals, objectives and policies for, and coordinating the Federal Government's civilian efforts to identify and develop countermeasures to chemical, biological,, and other emerging terrorist threats, including the development of comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts;

(3) supporting the Under Secretary for Intelligence and Analysis and the ⟦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 activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, except that such responsibility does not extend to human health-related research and development activities;

(5) establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for—

(A) preventing the importation of chemical, biological,, and related weapons and material; and

(B) detecting, preventing, protecting against, and responding to terrorist attacks;

(6) establishing a system for transferring homeland security developments or technologies to Federal, State, local government, and private sector entities;

(7) entering into work agreements, joint sponsorships, contracts, or any other agreements with the Department of Energy regarding the use of the national laboratories or sites and support of the science and technology base at those facilities;

(8) collaborating with the Secretary of Agriculture and the Attorney General as provided in section 212 of the Agricultural Bioterrorism Protection Act of 2002 (7 U.S.C. 8401), as amended by section 1709(b);

(9) collaborating with the Secretary of Health and Human Services and the Attorney General in determining any new biological agents and toxins that shall be listed as "select agents" in Appendix A of part 72 of title 42, Code of Federal Regulations, pursuant to section 351A of the Public Health Service Act (42 U.S.C. 262a);

(10) supporting United States leadership in science and technology;

(11) establishing and administering the primary research and development activities of the Department, including the long-term research and development needs and capabilities for all elements of the Department;

(12) coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department;

(13) coordinating with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs; and

(14) developing and overseeing the administration of guidelines for merit review of research and development projects throughout the Department, and for the dissemination of research conducted or sponsored by the Department.

* * * * * * *

TITLE V—NATIONAL EMERGENCY MANAGEMENT

* * * * * * *

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. 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 the Cybersecurity and Infrastructure Security Agency*, in consultation with the private sector, may develop guidance or recommendations and identify best practices to assist or foster action by the private sector in—

(1) identifying potential hazards and assessing risks and impacts;

(2) mitigating the impact of a wide variety of hazards, including weapons of mass destruction;

(3) managing necessary emergency preparedness and response resources;

(4) developing mutual aid agreements;

(5) developing and maintaining emergency preparedness and response plans, and associated operational procedures;

(6) developing and conducting training and exercises to support and evaluate emergency preparedness and response plans and operational procedures;

(7) developing and conducting training programs for security guards to implement emergency preparedness and response plans and operations procedures; and

(8) developing procedures to respond to requests for information from the media or the public.

(b) ISSUANCE AND PROMOTION.—Any guidance or recommendations developed or best practices identified under subsection (a) shall be—

(1) issued through the Administrator; and

(2) promoted by the Secretary to the private sector.

(c) SMALL BUSINESS CONCERNS.—In developing guidance or recommendations or identifying best practices under subsection (a), the Administrator and the [Assistant Secretary for Infrastructure Protection] *Director of the Cybersecurity and Infrastructure Security Agency* shall take into consideration small business concerns (under the meaning given that term in section 3 of the Small Business Act (15 U.S.C. 632)), including any need for separate guidance or recommendations or best practices, as necessary and appropriate.

(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed to supersede any requirement established under any other provision of law.

SEC. 524. VOLUNTARY PRIVATE SECTOR PREPAREDNESS ACCREDITATION AND CERTIFICATION PROGRAM.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Secretary, acting through the officer designated under paragraph (2), shall establish and implement the voluntary private sector preparedness accreditation and certification program in accordance with this section.

(2) DESIGNATION OF OFFICER.—The Secretary shall designate an officer responsible for the accreditation and certification program under this section. Such officer (hereinafter referred to in this section as the "designated officer") shall be one of the following:

(A) The Administrator, based on consideration of—

(i) the expertise of the Administrator in emergency management and preparedness in the United States; and

(ii) the responsibilities of the Administrator as the principal advisor to the President for all matters relating to emergency management in the United States.

(B) The [Assistant Secretary for Infrastructure Protection] *Director of the Cybersecurity and Infrastructure Security Agency*, based on consideration of the expertise [of the Assistant Secretary] *of the Director* in, and responsibilities for—

(i) protection of critical infrastructure;

(ii) risk assessment methodologies; and

(iii) interacting with the private sector on the issues described in clauses (i) and (ii).

(C) The Under Secretary for Science and Technology, based on consideration of the expertise of the Under Secretary in, and responsibilities associated with, standards.

(3) COORDINATION.—In carrying out the accreditation and certification program under this section, the designated officer shall coordinate with—

(A) the other officers of the Department referred to in paragraph (2), using the expertise and responsibilities of such officers; and

(B) the Special Assistant to the Secretary for the Private Sector, based on consideration of the expertise of the Special Assistant in, and responsibilities for, interacting with the private sector.

(b) VOLUNTARY PRIVATE SECTOR PREPAREDNESS STANDARDS; VOLUNTARY ACCREDITATION AND CERTIFICATION PROGRAM FOR THE PRIVATE SECTOR.—

(1) ACCREDITATION AND CERTIFICATION PROGRAM.—Not later than 210 days after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the designated officer shall—

(A) begin supporting the development and updating, as necessary, of voluntary preparedness standards through appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards and voluntary consensus standards development organizations; and

(B) in consultation with representatives of appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards, appropriate voluntary consensus standards development organizations, each private sector advisory council created under section 102(f)(4), appropriate representatives of State and local governments, including emergency management officials, and appropriate private sector advisory groups, such as

sector coordinating councils and information sharing and analysis centers—

(i) develop and promote a program to certify the preparedness of private sector entities that voluntarily choose to seek certification under the program; and

(ii) implement the program under this subsection through any entity with which the designated officer enters into an agreement under paragraph (3)(A), which shall accredit third parties to carry out the certification process under this section.

(2) PROGRAM ELEMENTS.—

(A) IN GENERAL.—

(i) PROGRAM.—The program developed and implemented under this subsection shall assess whether a private sector entity complies with voluntary preparedness standards.

(ii) GUIDELINES.—In developing the program under this subsection, the designated officer shall develop guidelines for the accreditation and certification processes established under this subsection.

(B) STANDARDS.—The designated officer, in consultation with representatives of appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards, representatives of appropriate voluntary consensus standards development organizations, each private sector advisory council created under section 102(f)(4), appropriate representatives of State and local governments, including emergency management officials, and appropriate private sector advisory groups such as sector coordinating councils and information sharing and analysis centers—

(i) shall adopt one or more appropriate voluntary preparedness standards that promote preparedness, which may be tailored to address the unique nature of various sectors within the private sector, as necessary and appropriate, that shall be used in the accreditation and certification program under this subsection; and

(ii) after the adoption of one or more standards under clause (i), may adopt additional voluntary preparedness standards or modify or discontinue the use of voluntary preparedness standards for the accreditation and certification program, as necessary and appropriate to promote preparedness.

(C) SUBMISSION OF RECOMMENDATIONS.—In adopting one or more standards under subparagraph (B), the designated officer may receive recommendations from any entity described in that subparagraph relating to appropriate voluntary preparedness standards, including appropriate sector specific standards, for adoption in the program.

(D) SMALL BUSINESS CONCERNS.—The designated officer and any entity with which the designated officer enters into an agreement under paragraph (3)(A) shall establish separate classifications and methods of certification for small business concerns (under the meaning given that

term in section 3 of the Small Business Act (15 U.S.C. 632)) for the program under this subsection.

(E) CONSIDERATIONS.—In developing and implementing the program under this subsection, the designated officer shall—

(i) consider the unique nature of various sectors within the private sector, including preparedness standards, business continuity standards, or best practices, established—

(I) under any other provision of Federal law; or

(II) by any sector-specific agency, as defined under Homeland Security Presidential Directive–7; and

(ii) coordinate the program, as appropriate, with—

(I) other Department private sector related programs; and

(II) preparedness and business continuity programs in other Federal agencies.

(3) ACCREDITATION AND CERTIFICATION PROCESSES.—

(A) AGREEMENT.—

(i) IN GENERAL.—Not later than 210 days after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the designated officer shall enter into one or more agreements with a highly qualified nongovernmental entity with experience or expertise in coordinating and facilitating the development and use of voluntary consensus standards and in managing or implementing accreditation and certification programs for voluntary consensus standards, or a similarly qualified private sector entity, to carry out accreditations and oversee the certification process under this subsection. An entity entering into an agreement with the designated officer under this clause (hereinafter referred to in this section as a "selected entity") shall not perform certifications under this subsection.

(ii) CONTENTS.—A selected entity shall manage the accreditation process and oversee the certification process in accordance with the program established under this subsection and accredit qualified third parties to carry out the certification program established under this subsection.

(B) PROCEDURES AND REQUIREMENTS FOR ACCREDITATION AND CERTIFICATION.—

(i) IN GENERAL.—Any selected entity shall collaborate to develop procedures and requirements for the accreditation and certification processes under this subsection, in accordance with the program established under this subsection and guidelines developed under paragraph (2)(A)(ii).

(ii) CONTENTS AND USE.—The procedures and requirements developed under clause (i) shall—

(I) ensure reasonable uniformity in any accreditation and certification processes if there is more than one selected entity; and

(II) be used by any selected entity in conducting accreditations and overseeing the certification process under this subsection.

(iii) DISAGREEMENT.—Any disagreement among selected entities in developing procedures under clause (i) shall be resolved by the designated officer.

(C) DESIGNATION.—A selected entity may accredit any qualified third party to carry out the certification process under this subsection.

(D) DISADVANTAGED BUSINESS INVOLVEMENT.—In accrediting qualified third parties to carry out the certification process under this subsection, a selected entity shall ensure, to the extent practicable, that the third parties include qualified small, minority, women-owned, or disadvantaged business concerns when appropriate. The term "disadvantaged business concern" means a small business that is owned and controlled by socially and economically disadvantaged individuals, as defined in section 124 of title 13, United States Code of Federal Regulations.

(E) TREATMENT OF OTHER CERTIFICATIONS.—At the request of any entity seeking certification, any selected entity may consider, as appropriate, other relevant certifications acquired by the entity seeking certification. If the selected entity determines that such other certifications are sufficient to meet the certification requirement or aspects of the certification requirement under this section, the selected entity may give credit to the entity seeking certification, as appropriate, to avoid unnecessarily duplicative certification requirements.

(F) THIRD PARTIES.—To be accredited under subparagraph (C), a third party shall—

(i) demonstrate that the third party has the ability to certify private sector entities in accordance with the procedures and requirements developed under subparagraph (B);

(ii) agree to perform certifications in accordance with such procedures and requirements;

(iii) agree not to have any beneficial interest in or any direct or indirect control over—

(I) a private sector entity for which that third party conducts a certification under this subsection; or

(II) any organization that provides preparedness consulting services to private sector entities;

(iv) agree not to have any other conflict of interest with respect to any private sector entity for which that third party conducts a certification under this subsection;

(v) maintain liability insurance coverage at policy limits in accordance with the requirements developed under subparagraph (B); and

(vi) enter into an agreement with the selected entity accrediting that third party to protect any proprietary information of a private sector entity obtained under this subsection.

(G) MONITORING.—

(i) IN GENERAL.—The designated officer and any selected entity shall regularly monitor and inspect the operations of any third party conducting certifications under this subsection to ensure that the third party is complying with the procedures and requirements established under subparagraph (B) and all other applicable requirements.

(ii) REVOCATION.—If the designated officer or any selected entity determines that a third party is not meeting the procedures or requirements established under subparagraph (B), the selected entity shall—

(I) revoke the accreditation of that third party to conduct certifications under this subsection; and

(II) review any certification conducted by that third party, as necessary and appropriate.

(4) ANNUAL REVIEW.—

(A) IN GENERAL.—The designated officer, in consultation with representatives of appropriate organizations that coordinate or facilitate the development and use of voluntary consensus standards, appropriate voluntary consensus standards development organizations, appropriate representatives of State and local governments, including emergency management officials, and each private sector advisory council created under section 102(f)(4), shall annually review the voluntary accreditation and certification program established under this subsection to ensure the effectiveness of such program (including the operations and management of such program by any selected entity and the selected entity's inclusion of qualified disadvantaged business concerns under paragraph (3)(D)) and make improvements and adjustments to the program as necessary and appropriate.

(B) REVIEW OF STANDARDS.—Each review under subparagraph (A) shall include an assessment of the voluntary preparedness standard or standards used in the program under this subsection.

(5) VOLUNTARY PARTICIPATION.—Certification under this subsection shall be voluntary for any private sector entity.

(6) PUBLIC LISTING.—The designated officer shall maintain and make public a listing of any private sector entity certified as being in compliance with the program established under this subsection, if that private sector entity consents to such listing.

(c) RULE OF CONSTRUCTION.—Nothing in this section may be construed as—

(1) a requirement to replace any preparedness, emergency response, or business continuity standards, requirements, or best practices established—

(A) under any other provision of federal law; or

(B) by any sector-specific agency, as those agencies are defined under Homeland Security Presidential Directive–7; or

(2) exempting any private sector entity seeking certification or meeting certification requirements under subsection (b) from compliance with all applicable statutes, regulations, directives, policies, and industry codes of practice.

* * * * * * *

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

* * * * * * *

Subtitle J—Secure Handling of Ammonium Nitrate

* * * * * * *

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.*

(b) AMMONIUM NITRATE MIXTURES.—Not later than 90 days after the date of the enactment of this subtitle, the Secretary, in consultation with the heads of appropriate Federal departments and agencies (including the Secretary of Agriculture), shall, after notice and an opportunity for comment, establish a threshold percentage for ammonium nitrate in a substance.

(c) REGISTRATION OF OWNERS OF AMMONIUM NITRATE FACILITIES.—

(1) REGISTRATION.—The Secretary shall establish a process by which any person that—

(A) owns an ammonium nitrate facility is required to register with the Department; and

(B) registers under subparagraph (A) is issued a registration number for purposes of this subtitle.

(2) REGISTRATION INFORMATION.—Any person applying to register under paragraph (1) shall submit to the Secretary—

(A) the name, address, and telephone number of each ammonium nitrate facility owned by that person;

(B) the name of the person designated by that person as the point of contact for each such facility, for purposes of this subtitle; and

(C) such other information as the Secretary may determine is appropriate.

(d) REGISTRATION OF AMMONIUM NITRATE PURCHASERS.—

(1) REGISTRATION.—The Secretary shall establish a process by which any person that—

(A) intends to be an ammonium nitrate purchaser is required to register with the Department; and

(B) registers under subparagraph (A) is issued a registration number for purposes of this subtitle.

(2) REGISTRATION INFORMATION.—Any person applying to register under paragraph (1) as an ammonium nitrate purchaser shall submit to the Secretary—

(A) the name, address, and telephone number of the applicant; and

(B) the intended use of ammonium nitrate to be purchased by the applicant.

(e) RECORDS.—

(1) MAINTENANCE OF RECORDS.—The owner of an ammonium nitrate facility shall—

(A) maintain a record of each sale or transfer of ammonium nitrate, during the two-year period beginning on the date of that sale or transfer; and

(B) include in such record the information described in paragraph (2).

(2) SPECIFIC INFORMATION REQUIRED.—For each sale or transfer of ammonium nitrate, the owner of an ammonium nitrate facility shall—

(A) record the name, address, telephone number, and registration number issued under subsection (c) or (d) of each person that purchases ammonium nitrate, in a manner prescribed by the Secretary;

(B) if applicable, record the name, address, and telephone number of an agent acting on behalf of the person described in subparagraph (A), at the point of sale;

(C) record the date and quantity of ammonium nitrate sold or transferred; and

(D) verify the identity of the persons described in subparagraphs (A) and (B), as applicable, in accordance with a procedure established by the Secretary.

(3) PROTECTION OF INFORMATION.—In maintaining records in accordance with paragraph (1), the owner of an ammonium nitrate facility shall take reasonable actions to ensure the protection of the information included in such records.

(f) EXEMPTION FOR EXPLOSIVE PURPOSES.—The Secretary may exempt from this subtitle a person producing, selling, or purchasing ammonium nitrate exclusively for use in the production of an explosive under a license or permit issued under chapter 40 of title 18, United States Code.

(g) CONSULTATION.—In carrying out this section, the Secretary shall consult with the Secretary of Agriculture, States, and appropriate private sector entities, to ensure that the access of agricultural producers to ammonium nitrate is not unduly burdened.

(h) DATA CONFIDENTIALITY.—

(1) IN GENERAL.—Notwithstanding section 552 of title 5, United States Code, or the USA PATRIOT ACT (Public Law 107–56; 115 Stat. 272), and except as provided in paragraph (2), the Secretary may not disclose to any person any information obtained under this subtitle.

(2) EXCEPTION.—The Secretary may disclose any information obtained by the Secretary under this subtitle to—

(A) an officer or employee of the United States, or a person that has entered into a contract with the United States, who has a need to know the information to perform the duties of the officer, employee, or person; or

(B) to a State agency under section 899D, under appropriate arrangements to ensure the protection of the information.

(i) REGISTRATION PROCEDURES AND CHECK OF TERRORIST SCREENING DATABASE.—

(1) REGISTRATION PROCEDURES.—

(A) GENERALLY.—The Secretary shall establish procedures to efficiently receive applications for registration numbers under this subtitle, conduct the checks required under paragraph (2), and promptly issue or deny a registration number.

(B) INITIAL SIX-MONTH REGISTRATION PERIOD.—The Secretary shall take steps to maximize the number of registration applications that are submitted and processed during the six-month period described in section 899F(e).

(2) CHECK OF TERRORIST SCREENING DATABASE.—

(A) CHECK REQUIRED.—The Secretary shall conduct a check of appropriate identifying information of any person seeking to register with the Department under subsection (c) or (d) against identifying information that appears in the terrorist screening database of the Department.

(B) AUTHORITY TO DENY REGISTRATION NUMBER.—If the identifying information of a person seeking to register with the Department under subsection (c) or (d) appears in the terrorist screening database of the Department, the Secretary may deny issuance of a registration number under this subtitle.

(3) EXPEDITED REVIEW OF APPLICATIONS.—

(A) IN GENERAL.—Following the six-month period described in section 899F(e), the Secretary shall, to the extent practicable, issue or deny registration numbers under this subtitle not later than 72 hours after the time the Secretary receives a complete registration application, unless the Secretary determines, in the interest of national security, that additional time is necessary to review an application.

(B) NOTICE OF APPLICATION STATUS.—In all cases, the Secretary shall notify a person seeking to register with the Department under subsection (c) or (d) of the status of the application of that person not later than 72 hours after the time the Secretary receives a complete registration application.

(4) EXPEDITED APPEALS PROCESS.—

(A) REQUIREMENT.—

(i) APPEALS PROCESS.—The Secretary shall establish an expedited appeals process for persons denied a registration number under this subtitle.

(ii) TIME PERIOD FOR RESOLUTION.—The Secretary shall, to the extent practicable, resolve appeals not

later than 72 hours after receiving a complete request for appeal unless the Secretary determines, in the interest of national security, that additional time is necessary to resolve an appeal.

(B) CONSULTATION.—The Secretary, in developing the appeals process under subparagraph (A), shall consult with appropriate stakeholders.

(C) GUIDANCE.—The Secretary shall provide guidance regarding the procedures and information required for an appeal under subparagraph (A) to any person denied a registration number under this subtitle.

(5) RESTRICTIONS ON USE AND MAINTENANCE OF INFORMATION.—

(A) IN GENERAL.—Any information constituting grounds for denial of a registration number under this section shall be maintained confidentially by the Secretary and may be used only for making determinations under this section.

(B) SHARING OF INFORMATION.—Notwithstanding any other provision of this subtitle, the Secretary may share any such information with Federal, State, local, and tribal law enforcement agencies, as appropriate.

(6) REGISTRATION INFORMATION.—

(A) AUTHORITY TO REQUIRE INFORMATION.—The Secretary may require a person applying for a registration number under this subtitle to submit such information as may be necessary to carry out the requirements of this section.

(B) REQUIREMENT TO UPDATE INFORMATION.—The Secretary may require persons issued a registration under this subtitle to update registration information submitted to the Secretary under this subtitle, as appropriate.

(7) RE-CHECKS AGAINST TERRORIST SCREENING DATABASE.—

(A) RE-CHECKS.—The Secretary shall, as appropriate, recheck persons provided a registration number pursuant to this subtitle against the terrorist screening database of the Department, and may revoke such registration number if the Secretary determines such person may pose a threat to national security.

(B) NOTICE OF REVOCATION.—The Secretary shall, as appropriate, provide prior notice to a person whose registration number is revoked under this section and such person shall have an opportunity to appeal, as provided in paragraph (4).

* * * * * * *

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 *Assistant* Director for Emergency Communications. The Director shall report to the [Assistant Secretary for Cybersecurity and Communications] *Director of the Cybersecurity and Infrastructure Security Agency*.

(c) RESPONSIBILITIES.—The *Assistant* Director for Emergency Communications shall—

(1) assist the Secretary in developing and implementing the program described in section 7303(a)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(a)(1)), except as provided in section 314;

(2) administer the Department's responsibilities and authorities relating to the SAFECOM Program, excluding elements related to research, development, testing, and evaluation and standards;

(3) administer the Department's responsibilities and authorities relating to the Integrated Wireless Network program;

(4) conduct extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other manmade disasters;

(5) conduct extensive, nationwide outreach and foster the development of interoperable emergency communications capabilities by State, regional, local, and tribal governments and public safety agencies, and by regional consortia thereof;

(6) provide technical assistance to State, regional, local, and tribal government officials with respect to use of interoperable emergency communications capabilities;

(7) coordinate with the Regional Administrators regarding the activities of Regional Emergency Communications Coordination Working Groups under section 1805;

(8) promote the development of standard operating procedures and best practices with respect to use of interoperable emergency communications capabilities for incident response, and facilitate the sharing of information on such best practices for achieving, maintaining, and enhancing interoperable emergency communications capabilities for such response;

(9) coordinate, in cooperation with the National Communications System, the establishment of a national response capability with initial and ongoing planning, implementation, and training for the deployment of communications equipment for relevant State, local, and tribal governments and emergency response providers in the event of a catastrophic loss of local and regional emergency communications services;

(10) assist the President, the National Security Council, the Homeland Security Council, and the Director of the Office of Management and Budget in ensuring the continued operation of the telecommunications functions and responsibilities of the Federal Government, excluding spectrum management;

(11) establish, in coordination with the Director of the Office for Interoperability and Compatibility, requirements for interoperable emergency communications capabilities, which shall be nonproprietary where standards for such capabilities exist, for all public safety radio and data communications systems and equipment purchased using homeland security assistance

administered by the Department, excluding any alert and warning device, technology, or system;

(12) review, in consultation with the Assistant Secretary for Grants and Training, all interoperable emergency communications plans of Federal, State, local, and tribal governments, including Statewide and tactical interoperability plans, developed pursuant to homeland security assistance administered by the Department, but excluding spectrum allocation and management related to such plans;

(13) develop and update periodically, as appropriate, a National Emergency Communications Plan under section 1802;

(14) perform such other duties of the Department necessary to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; [and]

(15) fully participate in the mechanisms required under subsection (c)(7) of section 2202; and

[(15)] *(16)* 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) The SAFECOM Program, excluding elements related to research, development, testing, and evaluation and standards.

(2) The responsibilities of the Chief Information Officer related to the implementation of the Integrated Wireless Network.

(3) The Interoperable Communications Technical Assistance Program.

(e) COORDINATION.—The *Assistant* Director for Emergency Communications shall coordinate—

(1) as appropriate, with the Director of the Office for Interoperability and Compatibility with respect to the responsibilities described in section 314; and

(2) with the Administrator of the Federal Emergency Management Agency with respect to the responsibilities described in this title.

(f) SUFFICIENCY OF RESOURCES PLAN.—

(1) REPORT.—Not later than 120 days after the date of enactment of this section, the Secretary shall submit to Congress a report on the resources and staff necessary to carry out fully the responsibilities under this title.

(2) COMPTROLLER GENERAL REVIEW.—The Comptroller General shall review the validity of the report submitted by the Secretary under paragraph (1). Not later than 60 days after the date on which such report is submitted, the Comptroller General shall submit to Congress a report containing the findings of such review.

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 Na-

tional Communications System (as appropriate), shall, in cooperation with State, local, and tribal governments, Federal departments and agencies, emergency response providers, and the private sector, develop not later than 180 days after the completion of the baseline assessment under section 1803, and periodically update, a National Emergency Communications Plan to provide recommendations regarding how the United States should—

(1) support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and

(2) ensure, accelerate, and attain interoperable emergency communications nationwide.

(b) COORDINATION.—The Emergency Communications Preparedness Center under section 1806 shall coordinate the development of the Federal aspects of the National Emergency Communications Plan.

(c) CONTENTS.—The National Emergency Communications Plan shall—

(1) include recommendations developed in consultation with the Federal Communications Commission and the National Institute of Standards and Technology for a process for expediting national voluntary consensus standards for emergency communications equipment for the purchase and use by public safety agencies of interoperable emergency communications equipment and technologies;

(2) identify the appropriate capabilities necessary for emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(3) identify the appropriate interoperable emergency communications capabilities necessary for Federal, State, local, and tribal governments in the event of natural disasters, acts of terrorism, and other man-made disasters;

(4) recommend both short-term and long-term solutions for ensuring that emergency response providers and relevant government officials can continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(5) recommend both short-term and long-term solutions for deploying interoperable emergency communications systems for Federal, State, local, and tribal governments throughout the Nation, including through the provision of existing and emerging technologies;

(6) identify how Federal departments and agencies that respond to natural disasters, acts of terrorism, and other man-made disasters can work effectively with State, local, and tribal governments, in all States, and with other entities;

(7) identify obstacles to deploying interoperable emergency communications capabilities nationwide and recommend short-term and long-term measures to overcome those obstacles, including recommendations for multijurisdictional coordination among Federal, State, local, and tribal governments;

(8) recommend goals and timeframes for the deployment of emergency, command-level communications systems based on

new and existing equipment across the United States and develop a timetable for the deployment of interoperable emergency communications systems nationwide;

(9) recommend appropriate measures that emergency response providers should employ to ensure the continued operation of relevant governmental communications infrastructure in the event of natural disasters, acts of terrorism, or other man-made disasters; and

(10) set a date, including interim benchmarks, as appropriate, by which State, local, and tribal governments, Federal departments and agencies, and emergency response providers expect to achieve a baseline level of national interoperable communications, as that term is defined under section 7303(g)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(g)(1)).

SEC. 1803. 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—

(1) defines the range of capabilities needed by emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;

(2) defines the range of interoperable emergency communications capabilities needed for specific events;

(3) assesses the current available capabilities to meet such communications needs;

(4) identifies the gap between such current capabilities and defined requirements; and

(5) includes a national interoperable emergency communications inventory to be completed by the Secretary of Homeland Security, the Secretary of Commerce, and the Chairman of the Federal Communications Commission that—

(A) identifies for each Federal department and agency—

(i) the channels and frequencies used;

(ii) the nomenclature used to refer to each channel or frequency used; and

(iii) the types of communications systems and equipment used; and

(B) identifies the interoperable emergency communications systems in use by public safety agencies in the United States.

(b) CLASSIFIED ANNEX.—The baseline assessment under this section may include a classified annex including information provided under subsection (a)(5)(A).

(c) SAVINGS CLAUSE.—In conducting the baseline assessment under this section, the Secretary may incorporate findings from assessments conducted before, or ongoing on, the date of enactment of this title.

(d) PROGRESS REPORTS.—Not later than one year after the date of enactment of this section and biennially thereafter, the Secretary, acting through the ⟦Director for Emergency Communica-

tions] *Assistant Director for Emergency Communications*, shall submit to Congress a report on the progress of the Department in achieving the goals of, and carrying out its responsibilities under, this title, including—

(1) a description of the findings of the most recent baseline assessment conducted under subsection (a);

(2) a determination of the degree to which interoperable emergency communications capabilities have been attained to date and the gaps that remain for interoperability to be achieved;

(3) an evaluation of the ability to continue to communicate and to provide and maintain interoperable emergency communications by emergency managers, emergency response providers, and relevant government officials in the event of—

(A) natural disasters, acts of terrorism, or other man-made disasters, including Incidents of National Significance declared by the Secretary under the National Response Plan; and

(B) a catastrophic loss of local and regional communications services;

(4) a list of best practices relating to the ability to continue to communicate and to provide and maintain interoperable emergency communications in the event of natural disasters, acts of terrorism, or other man-made disasters; and

(A) an evaluation of the feasibility and desirability of the Department developing, on its own or in conjunction with the Department of Defense, a mobile communications capability, modeled on the Army Signal Corps, that could be deployed to support emergency communications at the site of natural disasters, acts of terrorism, or other man-made disasters.

SEC. 1804. 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, 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—

(A) such government has not complied with the requirement to submit a Statewide Interoperable Communications Plan as required by section 7303(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(f));

(B) such government has proposed to upgrade or purchase new equipment or systems that do not meet or exceed any applicable national voluntary consensus standards and has not provided a reasonable explanation of why such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed such standards; and

(C) as of the date that is 3 years after the date of the completion of the initial National Emergency Communications Plan under section 1802, national voluntary consensus standards for interoperable emergency communications capabilities have not been developed and promulgated.

(2) STANDARDS.—The Secretary, in coordination with the Federal Communications Commission, the National Institute of Standards and Technology, and other Federal departments and agencies with responsibility for standards, shall support the development, promulgation, and updating as necessary of national voluntary consensus standards for interoperable emergency communications.

SEC. 1805. REGIONAL EMERGENCY COMMUNICATIONS COORDINATION.

(a) IN GENERAL.—There is established in each Regional Office a Regional Emergency Communications Coordination Working Group (in this section referred to as an "RECC Working Group"). Each RECC Working Group shall report to the relevant Regional Administrator and coordinate its activities with the relevant Regional Advisory Council.

(b) MEMBERSHIP.—Each RECC Working Group shall consist of the following:

(1) NON-FEDERAL.—Organizations representing the interests of the following:

(A) State officials.

(B) Local government officials, including sheriffs.

(C) State police departments.

(D) Local police departments.

(E) Local fire departments.

(F) Public safety answering points (9–1–1 services).

(G) State emergency managers, homeland security directors, or representatives of State Administrative Agencies.

(H) Local emergency managers or homeland security directors.

(I) Other emergency response providers as appropriate.

(2) FEDERAL.—Representatives from the Department, the Federal Communications Commission, and other Federal departments and agencies with responsibility for coordinating interoperable emergency communications with or providing emergency support services to State, local, and tribal governments.

(c) COORDINATION.—Each RECC Working Group shall coordinate its activities with the following:

(1) Communications equipment manufacturers and vendors (including broadband data service providers).

(2) Local exchange carriers.

(3) Local broadcast media.

(4) Wireless carriers.
(5) Satellite communications services.
(6) Cable operators.
(7) Hospitals.
(8) Public utility services.
(9) Emergency evacuation transit services.
(10) Ambulance services.
(11) HAM and amateur radio operators.
(12) Representatives from other private sector entities and nongovernmental organizations as the Regional Administrator determines appropriate.

(d) DUTIES.—The duties of each RECC Working Group shall include—

(1) assessing the survivability, sustainability, and interoperability of local emergency communications systems to meet the goals of the National Emergency Communications Plan;

(2) reporting annually to the relevant Regional Administrator, the [Director for Emergency Communications] *Assistant Director for Emergency Communications*, the Chairman of the Federal Communications Commission, and the Assistant Secretary for Communications and Information of the Department of Commerce on the status of its region in building robust and sustainable interoperable voice and data emergency communications networks and, not later than 60 days after the completion of the initial National Emergency Communications Plan under section 1802, on the progress of the region in meeting the goals of such plan;

(3) ensuring a process for the coordination of effective multijurisdictional, multi-agency emergency communications networks for use during natural disasters, acts of terrorism, and other man-made disasters through the expanded use of emergency management and public safety communications mutual aid agreements; and

(4) coordinating the establishment of Federal, State, local, and tribal support services and networks designed to address the immediate and critical human needs in responding to natural disasters, acts of terrorism, and other man-made disasters.

* * * * * * *

SEC. 1809. INTEROPERABLE EMERGENCY COMMUNICATIONS GRANT PROGRAM.

(a) ESTABLISHMENT.—The Secretary shall establish the Interoperable Emergency Communications Grant Program to make grants to States to carry out initiatives to improve local, tribal, statewide, regional, national and, where appropriate, international interoperable emergency communications, including communications in collective response to natural disasters, acts of terrorism, and other man-made disasters.

(b) POLICY.—The [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 Commu-*

nications Division under this title, including ensuring that activities funded by the grant—

(1) comply with the statewide plan for that State required by section 7303(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(f)); and

(2) comply with the National Emergency Communications Plan under section 1802, when completed.

(c) ADMINISTRATION.—

(1) IN GENERAL.—The Administrator of the Federal Emergency Management Agency shall administer the Interoperable Emergency Communications Grant Program pursuant to the responsibilities and authorities of the Administrator under title V of the Act.

(2) GUIDANCE.—In administering the grant program, the Administrator shall ensure that the use of grants is consistent with guidance established by the Director of Emergency Communications pursuant to section 7303(a)(1)(H) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(a)(1)(H)).

(d) USE OF FUNDS.—A State that receives a grant under this section shall use the grant to implement that State's Statewide Interoperability Plan required under section 7303(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(f)) and approved under subsection (e), and to assist with activities determined by the Secretary to be integral to interoperable emergency communications.

(e) APPROVAL OF PLANS.—

(1) APPROVAL AS CONDITION OF GRANT.—Before a State may receive a grant under this section, the Director of 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 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 of Emergency Communications may approve revisions to a State's plan if the Director determines that doing so is likely to further interoperability.

(f) LIMITATIONS ON USES OF FUNDS.—

(1) IN GENERAL.—The recipient of a grant under this section may not use the grant—

(A) to supplant State or local funds;

(B) for any State or local government cost-sharing contribution; or

(C) for recreational or social purposes.

(2) PENALTIES.—In addition to other remedies currently available, the Secretary may take such actions as necessary to

ensure that recipients of grant funds are using the funds for the purpose for which they were intended.

(g) LIMITATIONS ON AWARD OF GRANTS.—

(1) NATIONAL EMERGENCY COMMUNICATIONS PLAN REQUIRED.—The Secretary may not award a grant under this section before the date on which the Secretary completes and submits to Congress the National Emergency Communications Plan required under section 1802.

(2) VOLUNTARY CONSENSUS STANDARDS.—The Secretary may not award a grant to a State under this section for the purchase of equipment that does not meet applicable voluntary consensus standards, unless the State demonstrates that there are compelling reasons for such purchase.

(h) AWARD OF GRANTS.—In approving applications and awarding grants under this section, the Secretary shall consider—

(1) the risk posed to each State by natural disasters, acts of terrorism, or other manmade disasters, including—

(A) the likely need of a jurisdiction within the State to respond to such risk in nearby jurisdictions;

(B) the degree of threat, vulnerability, and consequences related to critical infrastructure (from all critical infrastructure sectors) or key resources identified by the Administrator or the State homeland security and emergency management plans, including threats to, vulnerabilities of, and consequences from damage to critical infrastructure and key resources in nearby jurisdictions;

(C) the size of the population and density of the population of the State, including appropriate consideration of military, tourist, and commuter populations;

(D) whether the State is on or near an international border;

(E) whether the State encompasses an economically significant border crossing; and

(F) whether the State has a coastline bordering an ocean, a major waterway used for interstate commerce, or international waters; and

(2) the anticipated effectiveness of the State's proposed use of grant funds to improve interoperability.

(i) OPPORTUNITY TO AMEND APPLICATIONS.—In considering applications for grants under this section, the Administrator shall provide applicants with a reasonable opportunity to correct defects in the application, if any, before making final awards.

(j) MINIMUM GRANT AMOUNTS.—

(1) STATES.—In awarding grants under this section, the Secretary shall ensure that for each fiscal year, except as provided in paragraph (2), no State receives a grant in an amount that is less than the following percentage of the total amount appropriated for grants under this section for that fiscal year:

(A) For fiscal year 2008, 0.50 percent.

(B) For fiscal year 2009, 0.50 percent.

(C) For fiscal year 2010, 0.45 percent.

(D) For fiscal year 2011, 0.40 percent.

(E) For fiscal year 2012 and each subsequent fiscal year, 0.35 percent.

(2) TERRITORIES AND POSSESSIONS.—In awarding grants under this section, the Secretary shall ensure that for each fiscal year, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the Virgin Islands each receive grants in amounts that are not less than 0.08 percent of the total amount appropriated for grants under this section for that fiscal year.

(k) CERTIFICATION.—Each State that receives a grant under this section shall certify that the grant is used for the purpose for which the funds were intended and in compliance with the State's approved Statewide Interoperable Communications Plan.

(l) STATE RESPONSIBILITIES.—

(1) AVAILABILITY OF FUNDS TO LOCAL AND TRIBAL GOVERNMENTS.—Not later than 45 days after receiving grant funds, any State that receives a grant under this section shall obligate or otherwise make available to local and tribal governments—

(A) not less than 80 percent of the grant funds;

(B) with the consent of local and tribal governments, eligible expenditures having a value of not less than 80 percent of the amount of the grant; or

(C) grant funds combined with other eligible expenditures having a total value of not less than 80 percent of the amount of the grant.

(2) ALLOCATION OF FUNDS.—A State that receives a grant under this section shall allocate grant funds to tribal governments in the State to assist tribal communities in improving interoperable communications, in a manner consistent with the Statewide Interoperable Communications Plan. A State may not impose unreasonable or unduly burdensome requirements on a tribal government as a condition of providing grant funds or resources to the tribal government.

(3) PENALTIES.—If a State violates the requirements of this subsection, in addition to other remedies available to the Secretary, the Secretary may terminate or reduce the amount of the grant awarded to that State or transfer grant funds previously awarded to the State directly to the appropriate local or tribal government.

(m) REPORTS.—

(1) ANNUAL REPORTS BY STATE GRANT RECIPIENTS.—A State that receives a grant under this section shall annually submit to the 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 shall make the reports publicly available, including by making them available on the Internet website of the [Office of Emergency Communications] *Emergency Communications Division*, subject to any redactions that the 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 shall submit to

Congress a report on the use of grants awarded under this section and any progress in implementing Statewide Interoperable Communications Plans and improving interoperability at the city, county, regional, State, and interstate level, as a result of the award of such grants.

(n) RULE OF CONSTRUCTION.—Nothing in this section shall be construed or interpreted to preclude a State from using a grant awarded under this section for interim or long-term Internet Protocol-based interoperable solutions.

(o) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for grants under this section—

(1) for fiscal year 2008, such sums as may be necessary;

(2) for each of fiscal years 2009 through 2012, $400,000,000; and

(3) for each subsequent fiscal year, such sums as may be necessary.

SEC. 1810. 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 the Emergency Communications Division (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) LOCATION OF COMMUNITIES.—No fewer than 3 of the communities selected under paragraph (2) shall be located on the northern border of the United States and no fewer than 3 of the communities selected under paragraph (2) shall be located on the southern border of the United States.

(b) CONDITIONS.—The [Director] *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) identify solutions to facilitate interoperable communications across national borders expeditiously;

(2) help ensure that emergency response providers can communicate with each other in the event of natural disasters, acts of terrorism, and other man-made disasters;

(3) provide technical assistance to enable emergency response providers to deal with threats and contingencies in a variety of environments;

(4) identify appropriate joint-use equipment to ensure communications access;

(5) identify solutions to facilitate communications between emergency response providers in communities of differing population densities; and

(6) take other actions or provide equipment as the [Director] *Assistant Director* deems appropriate to foster interoperable emergency communications.

(d) DISTRIBUTION OF FUNDS.—

(1) IN GENERAL.—The Secretary shall distribute funds under this section to each community participating in the demonstration project through the State, or States, in which each community is located.

(2) OTHER PARTICIPANTS.—A State shall make the funds available promptly to the local and tribal governments and emergency response providers selected by the Secretary to participate in the demonstration project.

(3) REPORT.—Not later than 90 days after a State receives funds under this subsection the State shall report to the [Director] *Assistant 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.

(g) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for grants under this section such sums as may be necessary.

* * * * * * *

TITLE XXI—CHEMICAL FACILITY ANTI–TERRORISM STANDARDS

SEC. 2101. DEFINITIONS.

In this title—

(1) the term "CFATS regulation" means—

(A) an existing CFATS regulation; and

(B) any regulation or amendment to an existing CFATS regulation issued pursuant to the authority under section 2107;

(2) the term "chemical facility of interest" means a facility that—

(A) holds, or that the Secretary has a reasonable basis to believe holds, a chemical of interest, as designated under Appendix A to part 27 of title 6, Code of Federal Regulations, or any successor thereto, at a threshold quantity set pursuant to relevant risk-related security principles; and

(B) is not an excluded facility;

(3) the term "covered chemical facility" means a facility that—

(A) the Secretary—

(i) identifies as a chemical facility of interest; and

(ii) based upon review of the facility's Top-Screen, determines meets the risk criteria developed under section 2102(e)(2)(B); and

(B) is not an excluded facility;

(4) the term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency;

[(4)] *(5)* the term "excluded facility" means—

(A) a facility regulated under the Maritime Transportation Security Act of 2002 (Public Law 107–295; 116 Stat. 2064);

(B) a public water system, as that term is defined in section 1401 of the Safe Drinking Water Act (42 U.S.C. 300f);

(C) a Treatment Works, as that term is defined in section 212 of the Federal Water Pollution Control Act (33 U.S.C. 1292);

(D) a facility owned or operated by the Department of Defense or the Department of Energy; or

(E) a facility subject to regulation by the Nuclear Regulatory Commission, or by a State that has entered into an agreement with the Nuclear Regulatory Commission under section 274 b. of the Atomic Energy Act of 1954 (42 U.S.C. 2021(b)) to protect against unauthorized access of any material, activity, or structure licensed by the Nuclear Regulatory Commission;

[(5)] *(6)* the term "existing CFATS regulation" means—

(A) a regulation promulgated under section 550 of the Department of Homeland Security Appropriations Act, 2007 (Public Law 109–295; 6 U.S.C. 121 note) that is in effect on the day before the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014; and

(B) a Federal Register notice or other published guidance relating to section 550 of the Department of Homeland Security Appropriations Act, 2007 that is in effect on the day before the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014;

[(6)] *(7)* the term "expedited approval facility" means a covered chemical facility for which the owner or operator elects to submit a site security plan in accordance with section 2102(c)(4);

[(7)] *(8)* the term "facially deficient", relating to a site security plan, means a site security plan that does not support a certification that the security measures in the plan address the

security vulnerability assessment and the risk-based performance standards for security for the facility, based on a review of—

(A) the facility's site security plan;

(B) the facility's Top-Screen;

(C) the facility's security vulnerability assessment; or

(D) any other information that—

(i) the facility submits to the Department; or

(ii) the Department obtains from a public source or other source;

[(8)] *(9)* the term "guidance for expedited approval facilities" means the guidance issued under section 2102(c)(4)(B)(i);

[(9)] *(10)* the term "risk assessment" means the Secretary's application of relevant risk criteria identified in section 2102(e)(2)(B);

[(10)] *(11)* the term "terrorist screening database" means the terrorist screening database maintained by the Federal Government Terrorist Screening Center or its successor;

[(11)] *(12)* the term "tier" has the meaning given the term in section 27.105 of title 6, Code of Federal Regulations, or any successor thereto;

[(12)] *(13)* the terms "tiering" and "tiering methodology" mean the procedure by which the Secretary assigns a tier to each covered chemical facility based on the risk assessment for that covered chemical facility;

[(13)] *(14)* the term "Top-Screen" has the meaning given the term in section 27.105 of title 6, Code of Federal Regulations, or any successor thereto; and

[(14)] *(15)* the term "vulnerability assessment" means the identification of weaknesses in the security of a chemical facility of interest.

SEC. 2102. CHEMICAL FACILITY ANTI-TERRORISM STANDARDS PROGRAM.

(a) PROGRAM ESTABLISHED.—

(1) IN GENERAL.—There is in the Department a Chemical Facility Anti-Terrorism Standards Program. *Such Program shall be located in the Cybersecurity and Infrastructure Security Agency.*

(2) REQUIREMENTS.—In carrying out the Chemical Facility Anti-Terrorism Standards Program, the Secretary shall—

(A) identify—

(i) chemical facilities of interest; and

(ii) covered chemical facilities;

(B) require each chemical facility of interest to submit a Top-Screen and any other information the Secretary determines necessary to enable the Department to assess the security risks associated with the facility;

(C) establish risk-based performance standards designed to address high levels of security risk at covered chemical facilities; and

(D) require each covered chemical facility to—

(i) submit a security vulnerability assessment; and

(ii) develop, submit, and implement a site security plan.

(b) SECURITY MEASURES.—

(1) IN GENERAL.—A facility, in developing a site security plan as required under subsection (a), shall include security measures that, in combination, appropriately address the security vulnerability assessment and the risk-based performance standards for security for the facility.

(2) EMPLOYEE INPUT.—To the greatest extent practicable, a facility's security vulnerability assessment and site security plan shall include input from at least 1 facility employee and, where applicable, 1 employee representative from the bargaining agent at that facility, each of whom possesses, in the determination of the facility's security officer, relevant knowledge, experience, training, or education as pertains to matters of site security.

(c) APPROVAL OR DISAPPROVAL OF SITE SECURITY PLANS.—

(1) IN GENERAL.—

(A) REVIEW.—Except as provided in paragraph (4), the Secretary shall review and approve or disapprove each site security plan submitted pursuant to subsection (a).

(B) BASES FOR DISAPPROVAL.—The Secretary—

(i) may not disapprove a site security plan based on the presence or absence of a particular security measure; and

(ii) shall disapprove a site security plan if the plan fails to satisfy the risk-based performance standards established pursuant to subsection (a)(2)(C).

(2) ALTERNATIVE SECURITY PROGRAMS.—

(A) AUTHORITY TO APPROVE.—

(i) IN GENERAL.—The Secretary may approve an alternative security program established by a private sector entity or a Federal, State, or local authority or under other applicable laws, if the Secretary determines that the requirements of the program meet the requirements under this section.

(ii) ADDITIONAL SECURITY MEASURES.—If the requirements of an alternative security program do not meet the requirements under this section, the Secretary may recommend additional security measures to the program that will enable the Secretary to approve the program.

(B) SATISFACTION OF SITE SECURITY PLAN REQUIREMENT.—A covered chemical facility may satisfy the site security plan requirement under subsection (a) by adopting an alternative security program that the Secretary has—

(i) reviewed and approved under subparagraph (A); and

(ii) determined to be appropriate for the operations and security concerns of the covered chemical facility.

(3) SITE SECURITY PLAN ASSESSMENTS.—

(A) RISK ASSESSMENT POLICIES AND PROCEDURES.—In approving or disapproving a site security plan under this subsection, the Secretary shall employ the risk assessment policies and procedures developed under this title.

(B) PREVIOUSLY APPROVED PLANS.—In the case of a covered chemical facility for which the Secretary approved a site security plan before the date of enactment of the Pro-

tecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, the Secretary may not require the facility to resubmit the site security plan solely by reason of the enactment of this title.

(4) EXPEDITED APPROVAL PROGRAM.—

(A) IN GENERAL.—A covered chemical facility assigned to tier 3 or 4 may meet the requirement to develop and submit a site security plan under subsection (a)(2)(D) by developing and submitting to the Secretary—

(i) a site security plan and the certification described in subparagraph (C); or

(ii) a site security plan in conformance with a template authorized under subparagraph (H).

(B) GUIDANCE FOR EXPEDITED APPROVAL FACILITIES.—

(i) IN GENERAL.—Not later than 180 days after the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, the Secretary shall issue guidance for expedited approval facilities that identifies specific security measures that are sufficient to meet the risk-based performance standards.

(ii) MATERIAL DEVIATION FROM GUIDANCE.—If a security measure in the site security plan of an expedited approval facility materially deviates from a security measure in the guidance for expedited approval facilities, the site security plan shall include an explanation of how such security measure meets the risk-based performance standards.

(iii) APPLICABILITY OF OTHER LAWS TO DEVELOPMENT AND ISSUANCE OF INITIAL GUIDANCE.—During the period before the Secretary has met the deadline under clause (i), in developing and issuing, or amending, the guidance for expedited approval facilities under this subparagraph and in collecting information from expedited approval facilities, the Secretary shall not be subject to—

(I) section 553 of title 5, United States Code;

(II) subchapter I of chapter 35 of title 44, United States Code; or

(III) section 2107(b) of this title.

(C) CERTIFICATION.—The owner or operator of an expedited approval facility shall submit to the Secretary a certification, signed under penalty of perjury, that—

(i) the owner or operator is familiar with the requirements of this title and part 27 of title 6, Code of Federal Regulations, or any successor thereto, and the site security plan being submitted;

(ii) the site security plan includes the security measures required by subsection (b);

(iii)(I) the security measures in the site security plan do not materially deviate from the guidance for expedited approval facilities except where indicated in the site security plan;

(II) any deviations from the guidance for expedited approval facilities in the site security plan meet the

risk-based performance standards for the tier to which the facility is assigned; and

(III) the owner or operator has provided an explanation of how the site security plan meets the risk-based performance standards for any material deviation;

(iv) the owner or operator has visited, examined, documented, and verified that the expedited approval facility meets the criteria set forth in the site security plan;

(v) the expedited approval facility has implemented all of the required performance measures outlined in the site security plan or set out planned measures that will be implemented within a reasonable time period stated in the site security plan;

(vi) each individual responsible for implementing the site security plan has been made aware of the requirements relevant to the individual's responsibility contained in the site security plan and has demonstrated competency to carry out those requirements;

(vii) the owner or operator has committed, or, in the case of planned measures will commit, the necessary resources to fully implement the site security plan; and

(viii) the planned measures include an adequate procedure for addressing events beyond the control of the owner or operator in implementing any planned measures.

(D) DEADLINE.—

(i) IN GENERAL.—Not later than 120 days after the date described in clause (ii), the owner or operator of an expedited approval facility shall submit to the Secretary the site security plan and the certification described in subparagraph (C).

(ii) DATE.—The date described in this clause is—

(I) for an expedited approval facility that was assigned to tier 3 or 4 under existing CFATS regulations before the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, the date that is 210 days after the date of enactment of that Act; and

(II) for any expedited approval facility not described in subclause (I), the later of—

(aa) the date on which the expedited approval facility is assigned to tier 3 or 4 under subsection (e)(2)(A); or

(bb) the date that is 210 days after the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014.

(iii) NOTICE.—An owner or operator of an expedited approval facility shall notify the Secretary of the intent of the owner or operator to certify the site security plan for the expedited approval facility not later than 30 days before the date on which the owner or

operator submits the site security plan and certification described in subparagraph (C).

(E) COMPLIANCE.—

(i) IN GENERAL.—For an expedited approval facility submitting a site security plan and certification in accordance with subparagraphs (A), (B), (C), and (D)—

(I) the expedited approval facility shall comply with all of the requirements of its site security plan; and

(II) the Secretary—

(aa) except as provided in subparagraph (G), may not disapprove the site security plan; and

(bb) may audit and inspect the expedited approval facility under subsection (d) to verify compliance with its site security plan.

(ii) NONCOMPLIANCE.—If the Secretary determines an expedited approval facility is not in compliance with the requirements of the site security plan or is otherwise in violation of this title, the Secretary may enforce compliance in accordance with section 2104.

(F) AMENDMENTS TO SITE SECURITY PLAN.—

(i) REQUIREMENT.—

(I) IN GENERAL.—If the owner or operator of an expedited approval facility amends a site security plan submitted under subparagraph (A), the owner or operator shall submit the amended site security plan and a certification relating to the amended site security plan that contains the information described in subparagraph (C).

(II) TECHNICAL AMENDMENTS.—For purposes of this clause, an amendment to a site security plan includes any technical amendment to the site security plan.

(ii) AMENDMENT REQUIRED.—The owner or operator of an expedited approval facility shall amend the site security plan if—

(I) there is a change in the design, construction, operation, or maintenance of the expedited approval facility that affects the site security plan;

(II) the Secretary requires additional security measures or suspends a certification and recommends additional security measures under subparagraph (G); or

(III) the owner or operator receives notice from the Secretary of a change in tiering under subsection (e)(3).

(iii) DEADLINE.—An amended site security plan and certification shall be submitted under clause (i)—

(I) in the case of a change in design, construction, operation, or maintenance of the expedited approval facility that affects the security plan, not later than 120 days after the date on which the change in design, construction, operation, or maintenance occurred;

(II) in the case of the Secretary requiring additional security measures or suspending a certification and recommending additional security measures under subparagraph (G), not later than 120 days after the date on which the owner or operator receives notice of the requirement for additional security measures or suspension of the certification and recommendation of additional security measures; and

(III) in the case of a change in tiering, not later than 120 days after the date on which the owner or operator receives notice under subsection (e)(3).

(G) FACIALLY DEFICIENT SITE SECURITY PLANS.—

(i) PROHIBITION.—Notwithstanding subparagraph (A) or (E), the Secretary may suspend the authority of a covered chemical facility to certify a site security plan if the Secretary—

(I) determines the certified site security plan or an amended site security plan is facially deficient; and

(II) not later than 100 days after the date on which the Secretary receives the site security plan and certification, provides the covered chemical facility with written notification that the site security plan is facially deficient, including a clear explanation of each deficiency in the site security plan.

(ii) ADDITIONAL SECURITY MEASURES.—

(I) IN GENERAL.—If, during or after a compliance inspection of an expedited approval facility, the Secretary determines that planned or implemented security measures in the site security plan of the facility are insufficient to meet the risk-based performance standards based on misrepresentation, omission, or an inadequate description of the site, the Secretary may—

(aa) require additional security measures; or

(bb) suspend the certification of the facility.

(II) RECOMMENDATION OF ADDITIONAL SECURITY MEASURES.—If the Secretary suspends the certification of an expedited approval facility under subclause (I), the Secretary shall—

(aa) recommend specific additional security measures that, if made part of the site security plan by the facility, would enable the Secretary to approve the site security plan; and

(bb) provide the facility an opportunity to submit a new or modified site security plan and certification under subparagraph (A).

(III) SUBMISSION; REVIEW.—If an expedited approval facility determines to submit a new or modified site security plan and certification as authorized under subclause (II)(bb)—

(aa) not later than 90 days after the date on which the facility receives recommendations under subclause (II)(aa), the facility shall submit the new or modified plan and certification; and

(bb) not later than 45 days after the date on which the Secretary receives the new or modified plan under item (aa), the Secretary shall review the plan and determine whether the plan is facially deficient.

(IV) DETERMINATION NOT TO INCLUDE ADDITIONAL SECURITY MEASURES.—

(aa) REVOCATION OF CERTIFICATION.—If an expedited approval facility does not agree to include in its site security plan specific additional security measures recommended by the Secretary under subclause (II)(aa), or does not submit a new or modified site security plan in accordance with subclause (III), the Secretary may revoke the certification of the facility by issuing an order under section 2104(a)(1)(B).

(bb) EFFECT OF REVOCATION.—If the Secretary revokes the certification of an expedited approval facility under item (aa) by issuing an order under section 2104(a)(1)(B)—

(AA) the order shall require the owner or operator of the facility to submit a site security plan or alternative security program for review by the Secretary review under subsection (c)(1); and

(BB) the facility shall no longer be eligible to certify a site security plan under this paragraph.

(V) FACIAL DEFICIENCY.—If the Secretary determines that a new or modified site security plan submitted by an expedited approval facility under subclause (III) is facially deficient—

(aa) not later than 120 days after the date of the determination, the owner or operator of the facility shall submit a site security plan or alternative security program for review by the Secretary under subsection (c)(1); and

(bb) the facility shall no longer be eligible to certify a site security plan under this paragraph.

(H) TEMPLATES.—

(i) IN GENERAL.—The Secretary may develop prescriptive site security plan templates with specific security measures to meet the risk-based performance standards under subsection (a)(2)(C) for adoption and certification by a covered chemical facility assigned to tier 3 or 4 in lieu of developing and certifying its own plan.

(ii) APPLICABILITY OF OTHER LAWS TO DEVELOPMENT AND ISSUANCE OF INITIAL SITE SECURITY PLAN TEM-

PLATES AND RELATED GUIDANCE.—During the period before the Secretary has met the deadline under subparagraph (B)(i), in developing and issuing, or amending, the site security plan templates under this subparagraph, in issuing guidance for implementation of the templates, and in collecting information from expedited approval facilities, the Secretary shall not be subject to—

(I) section 553 of title 5, United States Code;

(II) subchapter I of chapter 35 of title 44, United States Code; or

(III) section 2107(b) of this title.

(iii) RULE OF CONSTRUCTION.—Nothing in this subparagraph shall be construed to prevent a covered chemical facility from developing and certifying its own security plan in accordance with subparagraph (A).

(I) EVALUATION.—

(i) IN GENERAL.—Not later than 18 months after the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, the Secretary shall take any appropriate action necessary for a full evaluation of the expedited approval program authorized under this paragraph, including conducting an appropriate number of inspections, as authorized under subsection (d), of expedited approval facilities.

(ii) REPORT.—Not later than 18 months after the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives a report that contains—

(I)(aa) the number of eligible facilities using the expedited approval program authorized under this paragraph; and

(bb) the number of facilities that are eligible for the expedited approval program but are using the standard process for developing and submitting a site security plan under subsection (a)(2)(D);

(II) any costs and efficiencies associated with the expedited approval program;

(III) the impact of the expedited approval program on the backlog for site security plan approval and authorization inspections;

(IV) an assessment of the ability of expedited approval facilities to submit facially sufficient site security plans;

(V) an assessment of any impact of the expedited approval program on the security of chemical facilities; and

(VI) a recommendation by the Secretary on the frequency of compliance inspections that may be required for expedited approval facilities.

(d) COMPLIANCE.—

(1) AUDITS AND INSPECTIONS.—

(A) DEFINITIONS.—In this paragraph—

(i) the term "nondepartmental"—

(I) with respect to personnel, means personnel that is not employed by the Department; and

(II) with respect to an entity, means an entity that is not a component or other authority of the Department; and

(ii) the term "nongovernmental"—

(I) with respect to personnel, means personnel that is not employed by the Federal Government; and

(II) with respect to an entity, means an entity that is not an agency, department, or other authority of the Federal Government.

(B) AUTHORITY TO CONDUCT AUDITS AND INSPECTIONS.—The Secretary shall conduct audits or inspections under this title using—

(i) employees of the Department;

(ii) nondepartmental or nongovernmental personnel approved by the Secretary; or

(iii) a combination of individuals described in clauses (i) and (ii).

(C) SUPPORT PERSONNEL.—The Secretary may use nongovernmental personnel to provide administrative and logistical services in support of audits and inspections under this title.

(D) REPORTING STRUCTURE.—

(i) NONDEPARTMENTAL AND NONGOVERNMENTAL AUDITS AND INSPECTIONS.—Any audit or inspection conducted by an individual employed by a nondepartmental or nongovernmental entity shall be assigned in coordination with a regional supervisor with responsibility for supervising inspectors within the Infrastructure Security Compliance Division of the Department for the region in which the audit or inspection is to be conducted.

(ii) REQUIREMENT TO REPORT.—While an individual employed by a nondepartmental or nongovernmental entity is in the field conducting an audit or inspection under this subsection, the individual shall report to the regional supervisor with responsibility for supervising inspectors within the Infrastructure Security Compliance Division of the Department for the region in which the individual is operating.

(iii) APPROVAL.—The authority to approve a site security plan under subsection (c) or determine if a covered chemical facility is in compliance with an approved site security plan shall be exercised solely by the Secretary or a designee of the Secretary within the Department.

(E) STANDARDS FOR AUDITORS AND INSPECTORS.—The Secretary shall prescribe standards for the training and retraining of each individual used by the Department as an auditor or inspector, including each individual employed by the Department and all nondepartmental or nongovernmental personnel, including—

(i) minimum training requirements for new auditors and inspectors;

(ii) retraining requirements;

(iii) minimum education and experience levels;

(iv) the submission of information as required by the Secretary to enable determination of whether the auditor or inspector has a conflict of interest;

(v) the proper certification or certifications necessary to handle chemical-terrorism vulnerability information (as defined in section 27.105 of title 6, Code of Federal Regulations, or any successor thereto);

(vi) the reporting of any issue of non-compliance with this section to the Secretary within 24 hours; and

(vii) any additional qualifications for fitness of duty as the Secretary may require.

(F) CONDITIONS FOR NONGOVERNMENTAL AUDITORS AND INSPECTORS.—If the Secretary arranges for an audit or inspection under subparagraph (B) to be carried out by a nongovernmental entity, the Secretary shall—

(i) prescribe standards for the qualification of the individuals who carry out such audits and inspections that are commensurate with the standards for similar Government auditors or inspectors; and

(ii) ensure that any duties carried out by a nongovernmental entity are not inherently governmental functions.

(2) PERSONNEL SURETY.—

(A) PERSONNEL SURETY PROGRAM.—For purposes of this title, the Secretary shall establish and carry out a Personnel Surety Program that—

(i) does not require an owner or operator of a covered chemical facility that voluntarily participates in the program to submit information about an individual more than 1 time;

(ii) provides a participating owner or operator of a covered chemical facility with relevant information about an individual based on vetting the individual against the terrorist screening database, to the extent that such feedback is necessary for the facility to be in compliance with regulations promulgated under this title; and

(iii) provides redress to an individual—

(I) whose information was vetted against the terrorist screening database under the program; and

(II) who believes that the personally identifiable information submitted to the Department for such vetting by a covered chemical facility, or its designated representative, was inaccurate.

(B) PERSONNEL SURETY PROGRAM IMPLEMENTATION.—To the extent that a risk-based performance standard established under subsection (a) requires identifying individuals with ties to terrorism—

(i) a covered chemical facility—

(I) may satisfy its obligation under the standard by using any Federal screening program that periodically vets individuals against the terrorist screening database, or any successor program, including the Personnel Surety Program established under subparagraph (A); and

(II) shall—

(aa) accept a credential from a Federal screening program described in subclause (I) if an individual who is required to be screened presents such a credential; and

(bb) address in its site security plan or alternative security program the measures it will take to verify that a credential or documentation from a Federal screening program described in subclause (I) is current;

(ii) visual inspection shall be sufficient to meet the requirement under clause (i)(II)(bb), but the facility should consider other means of verification, consistent with the facility's assessment of the threat posed by acceptance of such credentials; and

(iii) the Secretary may not require a covered chemical facility to submit any information about an individual unless the individual—

(I) is to be vetted under the Personnel Surety Program; or

(II) has been identified as presenting a terrorism security risk.

(C) RIGHTS UNAFFECTED.—Nothing in this section shall supersede the ability—

(i) of a facility to maintain its own policies regarding the access of individuals to restricted areas or critical assets; or

(ii) of an employing facility and a bargaining agent, where applicable, to negotiate as to how the results of a background check may be used by the facility with respect to employment status.

(3) AVAILABILITY OF INFORMATION.—The Secretary shall share with the owner or operator of a covered chemical facility any information that the owner or operator needs to comply with this section.

(e) RESPONSIBILITIES OF THE SECRETARY.—

(1) IDENTIFICATION OF CHEMICAL FACILITIES OF INTEREST.—In carrying out this title, the Secretary shall consult with the heads of other Federal agencies, States and political subdivisions thereof, relevant business associations, and public and private labor organizations to identify all chemical facilities of interest.

(2) RISK ASSESSMENT.—

(A) IN GENERAL.—For purposes of this title, the Secretary shall develop a security risk assessment approach and corresponding tiering methodology for covered chemical facilities that incorporates the relevant elements of risk, including threat, vulnerability, and consequence.

(B) CRITERIA FOR DETERMINING SECURITY RISK.—The criteria for determining the security risk of terrorism associated with a covered chemical facility shall take into account—

(i) relevant threat information;

(ii) potential severe economic consequences and the potential loss of human life in the event of the facility being subject to attack, compromise, infiltration, or exploitation by terrorists; and

(iii) vulnerability of the facility to attack, compromise, infiltration, or exploitation by terrorists.

(3) CHANGES IN TIERING.—

(A) MAINTENANCE OF RECORDS.—The Secretary shall document the basis for each instance in which—

(i) tiering for a covered chemical facility is changed; or

(ii) a covered chemical facility is determined to no longer be subject to the requirements under this title.

(B) REQUIRED INFORMATION.—The records maintained under subparagraph (A) shall include information on whether and how the Secretary confirmed the information that was the basis for the change or determination described in subparagraph (A).

(4) SEMIANNUAL PERFORMANCE REPORTING.—Not later than 6 months after the date of enactment of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, and not less frequently than once every 6 months thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives a report that includes, for the period covered by the report—

(A) the number of covered chemical facilities in the United States;

(B) information—

(i) describing—

(I) the number of instances in which the Secretary—

(aa) placed a covered chemical facility in a lower risk tier; or

(bb) determined that a facility that had previously met the criteria for a covered chemical facility under section 2101(3) no longer met the criteria; and

(II) the basis, in summary form, for each action or determination under subclause (I); and

(ii) that is provided in a sufficiently anonymized form to ensure that the information does not identify any specific facility or company as the source of the in-

formation when viewed alone or in combination with other public information;

(C) the average number of days spent reviewing site security or an alternative security program for a covered chemical facility prior to approval;

(D) the number of covered chemical facilities inspected;

(E) the average number of covered chemical facilities inspected per inspector; and

(F) any other information that the Secretary determines will be helpful to Congress in evaluating the performance of the Chemical Facility Anti-Terrorism Standards Program.

* * * * * * *

SEC. 2104. CIVIL ENFORCEMENT.

(a) NOTICE OF NONCOMPLIANCE.—

(1) NOTICE.—If the Secretary determines that a covered chemical facility is not in compliance with this title, the Secretary shall—

(A) provide the owner or operator of the facility with—

(i) not later than 14 days after date on which the Secretary makes the determination, a written notification of noncompliance that includes a clear explanation of any deficiency in the security vulnerability assessment or site security plan; and

(ii) an opportunity for consultation with the Secretary or the Secretary's designee; and

(B) issue to the owner or operator of the facility an order to comply with this title by a date specified by the Secretary in the order, which date shall be not later than 180 days after the date on which the Secretary issues the order.

(2) CONTINUED NONCOMPLIANCE.—If an owner or operator remains noncompliant after the procedures outlined in paragraph (1) have been executed, or demonstrates repeated violations of this title, the Secretary may enter an order in accordance with this section assessing a civil penalty, an order to cease operations, or both.

(b) CIVIL PENALTIES.—

(1) VIOLATIONS OF ORDERS.—Any person who violates an order issued under this title shall be liable for a civil penalty under section 70119(a) of title 46, United States Code.

(2) NON-REPORTING CHEMICAL FACILITIES OF INTEREST.—Any owner of a chemical facility of interest who fails to comply with, or knowingly submits false information under, this title or the CFATS regulations shall be liable for a civil penalty under section 70119(a) of title 46, United States Code.

(c) EMERGENCY ORDERS.—

(1) IN GENERAL.—Notwithstanding subsection (a) or any site security plan or alternative security program approved under this title, if the Secretary determines that there is an imminent threat of death, serious illness, or severe personal injury, due to a violation of this title or the risk of a terrorist incident that may affect a chemical facility of interest, the Secretary—

(A) shall consult with the facility, if practicable, on steps to mitigate the risk; and

(B) may order the facility, without notice or opportunity for a hearing, effective immediately or as soon as practicable, to—

(i) implement appropriate emergency security measures; or

(ii) cease or reduce some or all operations, in accordance with safe shutdown procedures, if the Secretary determines that such a cessation or reduction of operations is the most appropriate means to address the risk.

(2) LIMITATION ON DELEGATION.—The Secretary may not delegate the authority under paragraph (1) to any official other than the **[**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 the Cybersecurity and Infrastructure Security Agency*.

(3) LIMITATION ON AUTHORITY.—The Secretary may exercise the authority under this subsection only to the extent necessary to abate the imminent threat determination under paragraph (1).

(4) DUE PROCESS FOR FACILITY OWNER OR OPERATOR.—

(A) WRITTEN ORDERS.—An order issued by the Secretary under paragraph (1) shall be in the form of a written emergency order that—

(i) describes the violation or risk that creates the imminent threat;

(ii) states the security measures or order issued or imposed; and

(iii) describes the standards and procedures for obtaining relief from the order.

(B) OPPORTUNITY FOR REVIEW.—After issuing an order under paragraph (1) with respect to a chemical facility of interest, the Secretary shall provide for review of the order under section 554 of title 5 if a petition for review is filed not later than 20 days after the date on which the Secretary issues the order.

(C) EXPIRATION OF EFFECTIVENESS OF ORDER.—If a petition for review of an order is filed under subparagraph (B) and the review under that paragraph is not completed by the last day of the 30-day period beginning on the date on which the petition is filed, the order shall vacate automatically at the end of that period unless the Secretary determines, in writing, that the imminent threat providing a basis for the order continues to exist.

(d) RIGHT OF ACTION.—Nothing in this title confers upon any person except the Secretary or his or her designee a right of action against an owner or operator of a covered chemical facility to enforce any provision of this title.

* * * * * * *

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 such term in section 2215.

(2) CRITICAL INFRASTRUCTURE RISK.—The term "critical infrastructure risk" means threats to and vulnerabilities of critical infrastructure and any related consequences, including consequences caused by or resulting from an act of terrorism.

(3) CYBERSECURITY RISK.—The term "cybersecurity risk" has the meaning given such term in section 2209.

(4) CYBERSECURITY THREAT.—The term "cybersecurity threat" has the meaning given such term in paragraph (5) of section 102 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)).

(5) FEDERAL ENTITY.—The term "Federal entity" has the meaning given such term in paragraph (8) of section 102 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)).

(6) NON-FEDERAL ENTITY.—The term "non-Federal entity" has the meaning given such term in paragraph (14) of section 102 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)).

(7) SHARING.—The term "sharing" has the meaning given such term in section 2209.

(8) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term "national cybersecurity asset response activities" means—

(A) furnishing 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.

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 the 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 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 Secretary's responsibilities 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;

(5) upon request provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and, where appropriate, provide such analyses, expertise, and other technical assistance in coordination with critical infrastructure sector specific agencies and other Federal departments and agencies;

(6) to the extent required by law, exercise duties in coordination with sector-specific agencies;

(7) maintain and utilize mechanisms for the regular and ongoing consultation and collaboration among the Agency's Divisions to further operational coordination, integrated situational awareness, and improved integration across the Agency in accordance with this Act;

(8) develop, coordinate, and implement—

(A) comprehensive strategic plans for the activities of the Agency; and

(B) risk assessments;

(9) carry out emergency communications responsibilities, in accordance with title XVIII;

(10) carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement; and

(11) 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 such 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 such 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 such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

(C) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether such information, analysis, or assessments are provided or produced by the Department) in order to identify priorities 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 such information from other Federal Government agencies.

(E) 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.

(F) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government 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 law enforcement information, and other 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 such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

(I) To consult with State, local, tribal, and territorial government agencies and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(J) To ensure that any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties.

(K) To request additional information from other Federal Government agencies, State, local, tribal, and territorial government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

(L) To establish and utilize, in conjunction with the chief information officer of the Department, a secure 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 ensure, in conjunction with the chief information officer of the Department, that any information databases

and analytical tools developed or utilized by the Department—

(i) are compatible with one another and with relevant information databases of other Federal Government agencies; and

(ii) treat information in such databases in a manner that complies with applicable Federal law on privacy.

(N) 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.

(O) To coordinate with Federal, State, local, tribal, and territorial law enforcement agencies, and the private sector, as appropriate.

(P) 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).

(Q) To carry out the functions of the national cybersecurity and communications integration center under section 2209.

(R) To carry out requirements of the Chemical Facilities Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate established under subtitle J of title VIII.

(2) MODIFICATION.—The Secretary may modify the functions specified in sections 2203(b) and 2204(b) upon certifying to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate 60 days prior to any such modification that such modification 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 its responsibilities 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 its responsibilities under this section, personnel of the Federal agencies referred to in subparagraph (B) may be detailed to the Agency for the performance of analytic functions and related duties.

(B) AGENCIES SPECIFIED.—The Federal agencies referred to in subparagraph (A) are the following:

(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) Any other agency of the Federal Government that the President considers appropriate.

(C) INTERAGENCY AGREEMENTS.—The Secretary and the head of an agency specified 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.—To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence. When establishing such locations, 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 existing leases, or agreeing to extend or newly occupy any Federal space or new construction.

(h) PRIVACY.—

(1) IN GENERAL.—There shall be a Privacy Officer of the Agency with primary responsibility for privacy policy and compliance for the Agency.

(2) RESPONSIBILITIES.—The responsibilities of the Privacy Officer of the Agency shall include—

(A) assuring that the use of technologies by the Agency sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(B) assuring that personal information contained in Privacy Act systems of records of the Agency is handled in full compliance with fair information practices as specified in 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 the 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 subtitle referred to as the "Assistant Director"), who shall—

(A) be at the level of Assistant Secretary within the Department; and

(B) 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 information and information systems for Federal entities 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 subsection (c)(7) of section 2202; 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 of Infrastructure Security (in this section referred to as the "Assistant Director"), who shall—

(A) be at the level of Assistant Secretary within the Department; and

(B) 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 efforts, at the direction of the Director, to secure the United States high-risk chemicals and chemical facilities consistent with law, including the Chemical Facilities Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate established under subtitle J of title VIII;

(3) fully participate in the mechanisms required under subsection (c)(7) of section 2202; and

(4) carry out such other duties and powers as prescribed by the Director.

SEC. [223.] *2205.* ENHANCEMENT OF FEDERAL AND NON-FEDERAL CYBERSECURITY.

In carrying out the responsibilities under section 201, the [Under Secretary appointed under section 103(a)(1)(H)] *Director of the Cybersecurity and Infrastructure Security Agency* shall—

(1) as appropriate, provide to State and local government entities, and upon request to private entities that own or operate critical information systems—

(A) analysis and warnings related to threats to, and vulnerabilities of, critical information systems; and

(B) in coordination with the Under Secretary for Emergency Preparedness and Response, crisis management support in response to threats to, or attacks on, critical information systems; and

(2) as appropriate, provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems; and

(3) fulfill the responsibilities of the Secretary to protect Federal information systems under subchapter II of chapter 35 of title 44, United States Code.

SEC. [224.] *2206.* NET GUARD.

The [Assistant Secretary for Infrastructure Protection] *Director of the Cybersecurity and Infrastructure Security Agency* may establish a national technology guard, to be known as "NET Guard", comprised of local teams of volunteers with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks.

SEC. [225.] *2207.* CYBER SECURITY ENHANCEMENT ACT OF 2002.

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

(b) AMENDMENT OF SENTENCING GUIDELINES RELATING TO CERTAIN COMPUTER CRIMES.—

(1) DIRECTIVE TO THE UNITED STATES SENTENCING COMMISSION.—Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this subsection, the United States Sentencing Commission shall review and, if appropriate, amend its guidelines and its policy statements applicable to persons convicted of an offense under section 1030 of title 18, United States Code.

(2) REQUIREMENTS.—In carrying out this subsection, the Sentencing Commission shall—

(A) ensure that the sentencing guidelines and policy statements reflect the serious nature of the offenses described in paragraph (1), the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses;

(B) consider the following factors and the extent to which the guidelines may or may not account for them—

(i) the potential and actual loss resulting from the offense;

(ii) the level of sophistication and planning involved in the offense;

(iii) whether the offense was committed for purposes of commercial advantage or private financial benefit;

(iv) whether the defendant acted with malicious intent to cause harm in committing the offense;

(v) the extent to which the offense violated the privacy rights of individuals harmed;

(vi) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;

(vii) whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and

(viii) whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person;

(C) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(D) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(E) make any necessary conforming changes to the sentencing guidelines; and

(F) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18, United States Code.

(c) STUDY AND REPORT ON COMPUTER CRIMES.—Not later than May 1, 2003, the United States Sentencing Commission shall submit a brief report to Congress that explains any actions taken by the Sentencing Commission in response to this section and includes any recommendations the Commission may have regarding statutory penalties for offenses under section 1030 of title 18, United States Code.

(d) EMERGENCY DISCLOSURE EXCEPTION.—

(1) [Omitted-Amendatory]

(2) REPORTING OF DISCLOSURES.—A government entity that receives a disclosure under section 2702(b) of title 18, United States Code, shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after the date of enactment of this Act.

[(e)-(j) omitted—Amendatory]

SEC. [226.] *2208.* CYBERSECURITY RECRUITMENT AND RETENTION.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term "appropriate committees of Congress" means the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on

Homeland Security and the Committee on Appropriations of the House of Representatives.

(2) COLLECTIVE BARGAINING AGREEMENT.—The term "collective bargaining agreement" has the meaning given that term in section 7103(a)(8) of title 5, United States Code.

(3) EXCEPTED SERVICE.—The term "excepted service" has the meaning given that term in section 2103 of title 5, United States Code.

(4) PREFERENCE ELIGIBLE.—The term "preference eligible" has the meaning given that term in section 2108 of title 5, United States Code.

(5) QUALIFIED POSITION.—The term "qualified position" means a position, designated by the Secretary for the purpose of this section, in which the incumbent performs, manages, or supervises functions that execute the responsibilities of the Department relating to cybersecurity.

(6) SENIOR EXECUTIVE SERVICE.—The term "Senior Executive Service" has the meaning given that term in section 2101a of title 5, United States Code.

(b) GENERAL AUTHORITY.—

(1) ESTABLISH POSITIONS, APPOINT PERSONNEL, AND FIX RATES OF PAY.—

(A) GENERAL AUTHORITY.—The Secretary may—

(i) establish, as positions in the excepted service, such qualified positions in the Department as the Secretary determines necessary to carry out the responsibilities of the Department relating to cybersecurity, including positions formerly identified as—

(I) senior level positions designated under section 5376 of title 5, United States Code; and

(II) positions in the Senior Executive Service;

(ii) appoint an individual to a qualified position (after taking into consideration the availability of preference eligibles for appointment to the position); and

(iii) subject to the requirements of paragraphs (2) and (3), fix the compensation of an individual for service in a qualified position.

(B) CONSTRUCTION WITH OTHER LAWS.—The authority of the Secretary under this subsection applies without regard to the provisions of any other law relating to the appointment, number, classification, or compensation of employees.

(2) BASIC PAY.—

(A) AUTHORITY TO FIX RATES OF BASIC PAY.—In accordance with this section, the Secretary shall fix the rates of basic pay for any qualified position established under paragraph (1) in relation to the rates of pay provided for employees in comparable positions in the Department of Defense and subject to the same limitations on maximum rates of pay established for such employees by law or regulation.

(B) PREVAILING RATE SYSTEMS.—The Secretary may, consistent with section 5341 of title 5, United States Code, adopt such provisions of that title as provide for prevailing rate systems of basic pay and may apply those provisions

to qualified positions for employees in or under which the Department may employ individuals described by section 5342(a)(2)(A) of that title.

(3) ADDITIONAL COMPENSATION, INCENTIVES, AND ALLOWANCES.—

(A) ADDITIONAL COMPENSATION BASED ON TITLE 5 AUTHORITIES.—The Secretary may provide employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by title 5, United States Code.

(B) ALLOWANCES IN NONFOREIGN AREAS.—An employee in a qualified position whose rate of basic pay is fixed under paragraph (2)(A) shall be eligible for an allowance under section 5941 of title 5, United States Code, on the same basis and to the same extent as if the employee was an employee covered by such section 5941, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

(4) PLAN FOR EXECUTION OF AUTHORITIES.—Not later than 120 days after the date of enactment of this section, the Secretary shall submit a report to the appropriate committees of Congress with a plan for the use of the authorities provided under this subsection.

(5) COLLECTIVE BARGAINING AGREEMENTS.—Nothing in paragraph (1) may be construed to impair the continued effectiveness of a collective bargaining agreement with respect to an office, component, subcomponent, or equivalent of the Department that is a successor to an office, component, subcomponent, or equivalent of the Department covered by the agreement before the succession.

(6) REQUIRED REGULATIONS.—The Secretary, in coordination with the Director of the Office of Personnel Management, shall prescribe regulations for the administration of this section.

(c) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this section, and every year thereafter for 4 years, the Secretary shall submit to the appropriate committees of Congress a detailed report that—

(1) discusses the process used by the Secretary in accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by an individual for a qualified position;

(2) describes—

(A) how the Secretary plans to fulfill the critical need of the Department to recruit and retain employees in qualified positions;

(B) the measures that will be used to measure progress; and

(C) any actions taken during the reporting period to fulfill such critical need;

(3) discusses how the planning and actions taken under paragraph (2) are integrated into the strategic workforce planning of the Department;

(4) provides metrics on actions occurring during the reporting period, including—

(A) the number of employees in qualified positions hired by occupation and grade and level or pay band;

(B) the placement of employees in qualified positions by directorate and office within the Department;

(C) the total number of veterans hired;

(D) the number of separations of employees in qualified positions by occupation and grade and level or pay band;

(E) the number of retirements of employees in qualified positions by occupation and grade and level or pay band; and

(F) the number and amounts of recruitment, relocation, and retention incentives paid to employees in qualified positions by occupation and grade and level or pay band; and

(5) describes the training provided to supervisors of employees in qualified positions at the Department on the use of the new authorities.

(d) THREE-YEAR PROBATIONARY PERIOD.—The probationary period for all employees hired under the authority established in this section shall be 3 years.

(e) INCUMBENTS OF EXISTING COMPETITIVE SERVICE POSITIONS.—

(1) IN GENERAL.—An individual serving in a position on the date of enactment of this section that is selected to be converted to a position in the excepted service under this section shall have the right to refuse such conversion.

(2) SUBSEQUENT CONVERSION.—After the date on which an individual who refuses a conversion under paragraph (1) stops serving in the position selected to be converted, the position may be converted to a position in the excepted service.

(f) STUDY AND REPORT.—Not later than 120 days after the date of enactment of this section, the National Protection and Programs Directorate shall submit a report regarding the availability of, and benefits (including cost savings and security) of using, cybersecurity personnel and facilities outside of the National Capital Region (as defined in section 2674 of title 10, United States Code) to serve the Federal and national need to—

(1) the Subcommittee on Homeland Security of the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Subcommittee on Homeland Security of the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives.

SEC. [227.] *2209.* NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITIONS.—In this section—

(1) the term "cybersecurity risk"—

(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;

(2) the terms "cyber threat indicator" and "defensive measure" have the meanings given those terms in section 102 of the Cybersecurity Act of 2015;

(3) the term "incident" means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;

(4) the term "information sharing and analysis organization" has the meaning given that term in section 212(5);

(5) the term "information system" has the meaning given that term in section 3502(8) of title 44, United States Code; and

(6) the term "sharing" (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each of such terms).

(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 of the Cybersecurity and Infrastructure Security Agency. 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) being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensivemeasures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including the implementationof title I of the Cybersecurity Act of 2015;

(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

(3) coordinating the sharing of information related to cyber threat indicators, defensive measures,cybersecurity risks, and incidents across the Federal Government;

(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;

(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cyber threat indicators, defensivemeasures, cybersecurity risks, and incidents; and

(B) sharing the analysis conducted under subparagraph (A) with Federal and non-Federal entities;

(6) upon request, providing timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurityrisks, and incidents, which may include attribution, mitigation, and remediation;

(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

(A) facilitate information security;

(B) strengthen information systems against cybersecurity risks and incidents; and

(C) sharing cyber threat indicators and defensive measures;

(8) engaging with international partners, in consultation with other appropriate agencies, to—

(A) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and

(B) enhance the security and resilience of global cybersecurity;

(9) sharing cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;

(10) participating, as appropriate, in national exercises run by the Department; and

(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) appropriate representatives of Federal entities, such as—

(i) sector-specific agencies;

(ii) civilian and law enforcement agencies; and

(iii) elements of the intelligence community, as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4));

(B) appropriate representatives of non-Federal entities, such as—

(i) State, local, and tribal governments;

(ii) information sharing and analysis organizations, including information sharing and analysis centers;

(iii) owners and operators of critical information systems; and

(iv) private entities;

(C) components within the Center that carry out cybersecurity and communications activities;

(D) a designated Federal official for operational coordination with and across each sector;

(E) an entity that collaborates with State and local governments on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center; and

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

(2) INCIDENTS.—In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.

(e) PRINCIPLES.—In carrying out the functions under subsection (c), the Center shall ensure—

(1) to the extent practicable, that—

(A) timely, actionable, and relevant cyber threatindicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is shared;

(B) when appropriate, cyber threatindicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;

(C) activities are prioritized and conducted based on the level of risk;

(D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;

(E) continuous, collaborative, and inclusive coordination occurs—

(i) across sectors; and

(ii) with—

(I) sector coordinating councils;

(II) information sharing and analysis organizations; and

(III) other appropriate non-Federal partners;

(F) as appropriate, the Center works to develop and use mechanisms for sharing information related to cyber threat indicators, defensive measures,cybersecurity risks, and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient;

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cyber threat indicators,defensive measures, cybersecurity risks, andincidents; and;

(H) the Center designates an agency contact for non-Federal entities;

(2) that information related to cyber threat indicators, defensive measures, cybersecurityrisks, and incidents is appropriately safeguarded against unauthorized access or disclosure; and

(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons, including by working withthe Privacy Officer appointed under section 222 to ensurethat the Center follows the policies and procedures specifiedin subsections (b) and (d)(5)(C) of section 105 of the CybersecurityAct of 2015.

(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 of the Cybersecurity and Infrastructure Security Agency*.

(2) CERTAIN ASSISTANCE OR INFORMATION.—The provision of certain assistance or information to, or inclusion in the Center of, one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

(g) AUTOMATED INFORMATION SHARING.—

(1) IN GENERAL.—The [Under Secretary appointed under section 103(a)(1)(H)] *Director of the Cybersecurity and Infrastructure Security Agency*, 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 of the Cybersecurity and Infrastructure Security Agency* 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 of the Cybersecurity and Infrastructure Security Agency*, 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 of the Cybersecurity and Infrastructure Security Agency*, for any reason, including if the Secretary determines that such is appropriate for national security.

(2) VOLUNTARY INFORMATION SHARING RELATIONSHIPS.—A voluntary information sharing relationship under this sub-

section may be characterized as an agreement described in this paragraph.

(A) STANDARD AGREEMENT.—For the use of a non-Federal entity, the Center shall make available a standard agreement, consistent with this section, on the Department's website.

(B) NEGOTIATED AGREEMENT.—At the request of a non-Federal entity, and if determined appropriate by the Center, at the sole and unreviewable discretion of the Secretary, acting through the [Under Secretary appointed under section 103(a)(1)(H)] *Director of the Cybersecurity and Infrastructure Security Agency*, the Department shall negotiate a non-standard agreement, consistent with this section.

(C) EXISTING AGREEMENTS.—An agreement between the Center and a non-Federal entity that is entered into before the date of enactment of this subsection, or such an agreement that is in effect before such date, shall be deemed in compliance with the requirements of this subsection, notwithstanding any other provision or requirement of this subsection. An agreement under this subsection shall include the relevant privacy protections as in effect under the Cooperative Research and Development Agreement for Cybersecurity Information Sharing and Collaboration, as of December 31, 2014. Nothing in this subsection may be construed to require a non-Federal entity to enter into either a standard or negotiated agreement to be in compliance with this subsection.

(i) DIRECT REPORTING.—The Secretary shall develop policies and procedures for direct reporting to the Secretary by the Director of the Center regarding significant cybersecurity risks and incidents.

(j) REPORTS ON INTERNATIONAL COOPERATION.—Not later than 180 days after the date of enactment of this subsection, and periodically thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners in accordance with subsection (c)(8).

(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 of the Cybersecurity and Infrastructure Security Agency*, shall—

(1) disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the Center; and

(2) enhance outreach to critical infrastructure owners and operators for purposes of such sharing.

(l) CYBERSECURITY OUTREACH.—

(1) IN GENERAL.—The Secretary may leverage small business development centers to provide assistance to small business concerns by disseminating information on cyber threat indicators, defense measures, cybersecurity risks, incidents, analyses, and warnings to help small business concerns in developing or

enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees.

(2) DEFINITIONS.—For purposes of this subsection, the terms "small business concern" and "small business development center" have the meaning given such terms, respectively, under section 3 of the Small Business Act.

(m) COORDINATED VULNERABILITY DISCLOSURE.—The Secretary, in coordination with industry and other stakeholders, may develop and adhere to Department policies and procedures for coordinating vulnerability disclosures.

SEC. [228.] *2210.* CYBERSECURITY PLANS.

(a) DEFINITIONS.—In this section—

(1) the term "agency information system" means an information system used or operated by an agency or by another entity on behalf of an agency;

(2) the terms "cybersecurity risk" and "information system" have the meanings given those terms in [section 227] *section 2209*;

(3) the term "intelligence community" has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and

(4) the term "national security system" has the meaning given the term in section 11103 of title 40, United States Code.

(b) INTRUSION ASSESSMENT PLAN.—

(1) REQUIREMENT.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall—

(A) develop and implement an intrusion assessment plan to proactively detect, identify, and remove intruders in agency information systems on a routine basis; and

(B) update such plan as necessary.

(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(c) CYBER INCIDENT RESPONSE PLAN.—The [Under Secretary appointed under section 103(a)(1)(H)] *Director of the Cybersecurity and Infrastructure Security Agency* shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 212(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) NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (c), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

SEC. [228A.] *2211.* CYBERSECURITY STRATEGY.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this section, the Secretary shall develop a departmental

strategy to carry out cybersecurity responsibilities as set forth in law.

(b) CONTENTS.—The strategy required under subsection (a) shall include the following:

(1) Strategic and operational goals and priorities to successfully execute the full range of the Secretary's cybersecurity responsibilities.

(2) Information on the programs, policies, and activities that are required to successfully execute the full range of the Secretary's cybersecurity responsibilities, including programs, policies, and activities in furtherance of the following:

(A) Cybersecurity functions set forth in the section 227 (relating to the national cybersecurity and communications integration center).

(B) Cybersecurity investigations capabilities.

(C) Cybersecurity research and development.

(D) Engagement with international cybersecurity partners.

(c) CONSIDERATIONS.—In developing the strategy required under subsection (a), the Secretary shall—

(1) consider—

(A) the cybersecurity strategy for the Homeland Security Enterprise published by the Secretary in November 2011;

(B) the Department of Homeland Security Fiscal Years 2014–2018 Strategic Plan; and

(C) the most recent Quadrennial Homeland Security Review issued pursuant to section 707; and

(2) include information on the roles and responsibilities of components and offices of the Department, to the extent practicable, to carry out such strategy.

(d) IMPLEMENTATION PLAN.—Not later than 90 days after the development of the strategy required under subsection (a), the Secretary shall issue an implementation plan for the strategy that includes the following:

(1) Strategic objectives and corresponding tasks.

(2) Projected timelines and costs for such tasks.

(3) Metrics to evaluate performance of such tasks.

(e) CONGRESSIONAL OVERSIGHT.—The Secretary shall submit to Congress for assessment the following:

(1) A copy of the strategy required under subsection (a) upon issuance.

(2) A copy of the implementation plan required under subsection (d) upon issuance, together with detailed information on any associated legislative or budgetary proposals.

(f) CLASSIFIED INFORMATION.—The strategy required under subsection (a) shall be in an unclassified form but may contain a classified annex.

(g) RULE OF CONSTRUCTION.—Nothing in this section may be construed as permitting the Department to engage in monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

(h) DEFINITION.—In this section, the term "Homeland Security Enterprise" means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State,

local, and tribal government officials, private sector representatives, academics, and other policy experts.

SEC. [229.] *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)), owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.

SEC. [210E.] *2214.* NATIONAL ASSET DATABASE.

(a) ESTABLISHMENT.—

(1) NATIONAL ASSET DATABASE.—The Secretary shall establish and maintain a national database of each system or asset that—

(A) the Secretary, in consultation with appropriate homeland security officials of the States, determines to be vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States, any State, or any local government; or

(B) the Secretary determines is appropriate for inclusion in the database.

(2) PRIORITIZED CRITICAL INFRASTRUCTURE LIST.—In accordance with Homeland Security Presidential Directive–7, as in effect on January 1, 2007, the Secretary shall establish and maintain a single classified prioritized list of systems and assets included in the database under paragraph (1) that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects.

(b) USE OF DATABASE.—The Secretary shall use the database established under subsection (a)(1) in the development and implementation of Department plans and programs as appropriate.

(c) MAINTENANCE OF DATABASE.—

(1) IN GENERAL.—The Secretary shall maintain and annually update the database established under subsection (a)(1) and the list established under subsection (a)(2), including—

(A) establishing data collection guidelines and providing such guidelines to the appropriate homeland security official of each State;

(B) regularly reviewing the guidelines established under subparagraph (A), including by consulting with the appropriate homeland security officials of States, to solicit feedback about the guidelines, as appropriate;

(C) after providing the homeland security official of a State with the guidelines under subparagraph (A), allowing the official a reasonable amount of time to submit to the Secretary any data submissions recommended by the official for inclusion in the database established under subsection (a)(1);

(D) examining the contents and identifying any submissions made by such an official that are described incor-

rectly or that do not meet the guidelines established under subparagraph (A); and

(E) providing to the appropriate homeland security official of each relevant State a list of submissions identified under subparagraph (D) for review and possible correction before the Secretary finalizes the decision of which submissions will be included in the database established under subsection (a)(1).

(2) ORGANIZATION OF INFORMATION IN DATABASE.—The Secretary shall organize the contents of the database established under subsection (a)(1) and the list established under subsection (a)(2) as the Secretary determines is appropriate. Any organizational structure of such contents shall include the categorization of the contents—

(A) according to the sectors listed in National Infrastructure Protection Plan developed pursuant to Homeland Security Presidential Directive–7; and

(B) by the State and county of their location.

(3) PRIVATE SECTOR INTEGRATION.—The Secretary shall identify and evaluate methods, including the Department's Protected Critical Infrastructure Information Program, to acquire relevant private sector information for the purpose of using that information to generate any database or list, including the database established under subsection (a)(1) and the list established under subsection (a)(2).

(4) RETENTION OF CLASSIFICATION.—The classification of information required to be provided to Congress, the Department, or any other department or agency under this section by a sector-specific agency, including the assignment of a level of classification of such information, shall be binding on Congress, the Department, and that other Federal agency.

(d) REPORTS.—

(1) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the database established under subsection (a)(1) and the list established under subsection (a)(2).

(2) CONTENTS OF REPORT.—Each such report shall include the following:

(A) The name, location, and sector classification of each of the systems and assets on the list established under subsection (a)(2).

(B) The name, location, and sector classification of each of the systems and assets on such list that are determined by the Secretary to be most at risk to terrorism.

(C) Any significant challenges in compiling the list of the systems and assets included on such list or in the database established under subsection (a)(1).

(D) Any significant changes from the preceding report in the systems and assets included on such list or in such database.

(E) If appropriate, the extent to which such database and such list have been used, individually or jointly, for allocating funds by the Federal Government to prevent, reduce, mitigate, or respond to acts of terrorism.

(F) The amount of coordination between the Department and the private sector, through any entity of the Department that meets with representatives of private sector industries for purposes of such coordination, for the purpose of ensuring the accuracy of such database and such list.

(G) Any other information the Secretary deems relevant.

(3) CLASSIFIED INFORMATION.—The report shall be submitted in unclassified form but may contain a classified annex.

(e) 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) NATIONAL INFRASTRUCTURE PROTECTION CONSORTIUM.—The Secretary may establish a consortium to be known as the "National Infrastructure Protection Consortium". The Consortium may advise the Secretary on the best way to identify, generate, organize, and maintain any database or list of systems and assets established by the Secretary, including the database established under subsection (a)(1) and the list established under subsection (a)(2). If the Secretary establishes the National Infrastructure Protection Consortium, the Consortium may—

(1) be composed of national laboratories, Federal agencies, State and local homeland security organizations, academic institutions, or national Centers of Excellence that have demonstrated experience working with and identifying critical infrastructure and key resources; and

(2) provide input to the Secretary on any request pertaining to the contents of such database or such list.

SEC. [230.] *2213.* FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.

(a) DEFINITIONS.—In this section—

(1) the term "agency" has the meaning given the term in section 3502 of title 44, United States Code;

(2) the term "agency information" means information collected or maintained by or on behalf of an agency;

(3) the term "agency information system" has the meaning given the term in section 228; and

(4) the terms "cybersecurity risk" and "information system" have the meanings given those terms in section 227.

(b) REQUIREMENT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling

to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

(2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

(c) ACTIVITIES.—In carrying out subsection (b), the Secretary—

(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with subsection (b);

(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and noncommercial technologies and detection technologies beyond signature-based detection, and acquire, test, and deploy such technologies when appropriate;

(5) shall establish a pilot through which the Secretary may acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4); and

(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note).

(d) PRINCIPLES.—In carrying out subsection (b), the Secretary shall ensure that—

(1) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(2) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

(3) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

(4) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

(e) PRIVATE ENTITIES.—

(1) CONDITIONS.—A private entity described in subsection (c)(2) may not—

(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity other than the Department or the agency that disclosed the information under subsection (c)(1), including personal information of a specific individual or information that identifies a specific individual not directly related to a cybersecurity risk; or

(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

(2) LIMITATION ON LIABILITY.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

(3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

(f) PRIVACY OFFICER REVIEW.—Not later than 1 year after the date of enactment of this section, the Privacy Officer appointed under section 222, in consultation with the Attorney General, shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable privacy laws, including those governing the acquisition, interception, retention, use, and disclosure of communications.

Subtitle B—Critical Infrastructure Information

SEC. [211.] *2221.* SHORT TITLE.

This subtitle may be cited as the "Critical Infrastructure Information Act of 2002".

SEC. [212.] *2222.* DEFINITIONS.

In this subtitle:

(1) AGENCY.—The term "agency" has the meaning given it in section 551 of title 5, United States Code.

(2) COVERED FEDERAL AGENCY.—The term "covered Federal agency" means the Department of Homeland Security.

(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term "critical infrastructure information" means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(4) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.—The term "critical infrastructure protection program" means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.

(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "Information Sharing and Analysis Organization" means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(6) PROTECTED SYSTEM.—The term "protected system"—

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element

thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(7) VOLUNTARY.—

(A) IN GENERAL.—The term "voluntary", in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency's exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) EXCLUSIONS.—The term "voluntary"—

(i) in the case of any action brought under the securities laws as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))—

(I) does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(I)); and

(II) with respect to the submittal of critical infrastructure information, does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and

(ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

(8) CYBERSECURITY RISK; INCIDENT.—The terms "cybersecurity risk" and "incident" have the meanings given those terms in section 227.

SEC. [213.] *2223.* DESIGNATION OF CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.

A critical infrastructure protection program may be designated as such by one of the following:

(1) The President.

(2) The Secretary of Homeland Security.

SEC. [214.] *2224.* PROTECTION OF VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.

(a) PROTECTION.—

(1) IN GENERAL.—Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)—

(A) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);

(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;

(C) shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;

(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this subtitle, except—

(i) in furtherance of an investigation or the prosecution of a criminal act; or

(ii) when disclosure of the information would be—

(I) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

(E) shall not, if provided to a State or local government or government agency—

(i) be made available pursuant to any State or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or

(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act; and

(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

(2) EXPRESS STATEMENT.—For purposes of paragraph (1), the term "express statement", with respect to information or records, means—

(A) in the case of written information or records, a written marking on the information or records substantially similar to the following: "This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002."; or

(B) in the case of oral information, a similar written statement submitted within a reasonable period following the oral communication.

(b) LIMITATION.—No communication of critical infrastructure information to a covered Federal agency made pursuant to this subtitle shall be considered to be an action subject to the requirements of the Federal Advisory Committee Act (5 U.S.C. App. 2).

(c) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law. For purposes of this section a permissible use of independently obtained information includes the disclosure of such information under section 2302(b)(8) of title 5, United States Code.

(d) TREATMENT OF VOLUNTARY SUBMITTAL OF INFORMATION.—The voluntary submittal to the Government of information or records that are protected from disclosure by this subtitle shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other provision of law.

(e) PROCEDURES.—

(1) IN GENERAL.—The Secretary of the Department of Homeland Security shall, in consultation with appropriate representatives of the National Security Council and the Office of Science and Technology Policy, establish uniform procedures for the receipt, care, and storage by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government. The procedures shall be established not later than 90 days after the date of the enactment of this subtitle.

(2) ELEMENTS.—The procedures established under paragraph (1) shall include mechanisms regarding—

(A) the acknowledgement of receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government;

(B) the maintenance of the identification of such information as voluntarily submitted to the Government for purposes of and subject to the provisions of this subtitle;

(C) the care and storage of such information; and

(D) the protection and maintenance of the confidentiality of such information so as to permit the sharing of such information within the Federal Government and with State and local governments, and the issuance of notices and warnings related to the protection of critical infrastructure and protected systems, in such manner as to protect from public disclosure the identity of the submitting person or entity, or information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is otherwise not appropriately in the public domain.

(f) PENALTIES.—Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this subtitle coming to him in the course of this employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States

Code, imprisoned not more than 1 year, or both, and shall be removed from office or employment.

(g) AUTHORITY TO ISSUE WARNINGS.—The Federal Government may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the Federal Government shall take appropriate actions to protect from disclosure—

(1) the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning; or

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(h) AUTHORITY TO DELEGATE.—The President may delegate authority to a critical infrastructure protection program, designated under section 213, to enter into a voluntary agreement to promote critical infrastructure security, including with any Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 708 of the Defense Production Act of 1950 (50 U.S.C. App. 2158).

SEC. [215.] *2225.* NO PRIVATE RIGHT OF ACTION.

Nothing in this subtitle may be construed to create a private right of action for enforcement of any provision of this Act.

TITLE 5, UNITED STATES CODE

* * * * * * *

PART III—EMPLOYEES

* * * * * * *

SUBPART D—PAY AND ALLOWANCES

* * * * * * *

CHAPTER 53—PAY RATES AND SYSTEMS

* * * * * * *

SUBCHAPTER II—EXECUTIVE SCHEDULE PAY RATES

§ 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:

Solicitor General of the United States.

Under Secretary of Commerce, Under Secretary of Commerce for Economic Affairs, Under Secretary of Commerce for Export Administration, and Under Secretary of Commerce for Travel and Tourism.

Under Secretaries of State (6).

Under Secretaries of the Treasury (3).

Administrator of General Services.

Administrator of the Small Business Administration.
Deputy Administrator, Agency for International Development.
Chairman of the Merit Systems Protection Board.
Chairman, Federal Communications Commission.
Chairman, Board of Directors, Federal Deposit Insurance Corporation.
Chairman, Federal Energy Regulatory Commission.
Chairman, Federal Trade Commission.
Chairman, Surface Transportation Board.
Chairman, National Labor Relations Board.
Chairman, Securities and Exchange Commission.
Chairman, National Mediation Board.
Chairman, Railroad Retirement Board.
Chairman, Federal Maritime Commission.
Comptroller of the Currency.
Commissioner of Internal Revenue.
Under Secretary of Defense for Policy.
Under Secretary of Defense (Comptroller).
Under Secretary of Defense for Personnel and Readiness.
Under Secretary of Defense for Intelligence.
Deputy Chief Management Officer of the Department of Defense.
Under Secretary of the Air Force.
Under Secretary of the Army.
Under Secretary of the Navy.
Deputy Administrator of the National Aeronautics and Space Administration.
Deputy Director of the Central Intelligence Agency.
Director of the Office of Emergency Planning.
Director of the Peace Corps.
Deputy Director, National Science Foundation.
President of the Export-Import Bank of Washington.
Members, Nuclear Regulatory Commission.
Members, Defense Nuclear Facilities Safety Board.
Director of the Federal Bureau of Investigation, Department of Justice.
Administrator of the National Highway Traffic Safety Administration.
Administrator of the Federal Motor Carrier Safety Administration.
Administrator, Federal Railroad Administration.
Chairman, National Transportation Safety Board.
Chairman of the National Endowment for the Arts the incumbent of which also serves as Chairman of the National Council on the Arts.
Chairman of the National Endowment for the Humanities.
Director of the Federal Mediation and Conciliation Service.
President, Overseas Private Investment Corporation.
Chairman, Postal Regulatory Commission.
Chairman, Occupational Safety and Health Review Commission.
Governor of the Farm Credit Administration.
Chairman, Equal Employment Opportunity Commission.
Chairman, Consumer Product Safety Commission.
Under Secretaries of Energy (3).
Chairman, Commodity Futures Trading Commission.
Deputy United States Trade Representatives (3).

Chief Agricultural Negotiator, Office of the United States Trade Representative.

Chief Innovation and Intellectual Property Negotiator, Office of the United States Trade Representative.

Chairman, United States International Trade Commission.

Under Secretary of Commerce for Oceans and Atmosphere, the incumbent of which also serves as Administrator of the National Oceanic and Atmospheric Administration.

Under Secretary of Commerce for Standards and Technology, who also serves as Director of the National Institute of Standards and Technology.

Associate Attorney General.

Chairman, Federal Mine Safety and Health Review Commission.

Chairman, National Credit Union Administration Board.

Deputy Director of the Office of Personnel Management.

Under Secretary of Agriculture for Farm and Foreign Agricultural Services.

Under Secretary of Agriculture for Food, Nutrition, and Consumer Services.

Under Secretary of Agriculture for Natural Resources and Environment.

Under Secretary of Agriculture for Research, Education, and Economics.

Under Secretary of Agriculture for Food Safety.

Under Secretary of Agriculture for Marketing and Regulatory Programs.

Director, Institute for Scientific and Technological Cooperation.

Under Secretary of Agriculture for Rural Development.

Administrator, Maritime Administration.

Executive Director Property Review Board.

Deputy Administrator of the Environmental Protection Agency.

Archivist of the United States.

Executive Director, Federal Retirement Thrift Investment Board.

Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics.

Director, Trade and Development Agency.

Under Secretary for Health, Department of Veterans Affairs.

Under Secretary for Benefits, Department of Veterans Affairs.

Under Secretary for Memorial Affairs, Department of Veterans Affairs.

Under Secretaries, Department of Homeland Security.

Director, Cybersecurity and Infrastructure Security Agency.

Director of the Bureau of Citizenship and Immigration Services.

Director of the Office of Government Ethics.

Administrator for Federal Procurement Policy.

Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget.

Director of the Office of Thrift Supervision.

Chairperson of the Federal Housing Finance Board.

Executive Secretary, National Space Council.

Controller, Office of Federal Financial Management, Office of Management and Budget.

Administrator, Office of the Assistant Secretary for Research and Technology of the Department of Transportation.

Deputy Director for Demand Reduction, Office of National Drug Control Policy.

Deputy Director for Supply Reduction, Office of National Drug Control Policy.

Deputy Director for State and Local Affairs, Office of National Drug Control Policy.

Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office.

Register of Copyrights.

Commissioner of U.S. Customs and Border Protection, Department of Homeland Security.

Under Secretary of Education

Administrator of the Centers for Medicare & Medicaid Services.

Administrator of the Office of Electronic Government.

Administrator, Pipeline and Hazardous Materials Safety Administration.

Director, Pension Benefit Guaranty Corporation.

Deputy Administrators, Federal Emergency Management Agency.

Chief Executive Officer, International Clean Energy Foundation.

Independent Member of the Financial Stability Oversight Council (1).

Director of the Office of Financial Research.

* * * * * * *

COMMITTEE CORRESPONDENCE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC, December 8, 2017.

Hon. MICHAEL T. MCCAUL,
Chairman, Committee on Homeland Security,
Washington, DC.

DEAR CHAIRMAN MCCAUL: I am writing to notify you that the Committee on Energy and Commerce will forgo action on H.R. 3359, Cybersecurity and Infrastructure Security Agency Act of 2017, so that it may proceed expeditiously to the House floor for consideration. This is done with the understanding that the Committee's jurisdictional interests over this and similar legislation are in no way diminished or altered. In addition, the Committee reserves the right to seek conferees on H.R. 3359 and expects your support when such a request is made.

Please include a copy of this letter outlining our mutual understanding with respect to H.R. 3359 in the *Congressional Record* during consideration of the bill on the House floor.

Sincerely,

GREG WARDEN,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, December 7, 2017.

Hon. GREG WALDEN,
Chairman, Committee on Energy and Commerce,
Washington, DC.

DEAR CHAIRMAN WALDEN: Thank you for your letter regarding H.R. 3359, the "Cybersecurity and Infrastructure Security Agency Act of 2017." I appreciate your support in bringing this legislation before the House of Representatives, and accordingly, understand that the Committee on Energy and Commerce will forego further consideration of the bill.

The Committee on Homeland Security concurs with the mutual understanding that by foregoing consideration of this bill at this time, the Committee on Energy and Commerce does not waive any jurisdiction over the subject matter contained in this bill or similar legislation in the future. In addition, should a conference on this bill be necessary, I would support your request to have the Committee represented on the conference committee.

I will insert copies of this exchange in the report on the bill and in the *Congressional Record* during consideration of this bill on the House floor. I thank you for your cooperation in this matter.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC, December 7, 2017.

Hon. MICHAEL T. MCCAUL,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: I write concerning H.R. 3359, the "Cybersecurity and Infrastructure Security Agency Act of 2017." This bill would amend the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security and contains provisions within the jurisdiction of the Committee on Oversight and Government Reform. As a result of your having consulted with me concerning the provisions of the bill that fall within our Rule X jurisdiction, I agree to forgo consideration of the bill, so the bill may proceed expeditiously to the House floor.

The Committee takes this action with our mutual understanding that by foregoing consideration of H.R. 3359 at this time we do not waive any jurisdiction over the subject matter contained in this or similar legislation, and we will be appropriately consulted and involved as the bill or similar legislation moves forward so that we may address any remaining issues that fall within our Rule X jurisdiction. Further, I request your support for the appointment of conferees from the Committee on Oversight and Government Reform during any House-Senate conference convened on this or related legislation.

Finally, I would appreciate your response to this letter confirming this understanding and ask that a copy of our exchange of letters on this matter be included in the bill report filed by the Committee on Homeland Security, as well as in the *Congressional Record* during floor consideration thereof.

Sincerely,

TREY GOWDY,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC, December 7, 2017.

Hon. TREY GOWDY,
Chairman, Committee on Oversight and Government Reform,
Washington, DC.

DEAR CHAIRMAN GOWDY: Thank you for your letter regarding H.R. 3359, the "Cybersecurity and Infrastructure Security Agency Act of 2017." I appreciate your support in bringing this legislation before the House of Representatives, and accordingly, understand that the Committee on Oversight and Government Reform will forego further consideration of the bill.

The Committee on Homeland Security concurs with the mutual understanding that by foregoing consideration of this bill at this time, the Committee on Oversight and Government Reform does not waive any jurisdiction over the subject matter contained in this bill or similar legislation in the future. In addition, should a conference on this bill be necessary, I would support your request to have the Committee represented on the conference committee.

I will insert copies of this exchange in the report on the bill and in the *Congressional Record* during consideration of this bill on the House floor. I thank you for your cooperation in this matter.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
HOUSE OF REPRESENTATIVES,
Washington, DC, December 7, 2017.

Hon. MICHAEL T. MCCAUL,
Chairman, Committee on Homeland Security,
Washington, DC.

DEAR CHAIRMAN MCCAUL: I write concerning H.R. 3359, the *Cybersecurity and Infrastructure Security Agency Act of 2017.* This legislation includes matters that fall within the Rule X jurisdiction of the Committee on Transportation and Infrastructure.

I recognize and appreciate your desire to bring this legislation before the House of Representatives in an expeditious manner, and accordingly, the Committee on Transportation and Infrastructure will forego action on the bill. However, this is conditional on our mutual understanding that foregoing consideration of the bill does not prejudice the Committee with respect to the appointment of conferees or to any future jurisdictional claim over the subject matters contained in the bill or similar legislation that fall within the

Committee's Rule X jurisdiction. Further, this is conditional on our understanding that mutually agreed upon changes to the legislation will be incorporated into the bill prior to floor consideration. Lastly, should a conference on the bill be necessary, I request your support for the appointment of conferees from the Committee on Transportation and Infrastructure during any House-Senate conference convened on this or related legislation.

I would ask that a copy of this letter and your response acknowledging our jurisdictional interest as well as the mutually agreed upon changes to be incorporated into the bill be included in the Congressional Record during consideration of the measure on the House floor, to memorialize our understanding.

I look forward to working with the Committee on Homeland Security as the bill moves through the legislative process.

Sincerely,

BILL SHUSTER,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, December 7, 2017.

Hon. BILL SHUSTER,
Chairman, Committee on Transportation and Infrastructure, House of Representatives, Washington, DC.

DEAR CHAIRMAN SHUSTER: Thank you for your letter regarding H.R. 3359, the "Cybersecurity and Infrastructure Security Agency Act of 2017." I appreciate your support in bringing this legislation before the House of Representatives, and accordingly, understand that the Committee on Transportation and Infrastructure will forego further consideration of the bill.

The Committee on Homeland Security concurs with the mutual understanding that by foregoing consideration of this bill at this time, the Committee on Transportation and Infrastructure does not waive any jurisdiction over the subject matter contained in this bill or similar legislation in the future. In addition, should a conference on this bill be necessary, I would support your request to have the Committee represented on the conference committee. The Committee on Homeland Security will include mutually agreed upon changes to the legislation into the bill prior to floor consideration.

I will insert copies of this exchange in the report on the bill and in the *Congressional Record* during consideration of this bill on the House floor. I thank you for your cooperation in this matter.

Sincerely,

MICHAEL T. MCCAUL
Chairman.

○