Calendar No. 698

111TH CONGRESS
2D SESSION

S. 3480

[Report No. 111–368]

To amend the Homeland Security Act of 2002 and other laws to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

IN THE SENATE OF THE UNITED STATES

JUNE 10, 2010

Mr. LIEBERMAN (for himself, Ms. COLLINS, and Mr. CARPER) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 15, 2010

Reported by Mr. LIEBERMAN, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

To amend the Homeland Security Act of 2002 and other laws to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Protecting Cyberspace as a National Asset Act of 2010''.

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

SEC. 3. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

(B) the Committee on Homeland Security of the House of Representatives;

(C) the Committee on Oversight and Government Reform of the House of Representatives; and

(D) any other congressional committee with jurisdiction over the particular matter.

(2) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given that term in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).

(3) CYBERSPACE.—The term ''cyberspace'' means the interdependent network of information infrastructure, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

(4) DIRECTOR.—The term ''Director'' means the Director of Cyberspace Policy established under section 101.

(5) FEDERAL AGENCY.—The term ''Federal agency''—

(A) means any executive department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

(B) does not include the governments of the District of Columbia and of the territories and possessions of the United States and their various subdivisions.

(6) FEDERAL INFORMATION INFRASTRUCTURE.—The term ''Federal information infrastructure''—

(A) means information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, any Federal agency, including information systems used or operated by another entity on behalf of a Federal agency; and

(B) does not include—

(i) a national security system; or

(ii) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community.

(7) INCIDENT.—The term ''incident'' means an occurrence that—

(A) actually or potentially jeopardizes—

(i) the information security of information infrastructure; or

(ii) the information that information infrastructure processes, stores, receives, or transmits; or

(B) constitutes a violation or threat of violation of security policies, security procedures, or acceptable use policies applicable to information infrastructure.

(8) INFORMATION INFRASTRUCTURE.—The term ''information infrastructure'' means the underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including programmable electronic devices and communications networks and any associated hardware, software, or data.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, by ensuring timely and reliable access to and use of information.

(10) INFORMATION TECHNOLOGY.—The term ''information technology'' has the meaning given that term in section 11101 of title 40, United States Code.

(11) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given that term under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(12) KEY RESOURCES.—The term ''key resources'' has the meaning given that term in section

~~2 of the Homeland Security Act of 2002 (6 U.S.C. 101).~~

~~(13) NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.—The term "National Center for Cybersecurity and Communications" means the National Center for Cybersecurity and Communications established under section 242(a) of the Homeland Security Act of 2002, as added by this Act.~~

~~(14) NATIONAL INFORMATION INFRASTRUCTURE.—The term "national information infrastructure" means information infrastructure—~~

~~(A)(i) that is owned, operated, or controlled within or from the United States; or~~

~~(ii) if located outside the United States, the disruption of which could result in national or regional catastrophic damage in the United States; and~~

~~(B) that is not owned, operated, controlled, or licensed for use by a Federal agency.~~

~~(15) NATIONAL SECURITY SYSTEM.—The term "national security system" has the meaning given that term in section 3551 of title 44, United States Code, as added by this Act.~~

(16) NATIONAL STRATEGY.—The term ''National Strategy'' means the national strategy to increase the security and resiliency of cyberspace developed under section 101(a)(1).

(17) OFFICE.—The term ''Office'' means the Office of Cyberspace Policy established under section 101.

(18) RISK.—The term ''risk'' means the potential for an unwanted outcome resulting from an incident, as determined by the likelihood of the occurrence of the incident and the associated consequences, including potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident.

(19) RISK-BASED SECURITY.—The term ''risk-based security'' has the meaning given that term in section 3551 of title 44, United States Code, as added by this Act.

TITLE I—OFFICE OF CYBERSPACE POLICY

SEC. 101. ESTABLISHMENT OF THE OFFICE OF CYBERSPACE POLICY.

(a) ESTABLISHMENT OF OFFICE.—There is established in the Executive Office of the President an Office of Cyberspace Policy which shall—

(1) develop, not later than 1 year after the date of enactment of this Act, and update as needed, but not less frequently than once every 2 years, a national strategy to increase the security and resiliency of cyberspace, that includes goals and objectives relating to—

(A) computer network operations, including offensive activities, defensive activities, and other activities;

(B) information assurance;

(C) protection of critical infrastructure and key resources;

(D) research and development priorities;

(E) law enforcement;

(F) diplomacy;

(G) homeland security; and

(H) military and intelligence activities;

(2) oversee, coordinate, and integrate all policies and activities of the Federal Government across all instruments of national power relating to ensuring the security and resiliency of cyberspace, including—

(A) diplomatic, economic, military, intelligence, homeland security, and law enforcement policies and activities within and among Federal agencies; and

(B) offensive activities, defensive activities, and other policies and activities necessary to ensure effective capabilities to operate in cyberspace;

(3) ensure that all Federal agencies comply with appropriate guidelines, policies, and directives from the Department of Homeland Security, other Federal agencies with responsibilities relating to cyberspace security or resiliency, and the National Center for Cybersecurity and Communications; and

(4) ensure that Federal agencies have access to, receive, and appropriately disseminate law enforcement information, intelligence information, terrorism information, and any other information (including information relating to incidents provided under subsections (a)(4) and (c) of section 246 of the Home-

land Security Act of 2002, as added by this Act) relevant to—

(A) the security of the Federal information infrastructure or the national information infrastructure; and

(B) the security of—

(i) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community; or

(ii) a national security system.

(b) DIRECTOR OF CYBERSPACE POLICY.—

(1) IN GENERAL.—There shall be a Director of Cyberspace Policy, who shall be the head of the Office.

(2) EXECUTIVE SCHEDULE POSITION.—Section 5312 of title 5, United States Code, is amended by adding at the end the following:

"Director of Cyberspace Policy.".

SEC. 102. APPOINTMENT AND RESPONSIBILITIES OF THE DIRECTOR.

(a) APPOINTMENT.—

(1) IN GENERAL.—The Director shall be appointed by the President, by and with the advice and consent of the Senate.

(2) QUALIFICATIONS.—The President shall appoint the Director from among individuals who have demonstrated ability and knowledge in information technology, cybersecurity, and the operations, security, and resiliency of communications networks.

(3) PROHIBITION.—No person shall serve as Director while serving in any other position in the Federal Government.

(b) RESPONSIBILITIES.—The Director shall—

(1) advise the President regarding the establishment of policies, goals, objectives, and priorities for securing the information infrastructure of the Nation;

(2) advise the President and other entities within the Executive Office of the President regarding mechanisms to build, and improve the resiliency and efficiency of, the information and communication industry of the Nation, in collaboration with the private sector, while promoting national economic interests;

(3) work with Federal agencies to—

(A) oversee, coordinate, and integrate the implementation of the National Strategy, including coordination with—

(i) the Department of Homeland Security;

(ii) the Department of Defense;

(iii) the Department of Commerce;

(iv) the Department of State;

(v) the Department of Justice;

(vi) the Department of Energy;

(vii) through the Director of National Intelligence, the intelligence community; and

(viii) and any other Federal agency with responsibilities relating to the National Strategy; and

(B) resolve any disputes that arise between Federal agencies relating to the National Strategy or other matters within the responsibility of the Office;

(4) if the policies or activities of a Federal agency are not in compliance with the responsibilities of the Federal agency under the National Strategy—

(A) notify the Federal agency;

(B) transmit a copy of each notification under subparagraph (A) to the President and the appropriate congressional committees; and

(C) coordinate the efforts to bring the Federal agency into compliance;

(5) ensure the adequacy of protections for privacy and civil liberties in carrying out the responsibilities of the Director under this title, including through consultation with the Privacy and Civil Liberties Oversight Board established under section 1061 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee);

(6) upon reasonable request, appear before any duly constituted committees of the Senate or of the House of Representatives;

(7) recommend to the Office of Management and Budget or the head of a Federal agency actions (including requests to Congress relating to the reprogramming of funds) that the Director determines are necessary to ensure risk-based security of—

(A) the Federal information infrastructure;

(B) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense,

a military department, or another element of the intelligence community; or

(C) a national security system;

(8) advise the Administrator of the Office of E-Government and Information Technology and the Administrator of the Office of Information and Regulatory Affairs on the development, and oversee the implementation, of policies, principles, standards, guidelines, and budget priorities for information technology functions and activities of the Federal Government;

(9) coordinate and ensure, to the maximum extent practicable, that the standards and guidelines developed for national security systems and the standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) are complementary and unified;

(10) in consultation with the Administrator of the Office of Information and Regulatory Affairs, coordinate efforts of Federal agencies relating to the development of regulations, rules, requirements, or other actions applicable to the national information infrastructure to ensure, to the maximum extent practicable, that the efforts are complementary;

(11) coordinate the activities of the Office of Science and Technology Policy, the National Economic Council, the Office of Management and Budget, the National Security Council, the Homeland Security Council, and the United States Trade Representative related to the National Strategy and other matters within the purview of the Office; and

(12) as assigned by the President, other duties relating to the security and resiliency of cyberspace.

SEC. 103. PROHIBITION ON POLITICAL CAMPAIGNING.

Section 7323(b)(2)(B) of title 5, United States Code, is amended—

(1) in clause (i), by striking "or" at the end;

(2) in clause (ii), by striking the period at the end and inserting "; or"; and

(3) by adding at the end the following:

"(iii) notwithstanding the exception under subparagraph (A) (relating to an appointment made by the President, by and with the advice and consent of the Senate), the Director of Cyberspace Policy.".

SEC. 104. REVIEW OF FEDERAL AGENCY BUDGET REQUESTS RELATING TO THE NATIONAL STRATEGY.

(a) IN GENERAL.—For each fiscal year, the head of each Federal agency shall transmit to the Director a copy of any portion of the budget of the Federal agency intended to implement the National Strategy at the same time as that budget request is submitted to the Office of Management and Budget in the preparation of the budget of the President submitted to Congress under section 1105 (a) of title 31, United States Code.

(b) TIMELY SUBMISSIONS.—The head of each Federal agency shall ensure the timely development and submission to the Director of each proposed budget under this section, in such format as may be designated by the Director with the concurrence of the Director of the Office of Management and Budget.

(c) ADEQUACY OF THE PROPOSED BUDGET REQUESTS.—With the assistance of, and in coordination with, the Office of E-Government and Information Technology and the National Center for Cybersecurity and Communications, the Director shall review each budget submission to assess the adequacy of the proposed request with regard to implementation of the National Strategy.

(d) INADEQUATE BUDGET REQUESTS.—If the Director concludes that a budget request submitted under sub-

section (a) is inadequate, in whole or in part, to implement the objectives of the National Strategy, the Director shall submit to the Director of the Office of Management and Budget and the head of the Federal agency submitting the budget request a written description of funding levels and specific initiatives that would, in the determination of the Director, make the request adequate.

SEC. 105. ACCESS TO INTELLIGENCE.

The Director shall have access to law enforcement information, intelligence information, terrorism information, and any other information (including information relating to incidents provided under subsections (a)(4) and (c) of section 246 of the Homeland Security Act of 2002, as added by this Act) that is obtained by, or in the possession of, any Federal agency that the Director determines relevant to the security of—

(1) the Federal information infrastructure;

(2) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community;

(3) a national security system; or

(4) national information infrastructure.

SEC. 106. CONSULTATION.

(a) IN GENERAL.—The Director may consult and obtain recommendations from, as needed, such Presidential and other advisory entities as the Director determines will assist in carrying out the mission of the Office, including—

(1) the National Security Telecommunications Advisory Committee;

(2) the National Infrastructure Advisory Council;

(3) the Privacy and Civil Liberties Oversight Board;

(4) the President's Intelligence Advisory Board;

(5) the Critical Infrastructure Partnership Advisory Council; and

(6) the National Cybersecurity Advisory Council established under section 239 of the Homeland Security Act of 2002, as added by this Act.

(b) NATIONAL STRATEGY.—In developing and updating the National Strategy the Director shall consult with the National Cybersecurity Advisory Council and, as appropriate, State and local governments and private entities.

SEC. 107. REPORTS TO CONGRESS.

(a) IN GENERAL.—The Director shall submit an annual report to the appropriate congressional committees

describing the activities, ongoing projects, and plans of the Federal Government designed to meet the goals and objectives of the National Strategy.

(b) CLASSIFIED ANNEX.—A report submitted under this section shall be submitted in an unclassified form, but may include a classified annex, if necessary.

(c) PUBLIC REPORT.—An unclassified version of each report submitted under this section shall be made available to the public.

TITLE II—NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS

SEC. 201. CYBERSECURITY.

Title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following:

"Subtitle E—Cybersecurity

"SEC. 241. DEFINITIONS.

"In this subtitle—

"(1) the term 'agency information infrastructure' means the Federal information infrastructure of a particular Federal agency;

"(2) the term 'appropriate committees of Congress' means the Committee on Homeland Security and Governmental Affairs of the Senate and the

Committee on Homeland Security of the House of Representatives;

"(3) the term 'Center' means the National Center for Cybersecurity and Communications established under section 242(a);

"(4) the term 'covered critical infrastructure' means a system or asset—

"(A) that is on the prioritized critical infrastructure list established by the Secretary under section 210E(a)(2); and

"(B)(i) that is a component of the national information infrastructure; or

"(ii) for which the national information infrastructure is essential to the reliable operation of the system or asset;

"(5) the term 'cyber vulnerability' means any security vulnerability that, if exploited, could pose a significant risk of disruption to the operation of information infrastructure essential to the reliable operation of covered critical infrastructure;

"(6) the term 'Director' means the Director of the Center appointed under section 242(b)(1);

"(7) the term 'Federal agency'—

"(A) means any executive department, military department, Government corporation,

Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

"(B) does not include the governments of the District of Columbia and of the territories and possessions of the United States and their various subdivisions;

"(8) the term 'Federal information infrastructure'—

"(A) means information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, any Federal agency, including information systems used or operated by another entity on behalf of a Federal agency; and

"(B) does not include—

"(i) a national security system; or

"(ii) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community;

''(9) the term 'incident' means an occurrence that—

''(A) actually or potentially jeopardizes—

''(i) the information security of information infrastructure; or

''(ii) the information that information infrastructure processes, stores, receives, or transmits; or

''(B) constitutes a violation or threat of violation of security policies, security procedures, or acceptable use policies applicable to information infrastructure.

''(10) the term 'information infrastructure' means the underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including—

''(A) programmable electronic devices and communications networks; and

''(B) any associated hardware, software, or data;

''(11) the term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

"(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

"(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

"(C) availability, by ensuring timely and reliable access to and use of information;

"(12) the term 'information sharing and analysis center' means a self-governed forum whose members work together within a specific sector of critical infrastructure to identify, analyze, and share with other members and the Federal Government critical information relating to threats, vulnerabilities, or incidents to the security and resiliency of the critical infrastructure that comprises the specific sector;

"(13) the term 'information system' has the meaning given that term in section 3502 of title 44, United States Code;

"(14) the term 'intelligence community' has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4));

"(15) the term 'management controls' means safeguards or countermeasures for an information system that focus on the management of risk and the management of information system security;

"(16) the term 'National Cybersecurity Advisory Council' means the National Cybersecurity Advisory Council established under section 239;

"(17) the term 'national cyber emergency' means an actual or imminent action by any individual or entity to exploit a cyber vulnerability in a manner that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure;

"(18) the term 'national information infrastructure' means information infrastructure—

"(A)(i) that is owned, operated, or controlled within or from the United States; or

"(ii) if located outside the United States, the disruption of which could result in national or regional catastrophic damage in the United States; and

"(B) that is not owned, operated, controlled, or licensed for use by a Federal agency;

''(19) the term 'national security system' has the same meaning given that term in section 3551 of title 44, United States Code;

''(20) the term 'operational controls' means the safeguards and countermeasures for an information system that are primarily implemented and executed by individuals not systems;

''(21) the term 'sector-specific agency' means the relevant Federal agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category under the National Infrastructure Protection Plan, or any other appropriate Federal agency identified by the President after the date of enactment of this subtitle;

''(22) the term 'sector coordinating councils' means self-governed councils that are composed of representatives of key stakeholders within a specific sector of critical infrastructure that serve as the principal private sector policy coordination and planning entities with the Federal Government relating to the security and resiliency of the critical infrastructure that comprise that sector;

''(23) the term 'security controls' means the management, operational, and technical controls pre-

scribed for an information system to protect the information security of the system;

''(24) the term 'small business concern' has the meaning given that term under section 3 of the Small Business Act (15 U.S.C. 632);

''(25) the term 'technical controls' means the safeguards or countermeasures for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system;

''(26) 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);

''(27) the term 'United States person' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and

''(28) the term 'US–CERT' means the United States Computer Readiness Team established under section 244.

''SEC. 242. NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.

''(a) ESTABLISHMENT.—

"(1) IN GENERAL.—There is established within the Department a National Center for Cybersecurity and Communications.

"(2) OPERATIONAL ENTITY.—The Center may—

"(A) enter into contracts for the procurement of property and services for the Center; and

"(B) appoint employees of the Center in accordance with the civil service laws of the United States.

"(b) DIRECTOR.—

"(1) IN GENERAL.—The Center shall be headed by a Director, who shall be appointed by the President, by and with the advice and consent of the Senate.

"(2) REPORTING TO SECRETARY.—The Director shall report directly to the Secretary and serve as the principal advisor to the Secretary on cybersecurity and the operations, security, and resiliency of the communications infrastructure of the United States.

"(3) PRESIDENTIAL ADVICE.—The Director shall regularly advise the President on the exercise of the authorities provided under this subtitle or any

other provision of law relating to the security of the Federal information infrastructure or an agency information infrastructure.

"(4) QUALIFICATIONS.—The Director shall be appointed from among individuals who have—

"(A) a demonstrated ability in and knowledge of information technology, cybersecurity, and the operations, security and resiliency of communications networks; and

"(B) significant executive leadership and management experience in the public or private sector.

"(5) LIMITATION ON SERVICE.—

"(A) IN GENERAL.—Subject to subparagraph (B), the individual serving as the Director may not, while so serving, serve in any other capacity in the Federal Government, except to the extent that the individual serving as Director is doing so in an acting capacity.

"(B) EXCEPTION.—The Director may serve on any commission, board, council, or similar entity with responsibilities or duties relating to cybersecurity or the operations, security, and resiliency of the communications infrastructure of the United States at the direction

of the President or as otherwise provided by law.

''(c) DEPUTY DIRECTORS.—

''(1) IN GENERAL.—There shall be not less than 2 Deputy Directors for the Center, who shall report to the Director.

''(2) INFRASTRUCTURE PROTECTION.—

''(A) APPOINTMENT.—There shall be a Deputy Director appointed by the Secretary, who shall have expertise in infrastructure protection.

''(B) RESPONSIBILITIES.—The Deputy Director appointed under subparagraph (A) shall—

''(i) assist the Director and the Assistant Secretary for Infrastructure Protection in coordinating, managing, and directing the information, communications, and physical infrastructure protection responsibilities and activities of the Department, including activities under Homeland Security Presidential Directive–7, or any successor thereto, and the National Infrastructure Protection Plan, or any successor thereto;

‘‘(ii) review the budget for the Center and the Office of Infrastructure Protection before submission of the budget to the Secretary to ensure that activities are appropriately coordinated;

‘‘(iii) develop, update periodically, and submit to the appropriate committees of Congress a strategic plan detailing how critical infrastructure protection activities will be coordinated between the Center, the Office of Infrastructure Protection, and the private sector;

‘‘(iv) subject to the direction of the Director resolve conflicts between the Center and the Office of Infrastructure Protection relating to the information, communications, and physical infrastructure protection responsibilities of the Center and the Office of Infrastructure Protection; and

‘‘(v) perform such other duties as the Director may assign.

‘‘(C) ANNUAL EVALUATION.—The Assistant Secretary for Infrastructure Protection shall submit annually to the Director an evalua-

tion of the performance of the Deputy Director appointed under subparagraph (A).

''(3) INTELLIGENCE COMMUNITY.—The Director of National Intelligence shall identify an employee of an element of the intelligence community to serve as a Deputy Director of the Center. The employee shall be detailed to the Center on a reimbursable basis for such period as is agreed to by the Director and the Director of National Intelligence, and, while serving as Deputy Director, shall report directly to the Director of the Center.

''(d) LIAISON OFFICERS.—The Secretary of Defense, the Attorney General, the Secretary of Commerce, and the Director of National Intelligence shall detail personnel to the Center to act as full-time liaisons with the Department of Defense, the Department of Justice, the National Institute of Standards and Technology, and elements of the intelligence community to assist in coordination between and among the Center, the Department of Defense, the Department of Justice, the National Institute of Standards and Technology, and elements of the intelligence community.

''(e) PRIVACY OFFICER.—

''(1) IN GENERAL.—The Director, in consultation with the Secretary, shall designate a full-time privacy officer, who shall report to the Director.

''(2) DUTIES.—The privacy officer designated under paragraph (1) shall have primary responsibility for implementation by the Center of the privacy policy for the Department established by the Privacy Officer appointed under section 222.

''(f) DUTIES OF DIRECTOR.—

''(1) IN GENERAL.—The Director shall—

''(A) working cooperatively with the private sector, lead the Federal effort to secure, protect, and ensure the resiliency of the Federal information infrastructure and national information infrastructure of the United States, including communications networks;

''(B) assist in the identification, remediation, and mitigation of vulnerabilities to the Federal information infrastructure and the national information infrastructure;

''(C) provide dynamic, comprehensive, and continuous situational awareness of the security status of the Federal information infrastructure, national information infrastructure, and information infrastructure that is owned, oper-

~~ated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community by sharing and integrating classified and unclassified information, including information relating to threats, vulnerabilities, traffic, trends, incidents, and other anomalous activities affecting the infrastructure or systems, on a routine and continuous basis with—~~

~~"(i) the National Threat Operations Center of the National Security Agency;~~

~~"(ii) the United States Cyber Command, including the Joint Task Force-Global Network Operations;~~

~~"(iii) the Cyber Crime Center of the Department of Defense;~~

~~"(iv) the National Cyber Investigative Joint Task Force;~~

~~"(v) the Intelligence Community Incident Response Center;~~

~~"(vi) any other Federal agency, or component thereof, identified by the Director; and~~

“(vii) any non-Federal entity, including, where appropriate, information sharing and analysis centers, identified by the Director, with the concurrence of the owner or operator of that entity and consistent with applicable law;

“(D) work with the entities described in subparagraph (C) to establish policies and procedures that enable information sharing between and among the entities;

“(E) develop, in coordination with the Assistant Secretary for Infrastructure Protection, other Federal agencies, the private sector, and State and local governments, a national incident response plan that details the roles of Federal agencies, State and local governments, and the private sector, including plans to be executed in response to a declaration of a national cyber emergency by the President under section 249;

“(F) conduct risk-based assessments of the Federal information infrastructure with respect to acts of terrorism, natural disasters, and other large-scale disruptions and provide the results of the assessments to the Director of Cyberspace Policy;

"(G) develop, oversee the implementation of, and enforce policies, principles, and guidelines on information security for the Federal information infrastructure, including timely adoption of and compliance with standards developed by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3);

"(H) provide assistance to the National Institute of Standards and Technology in developing standards under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3);

"(I) provide to Federal agencies mandatory security controls to mitigate and remediate vulnerabilities of and incidents affecting the Federal information infrastructure;

"(J) subject to paragraph (2), and as needed, assist the Director of the Office of Management and Budget and the Director of Cyberspace Policy in conducting analysis and prioritization of budgets, relating to the security of the Federal information infrastructure;

~~"(K) in accordance with section 253, develop, periodically update, and implement a supply chain risk management strategy to enhance, in a risk-based and cost-effective manner, the security of the communications and information technology products and services purchased by the Federal Government;~~

~~"(L) notify the Director of Cyberspace Policy of any incident involving the Federal information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, or the national information infrastructure that could compromise or significantly affect economic or national security;~~

~~"(M) consult, in coordination with the Director of Cyberspace Policy, with appropriate international partners to enhance the security of the Federal information infrastructure and national information infrastructure;~~

~~"(N)(i) coordinate and integrate information to analyze the composite security state of the Federal information infrastructure and in-~~

formation infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community;

"(ii) ensure the information required under clause (i) and section 3553(c)(1)(A) of title 44, United States Code, including the views of the Director on the adequacy and effectiveness of information security throughout the Federal information infrastructure and information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, is available on an automated and continuous basis through the system maintained under section 3552(a)(3)(D) of title 44, United States Code;

"(iii) in conjunction with the quadrennial homeland security review required under section 707, and at such other times determined appropriate by the Director, analyze the composite security state of the national information infrastructure and submit to the President, Congress, and the Secretary a report regarding ac-

tions necessary to enhance the composite security state of the national information infrastructure based on the analysis; and

‘‘(iv) foster collaboration and serve as the primary contact between the Federal Government, State and local governments, and private entities on matters relating to the security of the Federal information infrastructure and the national information infrastructure;

‘‘(O) oversee the development, implementation, and management of security requirements for Federal agencies relating to the external access points to or from the Federal information infrastructure;

‘‘(P) establish, develop, and oversee the capabilities and operations within the US–CERT as required by section 244;

‘‘(Q) oversee the operations of the National Communications System, as described in Executive Order 12472 (49 Fed. Reg. 13471, relating to the assignment of national security and emergency preparedness telecommunications functions), as amended by Executive Order 13286 (68 Fed. Reg. 10619) and Executive Order 13407 (71 Fed. Reg. 36975), or any suc-

cessor thereto, including planning for and providing communications for the Federal Government under all circumstances, including crises, emergencies, attacks, recoveries, and reconstitutions;

''(R) ensure, in coordination with the privacy officer designated under subsection (e), the Privacy Officer appointed under section 222, and the Director of the Office of Civil Rights and Civil Liberties appointed under section 705, that the activities of the Center comply with all policies, regulations, and laws protecting the privacy and civil liberties of United States persons;

''(S) subject to the availability of resources, and at the discretion of the Director, provide voluntary technical assistance—

''(i) at the request of an owner or operator of covered critical infrastructure, to assist the owner or operator in complying with sections 248 and 249, including implementing required security or emergency measures and developing response plans for national cyber emergencies declared under section 249; and

"(ii) at the request of the owner or operator of national information infrastructure that is not covered critical infrastructure, and based on risk, to assist the owner or operator in implementing best practices, and related standards and guidelines, recommended under section 247 and other measures necessary to mitigate or remediate vulnerabilities of the information infrastructure and the consequences of efforts to exploit the vulnerabilities;

"(T)(i) conduct, in consultation with the National Cybersecurity Advisory Council, the head of appropriate sector-specific agencies, and any private sector entity determined appropriate by the Director, risk-based assessments of national information infrastructure, on a sector-by-sector basis, with respect to acts of terrorism, natural disasters, and other large-scale disruptions or financial harm, which shall identify and prioritize risks to the national information infrastructure, including vulnerabilities and associated consequences; and

‘‘(ii) coordinate and evaluate the mitigation or remediation of cyber vulnerabilities and consequences identified under clause (i);

‘‘(U) regularly evaluate and assess technologies designed to enhance the protection of the Federal information infrastructure and national information infrastructure, including an assessment of the cost-effectiveness of the technologies;

‘‘(V) promote the use of the best practices recommended under section 247 to State and local governments and the private sector;

‘‘(W) develop and implement outreach and awareness programs on cybersecurity, including—

‘‘(i) a public education campaign to increase the awareness of cybersecurity, cyber safety, and cyber ethics, which shall include use of the Internet, social media, entertainment, and other media to reach the public;

‘‘(ii) an education campaign to increase the understanding of State and local governments and private sector entities of the costs of failing to ensure effective secu-

rity of information infrastructure and cost-effective methods to mitigate and remediate vulnerabilities; and

"(iii) outcome-based performance measures to determine the success of the programs;

"(X) develop and implement a national cybersecurity exercise program that includes—

"(i) the participation of State and local governments, international partners of the United States, and the private sector; and

"(ii) an after action report analyzing lessons learned from exercises and identifying vulnerabilities to be remediated or mitigated;

"(Y) coordinate with the Assistant Secretary for Infrastructure Protection to ensure that—

"(i) cybersecurity is appropriately addressed in carrying out the infrastructure protection responsibilities described in section 201(d); and

"(ii) the operations of the Center and the Office of Infrastructure Protection

avoid duplication and use, to the maximum extent practicable, joint mechanisms for information sharing and coordination with the private sector;

''(Z) oversee the activities of the Office of Emergency Communications established under section 1801; and

''(AA) perform such other duties as the Secretary may direct relating to the security and resiliency of the information and communications infrastructure of the United States.

''(2) BUDGET ANALYSIS.—In conducting analysis and prioritization of budgets under paragraph (1)(J), the Director—

''(A) in coordination with the Director of the Office of Management and Budget, may access information from any Federal agency regarding the finances, budget, and programs of the Federal agency relevant to the security of the Federal information infrastructure;

''(B) may make recommendations to the Director of the Office of Management and Budget and the Director of Cyberspace Policy regarding the budget for each Federal agency to ensure that adequate funding is devoted to

securing the Federal information infrastructure, in accordance with policies, principles, and guidelines established by the Director under this subtitle; and

"(C) shall provide copies of any recommendations made under subparagraph (B) to—

"(i) the Committee on Appropriations of the Senate;

"(ii) the Committee on Appropriations of the House of Representatives; and

"(iii) the appropriate committees of Congress.

"(g) USE OF MECHANISMS FOR COLLABORATION.—In carrying out the responsibilities and authorities of the Director under this subtitle, to the maximum extent practicable, the Director shall use mechanisms for collaboration and information sharing (including mechanisms relating to the identification and communication of threats, vulnerabilities, and associated consequences) established by other components of the Department or other Federal agencies to avoid unnecessary duplication or waste.

"(h) SUFFICIENCY OF RESOURCES PLAN.—

"(1) REPORT.—Not later than 120 days after the date of enactment of this subtitle, the Director

of the Office of Management and Budget shall submit to the appropriate committees of Congress and the Comptroller General of the United States a report on the resources and staff necessary to carry out fully the responsibilities under this subtitle.

"(2) COMPTROLLER GENERAL REVIEW.—

"(A) IN GENERAL.—The Comptroller General of the United States shall evaluate the reasonableness and adequacy of the report submitted by the Director under paragraph (1).

"(B) REPORT.—Not later than 60 days after the date on which the report is submitted under paragraph (1), the Comptroller General shall submit to the appropriate committees of Congress a report containing the findings of the review under subparagraph (A).

"(i) FUNCTIONS TRANSFERRED.—There are transferred to the Center the National Cyber Security Division, the Office of Emergency Communications, and the National Communications System, including all the functions, personnel, assets, authorities, and liabilities of the National Cyber Security Division and the National Communications System.

"SEC. 243. PHYSICAL AND CYBER INFRASTRUCTURE COLLABORATION.

"(a) IN GENERAL.—The Director and the Assistant Secretary for Infrastructure Protection shall coordinate the information, communications, and physical infrastructure protection responsibilities and activities of the Center and the Office of Infrastructure Protection.

"(b) OVERSIGHT.—The Secretary shall ensure that the coordination described in subsection (a) occurs.

"SEC. 244. UNITED STATES COMPUTER EMERGENCY READINESS TEAM.

"(a) ESTABLISHMENT OF OFFICE.—There is established within the Center, the United States Computer Emergency Readiness Team, which shall be headed by a Director, who shall be selected from the Senior Executive Service by the Secretary.

"(b) RESPONSIBILITIES.—The US–CERT shall—

"(1) collect, coordinate, and disseminate information on—

"(A) risks to the Federal information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, or the national information infrastructure; and

~~"(B) security controls to enhance the security of the Federal information infrastructure or the national information infrastructure against the risks identified in subparagraph (A); and~~

~~"(2) establish a mechanism for engagement with the private sector.~~

~~"(c) MONITORING, ANALYSIS, WARNING, AND RESPONSE.—~~

~~"(1) DUTIES.—Subject to paragraph (2), the US–CERT shall—~~

~~"(A) provide analysis and reports to Federal agencies on the security of the Federal information infrastructure;~~

~~"(B) provide continuous, automated monitoring of the Federal information infrastructure at external Internet access points, which shall include detection and warning of threats, vulnerabilities, traffic, trends, incidents, and other anomalous activities affecting the information security of the Federal information infrastructure;~~

~~"(C) warn Federal agencies of threats, vulnerabilities, incidents, and anomalous activi-~~

ties that could affect the Federal information infrastructure;

''(D) develop, recommend, and deploy security controls to mitigate or remediate vulnerabilities;

''(E) support Federal agencies in conducting risk assessments of the agency information infrastructure;

''(F) disseminate to Federal agencies risk analyses of incidents that could impair the risk-based security of the Federal information infrastructure;

''(G) develop and acquire predictive analytic tools to evaluate threats, vulnerabilities, traffic, trends, incidents, and anomalous activities;

''(H) aid in the detection of, and warn owners or operators of national information infrastructure regarding, threats, vulnerabilities, and incidents, affecting the national information infrastructure, including providing—

''(i) timely, targeted, and actionable notifications of threats, vulnerabilities, and incidents; and

"(ii) recommended security controls to mitigate or remediate vulnerabilities; and

"(I) respond to assistance requests from Federal agencies and, subject to the availability of resources, owners or operators of the national information infrastructure to—

"(i) isolate, mitigate, or remediate incidents;

"(ii) recover from damages and mitigate or remediate vulnerabilities; and

"(iii) evaluate security controls and other actions taken to secure information infrastructure and incorporate lessons learned into best practices, policies, principles, and guidelines.

"(2) REQUIREMENT.—With respect to the Federal information infrastructure, the US–CERT shall conduct the activities described in paragraph (1) in a manner consistent with the responsibilities of the head of a Federal agency described in section 3553 of title 44, United States Code.

"(3) REPORT.—Not later than 1 year after the date of enactment of this subtitle, and every year thereafter, the Secretary shall—

"(A) in conjunction with the Inspector General of the Department, conduct an independent audit or review of the activities of the US–CERT under paragraph (1)(B); and

"(B) submit to the appropriate committees of Congress and the President a report regarding the audit or report.

"(d) PROCEDURES FOR FEDERAL GOVERNMENT.—Not later than 90 days after the date of enactment of this subtitle, the head of each Federal agency shall establish procedures for the Federal agency that ensure that the US–CERT can perform the functions described in subsection (c) in relation to the Federal agency.

"(e) OPERATIONAL UPDATES.—The US–CERT shall provide unclassified and, as appropriate, classified updates regarding the composite security state of the Federal information infrastructure to the Federal Information Security Taskforce.

"(f) FEDERAL POINTS OF CONTACT.—The Director of the US–CERT shall designate a principal point of contact within the US–CERT for each Federal agency to—

"(1) maintain communication;

"(2) ensure cooperative engagement and information sharing; and

"(3) respond to inquiries or requests.

"(g) REQUESTS FOR INFORMATION OR PHYSICAL ACCESS.—

"(1) INFORMATION ACCESS.—Upon request of the Director of the US–CERT, the head of a Federal agency or an Inspector General for a Federal agency shall provide any law enforcement information, intelligence information, terrorism information, or any other information (including information relating to incidents provided under subsections (a)(4) and (c) of section 246) relevant to the security of the Federal information infrastructure or the national information infrastructure necessary to carry out the duties, responsibilities, and authorities under this subtitle.

"(2) PHYSICAL ACCESS.—Upon request of the Director, and in consultation with the head of a Federal agency, the Federal agency shall provide physical access to any facility of the Federal agency necessary to determine whether the Federal agency is in compliance with any policies, principles, and guidelines established by the Director under this subtitle, or otherwise necessary to carry out the duties, responsibilities, and authorities of the Director applicable to the Federal information infrastructure.

"SEC. 245. ADDITIONAL AUTHORITIES OF THE DIRECTOR OF THE NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.

"(a) ACCESS TO INFORMATION.—Unless otherwise directed by the President—

"(1) the Director shall access, receive, and analyze law enforcement information, intelligence information, terrorism information, and any other information (including information relating to incidents provided under subsections (a)(4) and (c) of section 246) relevant to the security of the Federal information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, or national information infrastructure from Federal agencies and, consistent with applicable law, State and local governments (including law enforcement agencies), and private entities, including information provided by any contractor to a Federal agency regarding the security of the agency information infrastructure;

"(2) any Federal agency in possession of law enforcement information, intelligence information, terrorism information, or any other information (including information relating to incidents provided

under subsections (a)(4) and (c) of section 246) relevant to the security of the Federal information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, or national information infrastructure shall provide that information to the Director in a timely manner; and

"(3) the Director, in coordination with the Attorney General, the Privacy and Civil Liberties Oversight Board established under section 1061 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee), the Director of National Intelligence, and the Archivist of the United States, shall establish guidelines to ensure that information is transferred, stored, and preserved in accordance with applicable law and in a manner that protects the privacy and civil liberties of United States persons.

"(b) OPERATIONAL EVALUATIONS.—

"(1) IN GENERAL.—The Director—

"(A) subject to paragraph (2), shall develop, maintain, and enhance capabilities to evaluate the security of the Federal information

infrastructure as described in section 3554(a)(3) of title 44, United States Code, including the ability to conduct risk-based penetration testing and vulnerability assessments;

''(B) in carrying out subparagraph (A), may request technical assistance from the Director of the Federal Bureau of Investigation, the Director of the National Security Agency, the head of any other Federal agency that may provide support, and any nongovernmental entity contracting with the Department or another Federal agency; and

''(C) in consultation with the Attorney General and the Privacy and Civil Liberties Oversight Board established under section 1061 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee), shall develop guidelines to ensure compliance with all applicable laws relating to the privacy of United States persons in carrying out the operational evaluations under subparagraph (A).

''(2) OPERATIONAL EVALUATIONS.—

''(A) IN GENERAL.—The Director may conduct risk-based operational evaluations of the agency information infrastructure of any

Federal agency, at a time determined by the Director, in consultation with the head of the Federal agency, using the capabilities developed under paragraph (1)(A).

''(B) ANNUAL EVALUATION REQUIREMENT.—If the Director conducts an operational evaluation under subparagraph (A) or an operational evaluation at the request of a Federal agency to meet the requirements of section 3554 of title 44, United States Code, the operational evaluation shall satisfy the requirements of section 3554 for the Federal agency for the year of the evaluation, unless otherwise specified by the Director.

''(c) CORRECTIVE MEASURES AND MITIGATION PLANS.—If the Director determines that a Federal agency is not in compliance with applicable policies, principles, standards, and guidelines applicable to the Federal information infrastructure—

''(1) the Director, in consultation with the Director of the Office of Management and Budget, may direct the head of the Federal agency to—

''(A) take corrective measures to meet the policies, principles, standards, and guidelines; and

"(B) develop a plan to remediate or mitigate any vulnerabilities addressed by the policies, principles, standards, and guidelines;

"(2) within such time period as the Director shall prescribe, the head of the Federal agency shall—

"(A) implement a corrective measure or develop a mitigation plan in accordance with paragraph (1); or

"(B) submit to the Director, the Director of the Office of Management and Budget, the Inspector General for the Federal agency, and the appropriate committees of Congress a report indicating why the Federal agency has not implemented the corrective measure or developed a mitigation plan; and

"(3) the Director may direct the isolation of any component of the agency information infrastructure, consistent with the contingency or continuity of operation plans applicable to the agency information infrastructure, until corrective measures are taken or mitigation plans approved by the Director are put in place, if—

‘‘(A) the head of the Federal agency has failed to comply with the corrective measures prescribed under paragraph (1); and

‘‘(B) the failure to comply presents a significant danger to the Federal information infrastructure.

‘‘SEC. 246. INFORMATION SHARING.

‘‘(a) FEDERAL AGENCIES.—

‘‘(1) INFORMATION SHARING PROGRAM.—Consistent with the responsibilities described in section 242 and 244, the Director, in consultation with the other members of the Chief Information Officers Council established under section 3603 of title 44, United States Code, and the Federal Information Security Taskforce, shall establish a program for sharing information with and between the Center and other Federal agencies that includes processes and procedures, including standard operating procedures—

‘‘(A) under which the Director regularly shares with each Federal agency—

‘‘(i) analysis and reports on the composite security state of the Federal information infrastructure and information infrastructure that is owned, operated, con-

trolled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, which shall include information relating to threats, vulnerabilities, incidents, or anomalous activities;

"(ii) any available analysis and reports regarding the security of the agency information infrastructure; and

"(iii) means and methods of preventing, responding to, mitigating, and remediating vulnerabilities; and

"(B) under which the Director may request information from Federal agencies concerning the security of the Federal information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, or the national information infrastructure necessary to carry out the duties of the Director under this subtitle or any other provision of law.

"(2) CONTENTS.—The program established under this section shall include—

"(A) timeframes for the sharing of information under paragraph (1);

"(B) guidance on what information shall be shared, including information regarding incidents;

"(C) a tiered structure that provides guidance for the sharing of urgent information; and

"(D) processes and procedures under which the Director or the head of a Federal agency may report noncompliance with the program to the Director of Cyberspace Policy.

"(3) US–CERT.—The Director of the US–CERT shall ensure that the head of each Federal agency has continual access to data collected by the US–CERT regarding the agency information infrastructure of the Federal agency.

"(4) FEDERAL AGENCIES.—

"(A) IN GENERAL.—The head of a Federal agency shall comply with all processes and procedures established under this subsection regarding notification to the Director relating to incidents.

~~"(B) IMMEDIATE NOTIFICATION REQUIRED.—Unless otherwise directed by the President, any Federal agency with a national security system shall immediately notify the Director regarding any incident affecting the risk-based security of the national security system.~~

~~"(b) STATE AND LOCAL GOVERNMENTS, PRIVATE SECTOR, AND INTERNATIONAL PARTNERS.—~~

~~"(1) IN GENERAL.—The Director, shall establish processes and procedures, including standard operating procedures, to promote bidirectional information sharing with State and local governments, private entities, and international partners of the United States on—~~

~~"(A) threats, vulnerabilities, incidents, and anomalous activities affecting the national information infrastructure; and~~

~~"(B) means and methods of preventing, responding to, and mitigating and remediating vulnerabilities.~~

~~"(2) CONTENTS.—The processes and procedures established under paragraph (1) shall include—~~

~~"(A) means or methods of accessing classified or unclassified information, as appropriate,~~

that will provide situational awareness of the security of the Federal information infrastructure and the national information infrastructure relating to threats, vulnerabilities, traffic, trends, incidents, and other anomalous activities affecting the Federal information infrastructure or the national information infrastructure;

"(B) a mechanism, established in consultation with the heads of the relevant sector-specific agencies, sector coordinating councils, and information sharing and analysis centers, by which owners and operators of covered critical infrastructure shall report incidents in the information infrastructure for covered critical infrastructure, to the extent the incident might indicate an actual or potential cyber vulnerability, or exploitation of that vulnerability; and

"(C) an evaluation of the need to provide security clearances to employees of State and local governments, private entities, and international partners to carry out this subsection.

"(3) GUIDELINES.—The Director, in consultation with the Attorney General and the Director of National Intelligence, shall develop guidelines to pro-

tect the privacy and civil liberties of United States persons and intelligence sources and methods, while carrying out this subsection.

"(c) INCIDENTS.—

"(1) NON-FEDERAL ENTITIES.—

"(A) IN GENERAL.—

"(i) MANDATORY REPORTING.—Subject to clause (i), the owner or operator of covered critical infrastructure shall report any incident affecting the information infrastructure of covered critical infrastructure to the extent the incident might indicate an actual or potential cyber vulnerability, or exploitation of a cyber vulnerability, in accordance with the policies and procedures for the mechanism established under subsection (b)(2)(B) and guidelines developed under subsection (b)(3).

"(ii) LIMITATION.—Clause (i) shall not authorize the Director, the Center, the Department, or any other Federal entity to compel the disclosure of information relating to an incident or conduct surveillance unless otherwise authorized under chapter 119, chapter 121, or chapter 206 of title

~~18, United States Code, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or any other provision of law.~~

~~"(B) REPORTING PROCEDURES.—The Director shall establish procedures that enable and encourage the owner or operator of national information infrastructure to report to the Director regarding incidents affecting such information infrastructure.~~

~~"(2) INFORMATION PROTECTION.—Notwithstanding any other provision of law, information reported under paragraph (1) shall be protected from unauthorized disclosure, in accordance with section 251.~~

~~"(d) ADDITIONAL RESPONSIBILITIES.—In accordance with section 251, the Director shall—~~

~~"(1) share data collected on the Federal information infrastructure with the National Science Foundation and other accredited research institutions for the sole purpose of cybersecurity research in a manner that protects privacy and civil liberties of United States persons and intelligence sources and methods;~~

‘‘(2) establish a website to provide an opportunity for the public to provide—

‘‘(A) input about the operations of the Center; and

‘‘(B) recommendations for improvements of the Center; and

‘‘(3) in coordination with the Secretary of Defense, the Director of National Intelligence, the Secretary of State, and the Attorney General, develop information sharing pilot programs with international partners of the United States.

‘‘SEC. 247. PRIVATE SECTOR ASSISTANCE.

‘‘(a) IN GENERAL.—The Director, in consultation with the Director of the National Institute of Standards and Technology, the Director of the National Security Agency, the head of any relevant sector-specific agency, the National Cybersecurity Advisory Council, State and local governments, and any private entities the Director determines appropriate, shall establish a program to promote, and provide technical assistance authorized under section 242(f)(1)(S) relating to the implementation of, best practices and related standards and guidelines for securing the national information infrastructure, including the costs and benefits associated with the implementation of the best practices and related standards and guidelines.

''(b) ANALYSIS AND IMPROVEMENT OF STANDARDS AND GUIDELINES.—For purposes of the program established under subsection (a), the Director shall—

''(1) regularly assess and evaluate cybersecurity standards and guidelines issued by private sector organizations, recognized international and domestic standards setting organizations, and Federal agencies; and

''(2) in coordination with the National Institute of Standards and Technology, encourage the development of, and recommend changes to, the standards and guidelines described in paragraph (1) for securing the national information infrastructure.

''(c) GUIDANCE AND TECHNICAL ASSISTANCE.—

''(1) IN GENERAL.—The Director shall promote best practices and related standards and guidelines to assist owners and operators of national information infrastructure in increasing the security of the national information infrastructure and protecting against and mitigating or remediating known vulnerabilities.

''(2) REQUIREMENT.—Technical assistance provided under section 242(f)(1)(S) and best practices promoted under this section shall be prioritized based on risk.

"(d) CRITERIA.—In promoting best practices or recommending changes to standards and guidelines under this section, the Director shall ensure that best practices, and related standards and guidelines—

"(1) address cybersecurity in a comprehensive, risk-based manner;

"(2) include consideration of the cost of implementing such best practices or of implementing recommended changes to standards and guidelines;

"(3) increase the ability of the owners or operators of national information infrastructure to protect against and mitigate or remediate known vulnerabilities;

"(4) are suitable, as appropriate, for implementation by small business concerns;

"(5) as necessary and appropriate, are sector specific;

"(6) to the maximum extent possible, incorporate standards and guidelines established by private sector organizations, recognized international and domestic standards setting organizations, and Federal agencies; and

"(7) provide sufficient flexibility to permit a range of security solutions.

"SEC. 248. CYBER VULNERABILITIES TO COVERED CRITICAL INFRASTRUCTURE.

"(a) IDENTIFICATION OF CYBER VULNERABILITIES.—

"(1) IN GENERAL.—Based on the risk-based assessments conducted under section 242(f)(1)(T)(i), the Director, in coordination with the head of the sector-specific agency with responsibility for covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure, and in consultation with the National Cybersecurity Advisory Council and any private sector entity determined appropriate by the Director, shall, on a continuous and sector-by-sector basis, identify and evaluate the cyber vulnerabilities to covered critical infrastructure.

"(2) FACTORS TO BE CONSIDERED.—In identifying and evaluating cyber vulnerabilities under paragraph (1), the Director shall consider—

"(A) the perceived threat, including a consideration of adversary capabilities and intent, preparedness, target attractiveness, and deterrence capabilities;

"(B) the potential extent and likelihood of death, injury, or serious adverse effects to

~~human health and safety caused by a disruption of the reliable operation of covered critical infrastructure;~~

~~"(C) the threat to or potential impact on national security caused by a disruption of the reliable operation of covered critical infrastructure;~~

~~"(D) the extent to which the disruption of the reliable operation of covered critical infrastructure will disrupt the reliable operation of other covered critical infrastructure;~~

~~"(E) the potential for harm to the economy that would result from a disruption of the reliable operation of covered critical infrastructure; and~~

~~"(F) other risk-based security factors that the Director, in consultation with the head of the sector-specific agency with responsibility for the covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure, determine to be appropriate and necessary to protect public health and safety, critical infrastructure, or national and economic security.~~

"(3) REPORT.—

"(A) IN GENERAL.—Not later than 180 days after the date of enactment of this subtitle, and annually thereafter, the Director, in coordination with the head of the sector-specific agency with responsibility for the covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure, shall submit to the appropriate committees of Congress a report on the findings of the identification and evaluation of cyber vulnerabilities under this subsection. Each report submitted under this paragraph shall be submitted in an unclassified form, but may include a classified annex.

"(B) INPUT.—For purposes of the reports required under subparagraph (A), the Director shall create a process under which owners and operators of covered critical infrastructure may provide input on the findings of the reports.

"(b) RISK-BASED PERFORMANCE REQUIREMENTS.—

"(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this subtitle, in coordination with the heads of the sector-specific

agencies with responsibility for covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure, and in consultation with the National Cybersecurity Advisory Council and any private sector entity determined appropriate by the Director, the Director shall issue interim final regulations establishing risk-based security performance requirements to secure covered critical infrastructure against cyber vulnerabilities through the adoption of security measures that satisfy the security performance requirements identified by the Director.

''(2) PROCEDURES.—The regulations issued under this subsection shall—

''(A) include a process under which owners and operators of covered critical infrastructure are informed of identified cyber vulnerabilities and security performance requirements designed to remediate or mitigate the cyber vulnerabilities, in combination with best practices recommended under section 247;

''(B) establish a process for owners and operators of covered critical infrastructure to select security measures, including any best

practices recommended under section 247, that, in combination, satisfy the security performance requirements established by the Director under this subsection;

"(C) establish a process for owners and operators of covered critical infrastructure to develop response plans for a national cyber emergency declared under section 249; and

"(D) establish a process by which the Director—

"(i) is notified of the security measures selected by the owner or operator of covered critical infrastructure under subparagraph (B); and

"(ii) may determine whether the proposed security measures satisfy the security performance requirements established by the Director under this subsection.

"(3) INTERNATIONAL COOPERATION ON SECURING COVERED CRITICAL INFRASTRUCTURE.—

"(A) IN GENERAL.—The Director, in coordination with the head of the sector-specific agency with responsibility for covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with

responsibilities for regulating the covered critical infrastructure, shall—

"(i) consistent with the protection of intelligence sources and methods and other sensitive matters, inform the owner or operator of covered critical infrastructure that is located outside the United States and the government of the country in which the covered critical infrastructure is located of any cyber vulnerabilities to the covered critical infrastructure; and

"(ii) coordinate with the government of the country in which the covered critical infrastructure is located and, as appropriate, the owner or operator of the covered critical infrastructure, regarding the implementation of security measures or other measures to the covered critical infrastructure to mitigate or remediate cyber vulnerabilities.

"(B) INTERNATIONAL AGREEMENTS.—The Director shall carry out the this paragraph in a manner consistent with applicable international agreements.

‘‘(4) RISK-BASED SECURITY PERFORMANCE REQUIREMENTS.—

‘‘(A) IN GENERAL.—The security performance requirements established by the Director under this subsection shall be—

‘‘(i) based on the factors listed in subsection (a)(2); and

‘‘(ii) designed to remediate or mitigate identified cyber vulnerabilities and any associated consequences of an exploitation based on such vulnerabilities.

‘‘(B) CONSULTATION.—In establishing security performance requirements under this subsection, the Director shall, to the maximum extent practicable, consult with—

‘‘(i) the Director of the National Security Agency;

‘‘(ii) the Director of the National Institute of Standards and Technology;

‘‘(iii) the National Cybersecurity Advisory Council;

‘‘(iv) the heads of sector-specific agencies; and

‘‘(v) the heads of Federal agencies that are not a sector-specific agency with

responsibilities for regulating the covered critical infrastructure.

''(C) ALTERNATIVE MEASURES.—

''(i) IN GENERAL.—The owners and operators of covered critical infrastructure shall have flexibility to implement any security measure, or combination thereof, to satisfy the security performance requirements described in subparagraph (A) and the Director may not disapprove under this section any proposed security measures, or combination thereof, based on the presence or absence of any particular security measure if the proposed security measures, or combination thereof, satisfy the security performance requirements established by the Director under this section.

''(ii) RECOMMENDED SECURITY MEASURES.—The Director may recommend to an owner and operator of covered critical infrastructure a specific security measure, or combination thereof, that will satisfy the security performance requirements established by the Director. The absence of the recommended security measures, or com-

bination thereof, may not serve as the basis for a disapproval of the security measure, or combination thereof, proposed by the owner or operator of covered critical infrastructure if the proposed security measure, or combination thereof, otherwise satisfies the security performance requirements established by the Director under this section.

"SEC. 249. NATIONAL CYBER EMERGENCIES.

"(a) DECLARATION.—

"(1) IN GENERAL.—The President may issue a declaration of a national cyber emergency to covered critical infrastructure. Any declaration under this section shall specify the covered critical infrastructure subject to the national cyber emergency.

"(2) NOTIFICATION.—Upon issuing a declaration under paragraph (1), the President shall, consistent with the protection of intelligence sources and methods, notify the owners and operators of the specified covered critical infrastructure of the nature of the national cyber emergency.

"(3) AUTHORITIES.—If the President issues a declaration under paragraph (1), the Director shall—

~~"(A) immediately direct the owners and operators of covered critical infrastructure subject to the declaration under paragraph (1) to implement response plans required under section 248(b)(2)(C);~~

~~"(B) develop and coordinate emergency measures or actions necessary to preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption, of covered critical infrastructure;~~

~~"(C) ensure that emergency measures or actions directed under this section represent the least disruptive means feasible to the operations of the covered critical infrastructure;~~

~~"(D) subject to subsection (f), direct actions by other Federal agencies to respond to the national cyber emergency;~~

~~"(E) coordinate with officials of State and local governments, international partners of the United States, and private owners and operators of covered critical infrastructure specified in the declaration to respond to the national cyber emergency;~~

~~"(F) initiate a process under section 248 to address the cyber vulnerability that may be exploited by the national cyber emergency; and~~

~~"(G) provide voluntary technical assistance, if requested, under section 242(f)(1)(S).~~

~~"(4) REIMBURSEMENT.—A Federal agency shall be reimbursed for expenditures under this section from funds appropriated for the purposes of this section. Any funds received by a Federal agency as reimbursement for services or supplies furnished under the authority of this section shall be deposited to the credit of the appropriation or appropriations available on the date of the deposit for the services or supplies.~~

~~"(5) CONSULTATION.—In carrying out this section, the Director shall consult with the Secretary, the Secretary of Defense, the Director of the National Security Agency, the Director of the National Institute of Standards and Technology, and any other official, as directed by the President.~~

~~"(6) PRIVACY.—In carrying out this section, the Director shall ensure that the privacy and civil liberties of United States persons are protected.~~

~~"(b) DISCONTINUANCE OF EMERGENCY MEASURES.—~~

"(1) IN GENERAL.—Any emergency measure or action developed under this section shall cease to have effect not later than 30 days after the date on which the President issued the declaration of a national cyber emergency, unless—

"(A) the Director affirms in writing that the emergency measure or action remains necessary to address the identified national cyber emergency; and

"(B) the President issues a written order or directive reaffirming the national cyber emergency, the continuing nature of the national cyber emergency, or the need to continue the adoption of the emergency measure or action.

"(2) EXTENSIONS.—An emergency measure or action extended in accordance with paragraph (1) may—

"(A) remain in effect for not more than 30 days after the date on which the emergency measure or action was to cease to have effect; and

"(B) be extended for additional 30-day periods, if the requirements of paragraph (1) and subsection (d) are met.

''(c) COMPLIANCE WITH EMERGENCY MEASURES.—

''(1) IN GENERAL.—Subject to paragraph (2), the owner or operator of covered critical infrastructure shall immediately comply with any emergency measure or action developed by the Director under this section during the pendency of any declaration by the President under subsection (a)(1) or an extension under subsection (b)(2).

''(2) ALTERNATIVE MEASURES.—If the Director determines that a proposed security measure, or any combination thereof, submitted by the owner or operator of covered critical infrastructure in accordance with the process established under section 248(b)(2) addresses the cyber vulnerability associated with the national cyber emergency that is the subject of the declaration under this section, the owner or operator may comply with paragraph (1) of this subsection by implementing the proposed security measure, or combination thereof, approved by the Director under the process established under section 248. Before submission of a proposed security measure, or combination thereof, and during the pendency of any review by the Director under the process established under section 248, the owner or operator of covered critical infrastructure shall re-

main in compliance with any emergency measure or action developed by the Director under this section during the pendency of any declaration by the President under subsection (a)(1) or an extension under subsection (b)(2), until such time as the Director has approved an alternative proposed security measure, or combination thereof, under this paragraph.

''(3) INTERNATIONAL COOPERATION ON NATIONAL CYBER EMERGENCIES.—

''(A) IN GENERAL.—The Director, in coordination with the head of the sector-specific agency with responsibility for covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure, shall—

''(i) consistent with the protection of intelligence sources and methods and other sensitive matters, inform the owner or operator of covered critical infrastructure that is located outside of the United States and the government of the country in which the covered critical infrastructure is located of any national cyber emergency

affecting the covered critical infrastructure; and

"(ii) coordinate with the government of the country in which the covered critical infrastructure is located and, as appropriate, the owner or operator of the covered critical infrastructure, regarding the implementation of emergency measures or actions necessary to preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption, of the covered critical infrastructure.

"(B) INTERNATIONAL AGREEMENTS.—The Director shall carry out this paragraph in a manner consistent with applicable international agreements.

"(4) LIMITATION ON COMPLIANCE AUTHORITY.—The authority to direct compliance with an emergency measure or action under this section shall not authorize the Director, the Center, the Department, or any other Federal entity to compel the disclosure of information or conduct surveillance unless otherwise authorized under chapter 119, chapter 121, or chapter 206 of title 18, United States Code, the Foreign Intelligence Surveillance Act of 1978

(50 U.S.C. 1801 et seq.), or any other provision of law.

''(d) REPORTING.—

''(1) IN GENERAL.—Except as provided in paragraph (2), the President shall ensure that any declaration under subsection (a)(1) or any extension under subsection (b)(2) is reported to the appropriate committees of Congress before the Director mandates any emergency measure or actions under subsection (a)(3).

''(2) EXCEPTION.—If notice cannot be given under paragraph (1) before mandating any emergency measure or actions under subsection (a)(3), the President shall provide the report required under paragraph (1) as soon as possible, along with a statement of the reasons for not providing notice in accordance with paragraph (1).

''(3) CONTENTS.—Each report under this subsection shall describe—

''(A) the nature of the national cyber emergency;

''(B) the reasons that risk-based security requirements under section 248 are not sufficient to address the national cyber emergency; and

"(C) the actions necessary to preserve the reliable operation and mitigate the consequences of the potential disruption of covered critical infrastructure.

"(c) STATUTORY DEFENSES AND CIVIL LIABILITY LIMITATIONS FOR COMPLIANCE WITH EMERGENCY MEASURES.—

"(1) DEFINITIONS.—In this subsection—

"(A) the term 'covered civil action'—

"(i) means a civil action filed in a Federal or State court against a covered entity; and

"(ii) does not include an action brought under section 2520 or 2707 of title 18, United States Code, or section 110 or 308 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1810 and 1828);

"(B) the term 'covered entity' means any entity that owns or operates covered critical infrastructure, including any owner, operator, officer, employee, agent, landlord, custodian, or other person acting for or on behalf of that entity with respect to the covered critical infrastructure; and

"(C) the term 'noneconomic damages' means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.

"(2) APPLICATION OF LIMITATIONS ON CIVIL LIABILITY.—The limitations on civil liability under paragraph (3) apply if—

"(A) the President has issued a declaration of national cyber emergency under subsection (a)(1);

"(B) the Director has—

"(i) issued emergency measures or actions for which compliance is required under subsection (c)(1); or

"(ii) approved security measures under subsection (c)(2);

"(C) the covered entity is in compliance with—

"(i) the emergency measures or actions required under subsection (c)(1); or

‘‘(ii) security measures which the Director has approved under subsection (c)(2); and

‘‘(D)(i) the Director certifies to the court in which the covered civil action is pending that the actions taken by the covered entity during the period covered by the declaration under subsection (a)(1) were consistent with—

‘‘(I) emergency measures or actions for which compliance is required under subsection (c)(1); or

‘‘(II) security measures which the Director has approved under subsection (c)(2); or

‘‘(ii) notwithstanding the lack of a certification, the covered entity demonstrates by a preponderance of the evidence that the actions taken during the period covered by the declaration under subsection (a)(1) are consistent with the implementation of—

‘‘(I) emergency measures or actions for which compliance is required under subsection (c)(1); or

"(II) security measures which the Director has approved under subsection (c)(2).

"(3) LIMITATIONS ON CIVIL LIABILITY.—In any covered civil action that is related to any incident associated with a cyber vulnerability covered by a declaration of a national cyber emergency and for which Director has issued emergency measures or actions for which compliance is required under subsection (c)(1) or for which the Director has approved security measures under subsection (c)(2), or that is the direct consequence of actions taken in good faith for the purpose of implementing security measures or actions which the Director has approved under subsection (c)(2)—

"(A) the covered entity shall not be liable for any punitive damages intended to punish or deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses; and

"(B) noneconomic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff, and no plaintiff may recover non-

economic damages unless the plaintiff suffered physical harm.

"(4) CIVIL ACTIONS ARISING OUT OF IMPLEMENTATION OF EMERGENCY MEASURES OR ACTIONS.—A covered civil action may not be maintained against a covered entity that is the direct consequence of actions taken in good faith for the purpose of implementing specific emergency measures or actions for which compliance is required under subsection (c)(1), if—

"(A) the President has issued a declaration of national cyber emergency under subsection (a)(1) and the action was taken during the period covered by that declaration;

"(B) the Director has issued emergency measures or actions for which compliance is required under subsection (c)(1);

"(C) the covered entity is in compliance with the emergency measures required under subsection (c)(1); and

"(D)(i) the Director certifies to the court in which the covered civil action is pending that the actions taken by the entity during the period covered by the declaration under subsection (a)(1) were consistent with the implementation

of emergency measures or actions for which compliance is required under subsection (c)(1); or

''(ii) notwithstanding the lack of a certification, the entity demonstrates by a preponderance of the evidence that the actions taken during the period covered by the declaration under subsection (a)(1) are consistent with the implementation of emergency measures or actions for which compliance is required under subsection (c)(1).

''(5) CERTAIN ACTIONS NOT SUBJECT TO LIMITATIONS ON LIABILITY.—

''(A) ADDITIONAL OR INTERVENING ACTS.—Paragraphs (2) through (4) shall not apply to a civil action relating to any additional or intervening acts or omissions by any covered entity.

''(B) SERIOUS OR SUBSTANTIAL DAMAGE.—Paragraph (4) shall not apply to any civil action brought by an individual—

''(i) whose recovery is otherwise precluded by application of paragraph (4); and

''(ii) who has suffered—

"(I) serious physical injury or death; or

"(II) substantial damage or destruction to his primary residence.

"(C) RULE OF CONSTRUCTION.—Recovery available under subparagraph (B) shall be limited to those damages available under subparagraphs (A) and (B) of paragraph (3), except that neither reasonable and necessary medical benefits nor lifetime total benefits for lost employment income due to permanent and total disability shall be limited herein.

"(D) INDEMNIFICATION.—In any civil action brought under subparagraph (B), the United States shall defend and indemnify any covered entity. Any covered entity defended and indemnified under this subparagraph shall fully cooperate with the United States in the defense by the United States in any proceeding and shall be reimbursed the reasonable costs associated with such cooperation.

"(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to—

"(1) alter or supersede the authority of the Secretary of Defense, the Attorney General, or the Di-

rector of National Intelligence in responding to a national cyber emergency; or

''(2) limit the authority of the Director under section 248, after a declaration issued under this section expires.

''SEC. 250. ENFORCEMENT.

''(a) ANNUAL CERTIFICATION OF COMPLIANCE.—

''(1) IN GENERAL.—Not later than 6 months after the date on which the Director promulgates regulations under section 248(b), and every year thereafter, each owner or operator of covered critical infrastructure shall certify in writing to the Director whether the owner or operator has developed and implemented, or is implementing, security measures approved by the Director under section 248 and any applicable emergency measures or actions required under section 249 for any cyber vulnerabilities and national cyber emergencies.

''(2) FAILURE TO COMPLY.—If an owner or operator of covered critical infrastructure fails to submit a certification in accordance with paragraph (1), or if the certification indicates the owner or operator is not in compliance, the Director may issue an order requiring the owner or operator to submit proposed security measures under section 248 or com-

ply with specific emergency measures or actions under section 249.

''(b) RISK-BASED EVALUATIONS.—

''(1) IN GENERAL.—Consistent with the factors described in paragraph (3), the Director may perform an evaluation of the information infrastructure of any specific system or asset constituting covered critical infrastructure to assess the validity of a certification of compliance submitted under subsection (a)(1).

''(2) DOCUMENT REVIEW AND INSPECTION.—An evaluation performed under paragraph (1) may include—

''(A) a review of all documentation submitted to justify an annual certification of compliance submitted under subsection (a)(1); and

''(B) a physical or electronic inspection of relevant information infrastructure to which the security measures required under section 248 or the emergency measures or actions required under section 249 apply.

''(3) EVALUATION SELECTION FACTORS.—In determining whether sufficient risk exists to justify an evaluation under this subsection, the Director shall consider—

~~"(A) the specific cyber vulnerabilities affecting or potentially affecting the information infrastructure of the specific system or asset constituting covered critical infrastructure;~~

~~"(B) any reliable intelligence or other information indicating a cyber vulnerability or credible national cyber emergency to the information infrastructure of the specific system or asset constituting covered critical infrastructure;~~

~~"(C) actual knowledge or reasonable suspicion that the certification of compliance submitted by a specific owner or operator of covered critical infrastructure is false or otherwise inaccurate;~~

~~"(D) a request by a specific owner or operator of covered critical infrastructure for such an evaluation; and~~

~~"(E) such other risk-based factors as identified by the Director.~~

~~"(4) SECTOR-SPECIFIC AGENCIES.—To carry out the risk-based evaluation authorized under this subsection, the Director may use the resources of a sector-specific agency with responsibility for the covered critical infrastructure or any Federal agency~~

that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure with the concurrence of the head of the agency.

''(5) INFORMATION PROTECTION.—Information provided to the Director during the course of an evaluation under this subsection shall be protected from disclosure in accordance with section 251.

''(c) CIVIL PENALTIES.—

''(1) IN GENERAL.—Any person who violates section 248 or 249 shall be liable for a civil penalty.

''(2) NO PRIVATE RIGHT OF ACTION.—Nothing in this section confers upon any person, except the Director, a right of action against an owner or operator of covered critical infrastructure to enforce any provision of this subtitle.

''(d) LIMITATION ON CIVIL LIABILITY.—

''(1) DEFINITION.—In this subsection—

''(A) the term 'covered civil action'—

''(i) means a civil action filed in a Federal or State court against a covered entity; and

''(ii) does not include an action brought under section 2520 or 2707 of title 18, United States Code, or section 110 or 308 of the Foreign Intelligence

Surveillance Act of 1978 (50 U.S.C. 1810 and 1828);

''(B) the term 'covered entity' means any entity that owns or operates covered critical infrastructure, including any owner, operator, officer, employee, agent, landlord, custodian, or other person acting for or on behalf of that entity with respect to the covered critical infrastructure; and

''(C) the term 'noneconomic damages' means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.

''(2) LIMITATIONS ON CIVIL LIABILITY.—If a covered entity experiences an incident related to a cyber vulnerability identified under section 248(a), in any covered civil action for damages directly caused by the incident related to that cyber vulnerability—

''(A) the covered entity shall not be liable for any punitive damages intended to punish or

deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses; and

"(B) noneconomic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff, and no plaintiff may recover noneconomic damages unless the plaintiff suffered physical harm.

"(3) APPLICATION.—This subsection shall apply to claims made by any individual or nongovernmental entity, including claims made by a State or local government agency on behalf of such individuals or nongovernmental entities, against a covered entity—

"(A) whose proposed security measures, or combination thereof, satisfy the security performance requirements established under subsection 248(b) and have been approved by the Director;

"(B) that has been evaluated under subsection (b) and has been found by the Director to have implemented the proposed security measures approved under section 248; and

"(C) that is in actual compliance with the approved security measures at the time of the incident related to that cyber vulnerability.

"(4) LIMITATION.—This subsection shall only apply to harm directly caused by the incident related to the cyber vulnerability and shall not apply to damages caused by any additional or intervening acts or omissions by the covered entity.

"(5) RULE OF CONSTRUCTION.—Except as provided under paragraph (3), nothing in this subsection shall be construed to abrogate or limit any right, remedy, or authority that the Federal Government or any State or local government, or any entity or agency thereof, may possess under any law, or that any individual is authorized by law to bring on behalf of the government.

"(c) REPORT TO CONGRESS.—The Director shall submit an annual report to the appropriate committees of Congress on the implementation and enforcement of the risk-based performance requirements of covered critical infrastructure under subsection 248(b) and this section including—

"(1) the level of compliance of covered critical infrastructure with the risk-based security performance requirements issued under section 248(b);

''(2) how frequently the evaluation authority under subsection (b) was utilized and a summary of the aggregate results of the evaluations; and

''(3) any civil penalties imposed on covered critical infrastructure.

''SEC. 251. PROTECTION OF INFORMATION.

''(a) DEFINITION.—In this section, the term 'covered information'—

''(1) means—

''(A) any information required to be submitted under sections 246, 248, and 249 to the Center by the owners and operators of covered critical infrastructure; and

''(B) any information submitted to the Center under the processes and procedures established under section 246 by State and local governments, private entities, and international partners of the United States regarding threats, vulnerabilities, and incidents affecting—

''(i) the Federal information infrastructure;

''(ii) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of

Defense, a military department, or another element of the intelligence community; or

"(iii) the national information infrastructure; and

"(2) shall not include any information described under paragraph (1), if that information is submitted to—

"(A) conceal violations of law, inefficiency, or administrative error;

"(B) prevent embarrassment to a person, organization, or agency; or

"(C) interfere with competition in the private sector.

"(b) VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.—Covered information submitted in accordance with this section shall be treated as voluntarily shared critical infrastructure information under section 214, except that the requirement of section 214 that the information be voluntarily submitted, including the requirement for an express statement, shall not be required for submissions of covered information.

"(c) GUIDELINES.—

"(1) IN GENERAL.—Subject to paragraph (2), the Director shall develop and issue guidelines, in consultation with the Secretary, Attorney General,

and the National Cybersecurity Advisory Council, as necessary to implement this section.

"(2) REQUIREMENTS.—The guidelines developed under this section shall—

"(A) consistent with section 214(c)(2)(D) and (g) and the guidelines developed under section 246(b)(3), include provisions for information sharing among Federal, State, and local and officials, private entities, or international partners of the United States necessary to carry out the authorities and responsibilities of the Director;

"(B) be consistent, to the maximum extent possible, with policy guidance and implementation standards developed by the National Archives and Records Administration for controlled unclassified information, including with respect to marking, safeguarding, dissemination and dispute resolution; and

"(C) describe, with as much detail as possible, the categories and type of information entities should voluntarily submit under subsections (b) and (c)(1)(B) of section 246.

"(d) PROCESS FOR REPORTING SECURITY PROBLEMS.—

"(1) ESTABLISHMENT OF PROCESS.—The Director shall establish through regulation, and provide information to the public regarding, a process by which any person may submit a report to the Secretary regarding cybersecurity threats, vulnerabilities, and incidents affecting—

"(A) the Federal information infrastructure;

"(B) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community; or

"(C) national information infrastructure.

"(2) ACKNOWLEDGMENT OF RECEIPT.—If a report submitted under paragraph (1) identifies the person making the report, the Director shall respond promptly to such person and acknowledge receipt of the report.

"(3) STEPS TO ADDRESS PROBLEM.—The Director shall review and consider the information provided in any report submitted under paragraph (1) and, at the sole, unreviewable discretion of the Director, determine what, if any, steps are necessary

or appropriate to address any problems or deficiencies identified.

''(4) DISCLOSURE OF IDENTITY.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), or with the written consent of the person, the Secretary may not disclose the identity of a person who has provided information described in paragraph (1).

''(B) REFERRAL TO THE ATTORNEY GENERAL.—The Secretary shall disclose to the Attorney General the identity of a person described under subparagraph (A) if the matter is referred to the Attorney General for enforcement. The Director shall provide reasonable advance notice to the affected person if disclosure of that person's identity is to occur, unless such notice would risk compromising a criminal or civil enforcement investigation or proceeding.

''(e) RULES OF CONSTRUCTION.—Nothing in this section shall be construed to—

''(1) limit or otherwise affect the right, ability, duty, or obligation of any entity to use or disclose any information of that entity, including in the conduct of any judicial or other proceeding;

''(2) prevent the classification of information submitted under this section if that information meets the standards for classification under Executive Order 12958 or any successor of that order;

''(3) limit the right of an individual to make any disclosure—

''(A) protected or authorized under section 2302(b)(8) or 7211 of title 5, United States Code;

''(B) to an appropriate official of information that the individual reasonably believes evidences a violation of any law, rule, or regulation, gross mismanagement, or substantial and specific danger to public health, safety, or security, and that is protected under any Federal or State law (other than those referenced in subparagraph (A)) that shields the disclosing individual against retaliation or discrimination for having made the disclosure if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs; or

"(C) to the Special Counsel, the inspector general of an agency, or any other employee designated by the head of an agency to receive similar disclosures;

"(4) prevent the Director from using information required to be submitted under sections 246, 248, or 249 for enforcement of this subtitle, including enforcement proceedings subject to appropriate safeguards;

"(5) authorize information to be withheld from Congress, the Government Accountability Office, or Inspector General of the Department; or

"(6) create a private right of action for enforcement of any provision of this section.

"(f) AUDIT.—

"(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Protecting Cyberspace as a National Asset Act of 2010, the Inspector General of the Department shall conduct an audit of the management of information submitted under subsection (b) and report the findings to appropriate committees of Congress.

"(2) CONTENTS.—The audit under paragraph (1) shall include assessments of—

''(A) whether the information is adequately safeguarded against inappropriate disclosure;

''(B) the processes for marking and disseminating the information and resolving any disputes;

''(C) how the information is used for the purposes of this section, and whether that use is effective;

''(D) whether information sharing has been effective to fulfill the purposes of this section;

''(E) whether the kinds of information submitted have been appropriate and useful, or overbroad or overnarrow;

''(F) whether the information protections allow for adequate accountability and transparency of the regulatory, enforcement, and other aspects of implementing this subtitle; and

''(G) any other factors at the discretion of the Inspector General.

''SEC. 252. SECTOR-SPECIFIC AGENCIES.

''(a) IN GENERAL.—The head of each sector-specific agency and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating covered critical infrastructure shall coordinate with the Director on any activities of the sector-specific agency or

Federal agency that relate to the efforts of the agency regarding security or resiliency of the national information infrastructure, including critical infrastructure and covered critical infrastructure, within or under the supervision of the agency.

''(b) DUPLICATIVE REPORTING REQUIREMENTS.—The head of each sector-specific agency and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating covered critical infrastructure shall coordinate with the Director to eliminate and avoid the creation of duplicate reporting or compliance requirements relating to the security or resiliency of the national information infrastructure, including critical infrastructure and covered critical infrastructure, within or under the supervision of the agency.

''(c) REQUIREMENTS.—

''(1) IN GENERAL.—To the extent that the head of each sector-specific agency and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating covered critical infrastructure has the authority to establish regulations, rules, or requirements or other required actions that are applicable to the security of national information infrastructure, including critical infra-

structure and covered critical infrastructure, the head of that agency shall—

"(A) notify the Director in a timely fashion of the intent to establish the regulations, rules, requirements, or other required actions;

"(B) coordinate with the Director to ensure that the regulations, rules, requirements, or other required actions are consistent with, and do not conflict or impede, the activities of the Director under sections 247, 248, and 249; and

"(C) in coordination with the Director, ensure that the regulations, rules, requirements, or other required actions are implemented, as they relate to covered critical infrastructure, in accordance with subsection (a).

"(2) COORDINATION.—Coordination under paragraph (1)(B) shall include the active participation of the Director in the process for developing regulations, rules, requirements, or other required actions.

"(3) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide additional authority for any sector-specific agency or any Federal agency that is not a sector-specific agency with

responsibilities for regulating national information infrastructure, including critical infrastructure or covered critical infrastructure, to establish standards or other measures that are applicable to the security of national information infrastructure not otherwise authorized by law.

"SEC. 253. STRATEGY FOR FEDERAL CYBERSECURITY SUPPLY CHAIN MANAGEMENT.

''(a) IN GENERAL.—The Secretary, in consultation with the Director of Cyberspace Policy, the Director, the Secretary of Defense, the Secretary of Commerce, the Secretary of State, the Director of National Intelligence, the Administrator of General Services, the Administrator for Federal Procurement Policy, the other members of the Chief Information Officers Council established under section 3603 of title 44, United States Code, the Chief Acquisition Officers Council established under section 16A of the Office of Federal Procurement Policy Act (41 U.S.C. 414b), the Chief Financial Officers Council established under section 302 of the Chief Financial Officers Act of 1990 (31 U.S.C. 901 note), and the private sector, shall develop, periodically update, and implement a supply chain risk management strategy designed to ensure the security of the Federal information infrastructure, including protection against unauthorized access to, alteration of infor-

mation in, disruption of operations of, interruption of communications or services of, and insertion of malicious software, engineering vulnerabilities, or otherwise corrupting software, hardware, services, or products intended for use in Federal information infrastructure.

''(b) CONTENTS.—The supply chain risk management strategy developed under subsection (a) shall—

''(1) address risks in the supply chain during the entire life cycle of any part of the Federal information infrastructure;

''(2) place particular emphasis on—

''(A) securing critical information systems and the Federal information infrastructure;

''(B) developing processes that—

''(i) incorporate all-source intelligence analysis into assessments of the supply chain for the Federal information infrastructure;

''(ii) assess risks from potential suppliers providing critical components or services of the Federal information infrastructure;

''(iii) assess risks from individual components, including all subcomponents,

or software used in or affecting the Federal information infrastructure;

''(iv) manage the quality, configuration, and security of software, hardware, and systems of the Federal information infrastructure throughout the life cycle of the software, hardware, or system, including components or subcomponents from secondary and tertiary sources;

''(v) detect the occurrence, reduce the likelihood of occurrence, and mitigate or remediate the risks associated with products containing counterfeit components or malicious functions;

''(vi) enhance developmental and operational test and evaluation capabilities, including software vulnerability detection methods and automated tools that shall be integrated into acquisition policy practices by Federal agencies and, where appropriate, make the capabilities available for use by the private sector; and

''(vii) protect the intellectual property and trade secrets of suppliers of informa-

tion and communications technology products and services;

"(C) the use of internationally-recognized standards and standards developed by the private sector and developing a process, with the National Institute for Standards and Technology, to make recommendations for improvements of the standards;

"(D) identifying acquisition practices of Federal agencies that increase risks in the supply chain and developing a process to provide recommendations for revisions to those processes; and

"(E) sharing with the private sector, to the fullest extent possible, the threats identified in the supply chain and working with the private sector to develop responses to those threats as identified; and

"(3) to the extent practicable, promote the ability of Federal agencies to procure commercial off the shelf information and communications technology products and services from a diverse pool of suppliers.

"(c) IMPLEMENTATION.—The Federal Acquisition Regulatory Council established under section 25(a) of the

Office of Federal Procurement Policy Act (41 U.S.C. 421(a)) shall—

"(1) amend the Federal Acquisition Regulation issued under section 25 of that Act to—

"(A) incorporate, where relevant, the supply chain risk management strategy developed under subsection (a) to improve security throughout the acquisition process; and

"(B) direct that all software and hardware purchased by the Federal Government shall comply with standards developed or be interoperable with automated tools approved by the National Institute of Standards and Technology, to continually enhance security; and

"(2) develop a clause or set of clauses for inclusion in solicitations, contracts, and task and delivery orders that sets forth the responsibility of the contractor under the Federal Acquisition Regulation provisions implemented under this subsection.".

TITLE III—FEDERAL INFORMATION SECURITY MANAGEMENT

SEC. 301. COORDINATION OF FEDERAL INFORMATION POLICY.

(a) FINDINGS.—Congress finds that—

(1) since 2002 the Federal Government has experienced multiple high-profile incidents that resulted in the theft of sensitive information amounting to more than the entire print collection contained in the Library of Congress, including personally identifiable information, advanced scientific research, and prenegotiated United States diplomatic positions; and

(2) chapter 35 of title 44, United States Code, must be amended to increase the coordination of Federal agency activities and to enhance situational awareness throughout the Federal Government using more effective enterprise-wide automated monitoring, detection, and response capabilities.

(b) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

"SUBCHAPTER II—INFORMATION SECURITY

"§ 3550. Purposes

"The purposes of this subchapter are to—

"(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support the Federal information infrastructure and the operations and assets of agencies;

~~"(2) recognize the highly networked nature of the current Federal information infrastructure and provide effective Government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;~~

~~"(3) provide for development and maintenance of prioritized and risk-based security controls required to protect Federal information infrastructure and information systems;~~

~~"(4) provide a mechanism for improved oversight of Federal agency information security programs;~~

~~"(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the Nation that are designed, built, and operated by the private sector; and~~

~~"(6) recognize that the selection of specific technical hardware and software information secu-~~

rity solutions should be left to individual agencies from among commercially developed products.

"§ 3551. Definitions

"(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

"(b) ADDITIONAL DEFINITIONS.—In this subchapter:

"(1) The term 'agency information infrastructure'—

"(A) means information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, an agency, including information systems used or operated by another entity on behalf of the agency; and

"(B) does not include national security systems.

"(2) The term 'automated and continuous monitoring' means monitoring at a frequency and sufficiency such that the data exchange requires little to no human involvement and is not interrupted;

"(3) The term 'incident' means an occurrence that—

"(A) actually or potentially jeopardizes—

"(i) the information security of an information system; or

‘‘(ii) the information the system processes, stores, or transmits; or

‘‘(B) constitutes a violation or threat of violation of security policies, security procedures, or acceptable use policies.

‘‘(4) The term ‘information infrastructure’ means the underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including programmable electronic devices and communications networks and any associated hardware, software, or data.

‘‘(5) The term ‘information security’ means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

‘‘(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

‘‘(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

''(C) availability, by ensuring timely and reliable access to and use of information.

''(6) The term 'information technology' has the meaning given that term in section 11101 of title 40.

''(7) The term 'management controls' means safeguards or countermeasures for an information system that focus on the management of risk and the management of information system security.

''(8)(A) The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) that is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(9) The term 'operational controls' means the safeguards and countermeasures for an information system that are primarily implemented and executed by individuals, not systems.

''(10) The term 'risk' means the potential for an unwanted outcome resulting from an incident, as determined by the likelihood of the occurrence of the incident and the associated consequences, including potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident.

''(11) The term 'risk-based security' means security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification, of information, including assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability.

''(12) The term 'security controls' means the management, operational, and technical controls prescribed for an information system to protect the information security of the system.

''(13) The term 'technical controls' means the safeguards or countermeasures for an information system that are primarily implemented and executed by the information system through mechanism contained in the hardware, software, or firmware components of the system.

''§ 3552. Authority and functions of the National Center for Cybersecurity and Communications

''(a) IN GENERAL.—The Director of the National Center for Cybersecurity and Communications shall—

''(1) develop, oversee the implementation of, and enforce policies, principles, and guidelines on information security, including through ensuring time-

ly agency adoption of and compliance with standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and subtitle E of title H of the Homeland Security Act of 2002;

"(2) provide to agencies security controls that agencies shall be required to be implemented to mitigate and remediate vulnerabilities, attacks, and exploitations discovered as a result of activities required under this subchapter or subtitle E of title H of the Homeland Security Act of 2002;

"(3) to the extent practicable—

"(A) prioritize the policies, principles, standards, and guidelines promulgated under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), paragraph (1), and subtitle E of title H of the Homeland Security Act of 2002, based upon the risk of an incident; and

"(B) develop guidance that requires agencies to monitor, including automated and continuous monitoring of, the effective implementation of policies, principles, standards, and guidelines developed under section 20 of the National Institute of Standards and Technology

Act (15 U.S.C. 278g–3), paragraph (1), and subtitle E of title H of the Homeland Security Act of 2002;

"(C) ensure the effective operation of technical capabilities within the National Center for Cybersecurity and Communications to enable automated and continuous monitoring of any information collected as a result of the guidance developed under subparagraph (B) and use the information to enhance the risk-based security of the Federal information infrastructure; and

"(D) ensure the effective operation of a secure system that satisfies information reporting requirements under sections 3553(c) and 3556(c);

"(4) require agencies, consistent with the standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) or paragraph (1) and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk resulting from the disruption or unauthorized access, use, disclosure, modification, or destruction of—

"(A) information collected or maintained by or on behalf of an agency; or

"(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

"(5) oversee agency compliance with the requirements of this subchapter, including coordinating with the Office of Management and Budget to use any authorized action under section 11303 of title 40 to enforce accountability for compliance with such requirements;

"(6) review, at least annually, and approve or disapprove, agency information security programs required under section 3553(b); and

"(7) coordinate information security policies and procedures with the Administrator for Electronic Government and the Administrator for the Office of Information and Regulatory Affairs with related information resources management policies and procedures.

"(b) NATIONAL SECURITY SYSTEMS.—The authorities of the Director under this section shall not apply to national security systems.

"§ 3553. Agency responsibilities

"(a) IN GENERAL.—The head of each agency shall—

"(1) be responsible for—

"(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

"(i) information collected or maintained by or on behalf of the agency; and

"(ii) agency information infrastructure;

"(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

"(i) information security requirements, including security controls, developed by the Director of the National Center for Cybersecurity and Communications under section 3552, subtitle E of title H of the Homeland Security Act of 2002, or any other provision of law;

"(ii) information security policies, principles, standards, and guidelines promulgated under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and section 3552(a)(1);

‘‘(iii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

‘‘(iv) ensuring the standards implemented for information systems and national security systems of the agency are complementary and uniform, to the extent practicable;

‘‘(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes, including policies, procedures, and practices described in subsection (c)(1)(C);

‘‘(D) as appropriate, maintaining secure facilities that have the capability of accessing, sending, receiving, and storing classified information;

‘‘(E) maintaining a sufficient number of personnel with security clearances, at the appropriate levels, to access, send, receive and analyze classified information to carry out the responsibilities of this subchapter; and

‘‘(F) ensuring that information security performance indicators and measures are in-

cluded in the annual performance evaluations of all managers, senior managers, senior executive service personnel, and political appointees;

"(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under the control of those officials, including through—

"(A) assessing the risk and magnitude of the harm that could result from the disruption or unauthorized access, use, disclosure, modification, or destruction of such information or information systems;

"(B) determining the levels of information security appropriate to protect such information and information systems in accordance with policies, principles, standards, and guidelines promulgated under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), section 3552(a)(1), and subtitle E of title II of the Homeland Security Act of 2002, for information security categorizations and related requirements;

"(C) implementing policies and procedures to cost effectively reduce risks to an acceptable level;

"(D) periodically testing and evaluating information security controls and techniques to ensure that such controls and techniques are operating effectively; and

"(E) withholding all bonus and cash awards to senior agency officials accountable for the operation of such agency information infrastructure that are recognized by the Chief Information Security Officer as impairing the risk-based security information, information system, or agency information infrastructure;

"(3) delegate to a senior agency officer designated as the Chief Information Security Officer the authority and budget necessary to ensure and enforce compliance with the requirements imposed on the agency under this subchapter, subtitle E of title II of the Homeland Security Act of 2002, or any other provision of law, including—

"(A) overseeing the establishment, maintenance, and management of a security operations center that has technical capabilities that

can, through automated and continuous monitoring—

"(i) detect, report, respond to, contain, remediate, and mitigate incidents that impair risk-based security of the information, information systems, and agency information infrastructure, in accordance with policy provided by the National Center for Cybersecurity and Communications;

"(ii) monitor and, on a risk-based basis, mitigate and remediate the vulnerabilities of every information system within the agency information infrastructure;

"(iii) continually evaluate risks posed to information collected or maintained by or on behalf of the agency and information systems and hold senior agency officials accountable for ensuring the risk-based security of such information and information systems;

"(iv) collaborate with the National Center for Cybersecurity and Communications and appropriate public and private

sector security operations centers to address incidents that impact the security of information and information systems that extend beyond the control of the agency; and

"(v) report any incident described under clauses (i) and (ii), as directed by the policy of the National Center for Cybersecurity and Communications or the Inspector General of the agency;

"(B) collaborating with the Administrator for E–Government and the Chief Information Officer to establish, maintain, and update an enterprise network, system, storage, and security architecture, that can be accessed by the National Cybersecurity Communications Center and includes—

"(i) information on how security controls are implemented throughout the agency information infrastructure; and

"(ii) information on how the controls described under subparagraph (A) maintain the appropriate level of confidentiality, integrity, and availability of information and information systems based on—

"(I) the policy of the National Center for Cybersecurity and Communications; and

"(II) the standards or guidance developed by the National Institute of Standards and Technology;

"(C) developing, maintaining, and overseeing an agency-wide information security program as required by subsection (b);

"(D) developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3552;

"(E) training, consistent with the requirements of section 406 of the Protecting Cyberspace as a National Asset Act of 2010, and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

"(F) assisting senior agency officers concerning their responsibilities under paragraph (2);

"(4) ensure that the Chief Information Security Officer has a sufficient number of cleared and

trained personnel with technical skills identified by the National Center for Cybersecurity and Communications as critical to maintaining the risk-based security of agency information infrastructure as required by the subchapter and other applicable laws;

"(5) ensure that the agency Chief Information Security Officer, in coordination with appropriate senior agency officials, reports not less than annually to the head of the agency on the effectiveness of the agency information security program, including progress of remedial actions;

"(6) ensure that the Chief Information Security Officer—

"(A) possesses necessary qualifications, including education, professional certifications, training, experience, and the security clearance required to administer the functions described under this subchapter; and

"(B) has information security duties as the primary duty of that officer; and

"(7) ensure that components of that agency establish and maintain an automated reporting mechanism that allows the Chief Information Security Officer with responsibility for the entire agency, and all components thereof, to implement, monitor, and hold

senior agency officers accountable for the implementation of appropriate security policies, procedures, and controls of agency components.

''(b) AGENCY-WIDE INFORMATION SECURITY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program, approved by the National Center for Cybersecurity and Communications under section 3552(a)(6) and consistent with components across and within agencies, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

''(1) frequent assessments, at least twice each month—

''(A) of the risk and magnitude of the harm that could result from the disruption or unauthorized access, use, disclosure, modification, or destruction of information and information systems that support the operations and assets of the agency; and

''(B) that assess whether information or information systems should be removed or migrated to more secure networks or standards and make recommendations to the head of the

agency and the Director of the National Center for Cybersecurity and Communications based on that assessment;

"(2) consistent with guidance developed under section 3554, vulnerability assessments and penetration tests commensurate with the risk posed to an agency information infrastructure;

"(3) ensure that information security vulnerabilities are remediated or mitigated based on the risk posed to the agency;

"(4) policies and procedures that—

"(A) are informed and revised by the assessments required under paragraphs (1) and (2);

"(B) cost effectively reduce information security risks to an acceptable level;

"(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

"(D) ensure compliance with—

"(i) the requirements of this subchapter;

"(ii) policies and procedures prescribed by the National Center for Cybersecurity and Communications;

~~"(iii) minimally acceptable system configuration requirements, as determined by the National Center for Cybersecurity and Communications; and~~

~~"(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;~~

~~"(5) subordinate plans for providing risk-based information security for networks, facilities, and systems or groups of information systems, as appropriate;~~

~~"(6) role-based security awareness training, consistent with the requirements of section 406 of the Protecting Cyberspace as a National Asset Act of 2010, to inform personnel with access to the agency network, including contractors and other users of information systems that support the operations and assets of the agency, of—~~

~~"(A) information security risks associated with agency activities; and~~

~~"(B) agency responsibilities in complying with agency policies and procedures designed to reduce those risks;~~

‘‘(7) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a rigor and frequency depending on risk, which shall include—

‘‘(A) testing and evaluation not less than twice each year of security controls of information collected or maintained by or on behalf of the agency and every information system identified in the inventory required under section 3505(c);

‘‘(B) the effectiveness of ongoing monitoring, including automated and continuous monitoring, vulnerability scanning, and intrusion detection and prevention of incidents posed to the risk-based security of information and information systems as required under subsection (a)(3); and

‘‘(C) testing relied on in—

‘‘(i) an operational evaluation under section 3554;

‘‘(ii) an independent assessment under section 3556; or

‘‘(iii) another evaluation, to the extent specified by the Director;

"(8) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

"(9) procedures for detecting, reporting, and responding to incidents, consistent with requirements issued under section 3552, that include—

"(A) to the extent practicable, automated and continuous monitoring of the use of information and information systems;

"(B) requirements for mitigating risks and remediating vulnerabilities associated with such incidents systemically within the agency information infrastructure before substantial damage is done; and

"(C) notifying and coordinating with the National Center for Cybersecurity and Communications, as required by this subchapter, subtitle E of title H of the Homeland Security Act of 2002, and any other provision of law; and

"(10) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

"(c) AGENCY REPORTING.—

"(1) IN GENERAL.—Each agency shall—

‘‘(A) ensure that information relating to the adequacy and effectiveness of information security policies, procedures, and practices, is available to the entities identified under paragraph (2) through the system developed under section 3552(a)(3), including information relating to—

‘‘(i) compliance with the requirements of this subchapter;

‘‘(ii) the effectiveness of the information security policies, procedures, and practices of the agency based on a determination of the aggregate effect of identified deficiencies and vulnerabilities;

‘‘(iii) an identification and analysis of any significant deficiencies identified in such policies, procedures, and practices;

‘‘(iv) an identification of any vulnerability that could impair the risk-based security of the agency information infrastructure; and

‘‘(v) results of any operational evaluation conducted under section 3554 and plans of action to address the deficiencies

and vulnerabilities identified as a result of such operational evaluation;

''(B) follow the policy, guidance, and standards of the National Center for Cybersecurity and Communications, in consultation with the Federal Information Security Taskforce, to continually update, and ensure the electronic availability of both a classified and unclassified version of the information required under subparagraph (A);

''(C) ensure the information under subparagraph (A) addresses the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

''(i) annual agency budgets;

''(ii) information resources management of this subchapter;

''(iii) information technology management and procurement under this chapter or any other applicable provision of law;

''(iv) subtitle E of title H of the Homeland Security Act of 2002;

''(v) program performance under sections 1105 and 1115 through 1119 of title

~~31, and sections 2801 and 2805 of title 39;~~

~~"(vi) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);~~

~~"(vii) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note);~~

~~"(viii) internal accounting and administrative controls under section 3512 of title 31; and~~

~~"(ix) performance ratings, salaries, and bonuses provided to the senior managers and supporting personnel taking into account program performance as it relates to complying with this subchapter; and~~

~~"(D) report any significant deficiency in a policy, procedure, or practice identified under subparagraph (A) or (B)—~~

~~"(i) as a material weakness in reporting under section 3512 of title 31; and~~

~~"(ii) if relating to financial management systems, as an instance of a lack of~~

substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

"(2) ADEQUACY AND EFFECTIVENESS INFORMATION.—Information required under paragraph (1)(A) shall, to the extent possible and in accordance with applicable law, policy, guidance, and standards, be available on an automated and continuous basis to—

"(A) the National Center for Cybersecurity and Communications;

"(B) the Committee on Homeland Security and Governmental Affairs of the Senate;

"(C) the Committee on Government Oversight and Reform of the House of Representatives;

"(D) the Committee on Homeland Security of the House of Representatives;

"(E) other appropriate authorization and appropriations committees of Congress;

"(F) the Inspector General of the Federal agency; and

"(G) the Comptroller General.

"(d) INCLUSIONS IN PERFORMANCE PLANS.—

''(1) IN GENERAL.—In addition to the requirements of subsection (c), each agency, in consultation with the National Center for Cybersecurity and Communications, shall include as part of the performance plan required under section 1115 of title 31 a description of the time periods the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

''(2) RISK ASSESSMENTS.—The description under paragraph (1) shall be based on the risk and vulnerability assessments required under subsection (b) and evaluations required under section 3554.

''(c) NOTICE AND COMMENT.—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

''(f) MORE STRINGENT STANDARDS.—The head of an agency may employ standards for the cost effective information security for information systems within or under the supervision of that agency that are more stringent than the standards the Director of the National Center for Cybersecurity and Communications prescribes under this subchapter, subtitle E of title H of the Home-

land Security Act of 2002, or any other provision of law, if the more stringent standards—

"(1) contain at least the applicable standards made compulsory and binding by the Director of the National Center for Cybersecurity and Communications; and

"(2) are otherwise consistent with policies and guidelines issued under section 3552.

"§ 3554. Annual operational evaluation

"(a) GUIDANCE.—

"(1) IN GENERAL.—Each year the National Center for Cybersecurity and Communications shall oversee, coordinate, and develop guidance for the effective implementation of operational evaluations of the Federal information infrastructure and agency information security programs and practices to determine the effectiveness of such program and practices.

"(2) COLLABORATION IN DEVELOPMENT.—In developing guidance for the operational evaluations described under this section, the National Center for Cybersecurity and Communications shall collaborate with the Federal Information Security Taskforce and the Council of Inspectors General on Integrity and Efficiency, and other agencies as necessary, to

develop and update risk-based performance indicators and measures that assess the adequacy and effectiveness of information security of an agency and the Federal information infrastructure.

''(3) CONTENTS OF OPERATIONAL EVALUATION.—Each operational evaluation under this section—

''(A) shall be prioritized based on risk; and

''(B) shall—

''(i) test the effectiveness of agency information security policies, procedures, and practices of the information systems of the agency, or a representative subset of those information systems;

''(ii) assess (based on the results of the testing) compliance with—

''(I) the requirements of this subchapter; and

''(II) related information security policies, procedures, standards, and guidelines;

''(iii) evaluate whether agencies—

''(I) effectively monitor, detect, analyze, protect, report, and respond to vulnerabilities and incidents;

"(II) report to and collaborate with the appropriate public and private security operation centers, the National Center for Cybersecurity and Communications, and law enforcement agencies; and

"(III) remediate or mitigate the risk posed by attacks and exploitations in a timely fashion in order to prevent future vulnerabilities and incidents; and

"(iv) identify deficiencies of agency information security policies, procedures, and controls on the agency information infrastructure.

"(b) CONDUCT AN OPERATIONAL EVALUATION.—

"(1) IN GENERAL.—Except as provided under paragraph (2), and in consultation with the Chief Information Officer and senior officials responsible for the affected systems, the Chief Information Security Officer of each agency shall not less than annually—

"(A) conduct an operational evaluation of the agency information infrastructure for

vulnerabilities, attacks, and exploitations of the agency information infrastructure;

"(B) evaluate the ability of the agency to monitor, detect, correlate, analyze, report, and respond to incidents; and

"(C) report to the head of the agency, the National Center for Cybersecurity and Communications, the Chief Information Officer, and the Inspector General for the agency the findings of the operational evaluation.

"(2) SATISFACTION OF REQUIREMENTS BY OTHER EVALUATION.—Unless otherwise specified by the Director of the National Center for Cybersecurity and Communications, if the National Center for Cybersecurity and Communications conducts an operational evaluation of the agency information infrastructure under section 245(b)(2)(A) of the Homeland Security Act of 2002, the Chief Information Security Officer may deem the requirements of paragraph (1) satisfied for the year in which the operational evaluation described under this paragraph is conducted.

"(c) CORRECTIVE MEASURES MITIGATION AND REMEDIATION PLANS.—

~~"(1) IN GENERAL.—In consultation with the National Center for Cybersecurity and Communications and the Chief Information Officer, Chief Information Security Officers shall remediate or mitigate vulnerabilities in accordance with this subsection.~~

~~"(2) RISK-BASED PLAN.—After an operational evaluation is conducted under this section or under section 245(b) of the Homeland Security Act of 2002, the agency shall submit to the National Center for Cybersecurity and Communications in a timely fashion a risk-based plan for addressing recommendations and mitigating and remediating vulnerabilities identified as a result of such operational evaluation, including a timeline and budget for implementing such plan.~~

~~"(3) APPROVAL OR DISAPPROVAL.—Not later than 15 days after receiving a plan submitted under paragraph (2), the National Center for Cybersecurity and Communications shall—~~

~~"(A) approve or disprove the agency plan; and~~

~~"(B) comment on the adequacy and effectiveness of the plan.~~

~~"(4) ISOLATION FROM INFRASTRUCTURE.—~~

~~"(A) IN GENERAL.—The Director of the National Center for Cybersecurity and Communications may, consistent with the contingency or continuity of operation plans applicable to such agency information infrastructure, order the isolation of any component of the Federal information infrastructure from any other Federal information infrastructure, if—~~

~~"(i) an agency does not implement measures in a risk-based plan approved under this subsection; and~~

~~"(ii) the failure to comply presents a significant danger to the Federal information infrastructure.~~

~~"(B) DURATION.—An isolation under subparagraph (A) shall remain in effect until—~~

~~"(i) the Director of the National Center for Cybersecurity and Communications determines that corrective measures have been implemented; or~~

~~"(ii) an updated risk-based plan is approved by the National Center for Cybersecurity and Communications and implemented by the agency.~~

‘‘(d) OPERATIONAL GUIDANCE.—The Director of the National Center for Cybersecurity and Communications shall—

‘‘(1) not later than 180 days after the date of enactment of the Protecting Cyberspace as a National Asset Act of 2010, develop operational guidance for operational evaluations as required under this section that are risk-based and cost effective; and

‘‘(2) periodically evaluate and ensure information is available on an automated and continuous basis through the system required under section 3552(a)(3)(D) to Congress on—

‘‘(A) the adequacy and effectiveness of the operational evaluations conducted under this section or section 245(b) of the Homeland Security Act of 2002; and

‘‘(B) possible executive and legislative actions for cost-effectively managing the risks to the Federal information infrastructure.

‘‘§ 3555. Federal Information Security Taskforce

‘‘(a) ESTABLISHMENT.—There is established in the executive branch a Federal Information Security Taskforce.

~~"(b) MEMBERSHIP.—The members of the Federal Information Security Taskforce shall be full-time senior Government employees and shall be as follows:~~

~~"(1) The Director of the National Center for Cybersecurity and Communications.~~

~~"(2) The Administrator of the Office of Electronic Government of the Office of Management and Budget.~~

~~"(3) The Chief Information Security Officer of each agency described under section 901(b) of title 31.~~

~~"(4) The Chief Information Security Officer of the Department of the Army, the Department of the Navy, and the Department of the Air Force.~~

~~"(5) A representative from the Office of Cyberspace Policy.~~

~~"(6) A representative from the Office of the Director of National Intelligence.~~

~~"(7) A representative from the United States Cyber Command.~~

~~"(8) A representative from the National Security Agency.~~

~~"(9) A representative from the United States Computer Emergency Readiness Team.~~

~~"(10) A representative from the Intelligence Community Incident Response Center.~~

~~"(11) A representative from the Committee on National Security Systems.~~

~~"(12) A representative from the National Institute for Standards and Technology.~~

~~"(13) A representative from the Council of Inspectors General on Integrity and Efficiency.~~

~~"(14) A representative from State and local government.~~

~~"(15) Any other officer or employee of the United States designated by the chairperson.~~

~~"(c) CHAIRPERSON AND VICE-CHAIRPERSON.—~~

~~"(1) CHAIRPERSON.—The Director of the National Center for Cybersecurity and Communications shall act as chairperson of the Federal Information Security Taskforce.~~

~~"(2) VICE-CHAIRPERSON.—The vice chairperson of the Federal Information Security Taskforce shall—~~

~~"(A) be selected by the Federal Information Security Taskforce from among its members;~~

~~"(B) serve a 1-year term and may serve multiple terms; and~~

‘‘(C) serve as a liaison to the Chief Information Officer, Council of the Inspectors General on Integrity and Efficiency, Committee on National Security Systems, and other councils or committees as appointed by the chairperson.

‘‘(d) FUNCTIONS.—The Federal Information Security Taskforce shall—

‘‘(1) be the principal interagency forum for collaboration regarding best practices and recommendations for agency information security and the security of the Federal information infrastructure;

‘‘(2) assist in the development of and annually evaluate guidance to fulfill the requirements under sections 3554 and 3556;

‘‘(3) share experiences and innovative approaches relating to threats against the Federal information infrastructure, information sharing and information security best practices, penetration testing regimes, and incident response, mitigation, and remediation;

‘‘(4) promote the development and use of standard performance indicators and measures for agency information security that—

‘‘(A) are outcome-based;

‘‘(B) focus on risk management;

“(C) align with the business and program goals of the agency;

“(D) measure improvements in the agency security posture over time; and

“(E) reduce burdensome and efficient performance indicators and measures;

“(5) recommend to the Office of Personnel Management the necessary qualifications to be established for Chief Information Security Officers to be capable of administering the functions described under this subchapter including education, training, and experience;

“(6) enhance information system processes by establishing a prioritized baseline of information security measures and controls that can be continuously monitored through automated mechanisms;

“(7) evaluate the effectiveness and efficiency of any reporting and compliance requirements that are required by law related to the information security of Federal information infrastructure; and

“(8) submit proposed enhancements developed under paragraphs (1) through (7) to the Director of the National Center for Cybersecurity and Communications.

“(c) TERMINATION.—

"(1) IN GENERAL.—Except as provided under paragraph (2), the Federal Information Security Taskforce shall terminate 4 years after the date of enactment of the Protecting Cyberspace as a National Asset Act of 2010.

"(2) EXTENSION.—The President may—

"(A) extend the Federal Information Security Taskforce by executive order; and

"(B) make more than 1 extension under this paragraph for any period as the President may determine.

"§ 3556. Independent Assessments

"(a) IN GENERAL.—

"(1) INSPECTORS GENERAL ASSESSMENTS.—Not less than every 2 years, each agency with an Inspector General appointed under the Inspector General Act of 1978 (5 U.S.C. App.) shall assess the adequacy and effectiveness of the information security program developed under section 3553(b) and (c), and evaluations conducted under section 3554.

"(2) INDEPENDENT ASSESSMENTS.—For each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the assessment.

''(b) EXISTING ASSESSMENTS.—The assessments required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

''(c) INSPECTORS GENERAL REPORTING.—Inspectors General shall ensure information obtained as a result of the assessment required under this section, or any other relevant information, is available through the system required under section 3552(a)(3)(D) to Congress and the National Center for Cybersecurity and Communications.

''§ 3557. Protection of Information

''In complying with this subchapter, agencies, evaluators, and Inspectors General shall take appropriate actions to ensure the protection of information which, if disclosed, may adversely affect information security. Protections under this chapter shall be commensurate with the risk and comply with all applicable laws and regulations.''.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TABLE OF SECTIONS.—The table of sections for chapter 35 of title 44, United States Code, is amended by striking the matter relating to subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(c)(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3551(b)''.

(B) Section 2222(j)(6) of title 10, United States Code, is amended by striking ''section 3542(b)(2))'' and inserting ''section 3551(b)''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2))'' and inserting ''section 3551(b)''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2))'' and inserting ''section 3551(b)''.

(E) Section 20(a)(2) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by striking ''section 3532(b)(2)'' and inserting ''section 3551(b)''.

(F) Section 21(b)(2) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)(2)) is amended by striking ''Institute and'' and inserting ''Institute, the Director of the National Center on Cybersecurity and Communications, and''.

(G) Section 21(b)(3) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)(3)) is amended by inserting ''the Director of the National Center on Cybersecurity and Communications,'' after ''the Director of the National Security Agency,''.

(H) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3553(b)''.

(3) HOMELAND SECURITY ACT OF 2002.—

(A) TITLE X.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by striking title X.

(B) TABLE OF CONTENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by striking the matter relating to title X.

(d) REPEAL OF OTHER STANDARDS.—

(1) IN GENERAL.—Section 11331 of title 40, United States Code, is repealed.

(2) TECHNICAL AND CONFORMING AMENDMENTS.—

(A) Section 20(c)(3) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(c)(3)) is amended by striking ''under section 11331 of title 40, United States Code''.

(B) Section 20(d)(1) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(d)(1)) is amended by striking ''the Director of the Office of Management and Budget for promulgation under section 11331 of title 40, United States Code'' and inserting ''the Secretary of Commerce for promulgation''.

(C) Section 11302(d) of title 40, United States Code, is amended by striking ''under section 11331 of this title and''.

(D) Section 1874A (e)(2)(A)(ii) of the Social Security Act (42 U.S.C. 1395kk–1(e)(2)(A)(ii)) is amended by striking ''section 11331 of title 40, United States Code'' and inserting ''section 3552 of title 44, United States Code''.

(E) Section 3504(g)(2) of title 44, United States Code, is amended by striking ''section 11331 of title 40'' and inserting ''section 3552 of title 44''.

(F) Section 3504(h)(1) of title 44, United States Code, is amended by inserting ", the Director of the National Center for Cybersecurity and Communications," after "the National Institute of Standards and Technology".

(G) Section 3504(h)(1)(B) of title 44, United States Code, is amended by striking "under section 11331 of title 40" and inserting "section 3552 of title 44".

(H) Section 3518(d) of title 44, United States Code, is amended by striking "sections 11331 and 11332" and inserting "section 11332".

(I) Section 3602(f)(8) of title 44, United States Code, is amended by striking "under section 11331 of title 40.

(J) Section 3603(f)(5) of title 44, United States Code, is amended by striking "and promulgated under section 11331 of title 40,".

TITLE IV—RECRUITMENT AND PROFESSIONAL DEVELOPMENT

SEC. 401. DEFINITIONS.

In this title:

(1) CYBERSECURITY MISSION.—The term "cybersecurity mission" means the activities of the Fed-

eral Government that encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as such activities relate to the security and stability of cyberspace.

(2) FEDERAL AGENCY'S CYBERSECURITY MISSION.—The term ''Federal agency's cybersecurity mission'' means, with respect to any Federal agency, the portion of the cybersecurity mission that is the responsibility of the Federal agency.

SEC. 402. ASSESSMENT OF CYBERSECURITY WORKFORCE.

(a) IN GENERAL.—The Director of the Office of Personnel Management and the Director shall assess the readiness and capacity of the Federal workforce to meet the needs of the cybersecurity mission of the Federal Government.

(b) STRATEGY.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Personnel Management shall develop and implement a comprehensive workforce strategy that enhances the readiness, capacity, training, and

recruitment and retention of Federal cybersecurity personnel.

(2) CONTENTS.—The strategy developed under paragraph (1) shall include—

(A) a 5-year plan on recruitment of personnel for the Federal workforce; and

(B) 10-year and 20-year projections of workforce needs.

SEC. 403. STRATEGIC CYBERSECURITY WORKFORCE PLANNING.

(a) FEDERAL AGENCY DEVELOPMENT OF STRATEGIC CYBERSECURITY WORKFORCE PLANS.—Not later than 180 days after the date of enactment of this Act and in every subsequent year, the head of each Federal agency shall develop a strategic cybersecurity workforce plan as part of the Federal agency performance plan required under section 1115 of title 31, United States Code.

(b) INTERAGENCY COORDINATION.—Each Federal agency shall develop a plan prepared under subsection (a)—

(1) on the basis of the assessment developed under section 402 and any subsequent guidance from the Director of the Office of Personnel Management and the Director; and

~~(2) in consultation with the Director and the Director of the Office of Management and Budget.~~

~~(c) CONTENTS OF THE PLAN.—~~

~~(1) IN GENERAL.—Each plan prepared under subsection (a) shall include—~~

~~(A) a description of the Federal agency's cybersecurity mission;~~

~~(B) subject to paragraph (2), a description and analysis, relating to the specialized workforce needed by the Federal agency to fulfill the Federal agency's cybersecurity mission, including—~~

~~(i) the workforce needs of the Federal agency on the date of the report, and 10-year and 20-year projections of workforce needs;~~

~~(ii) hiring projections to meet workforce needs, including, for at least a 2-year period, specific occupation and grade levels;~~

~~(iii) long-term and short-term strategic goals to address critical skills deficiencies, including analysis of the numbers of and reasons for attrition of employees;~~

(iv) recruitment strategies, including the use of student internships, part-time employment, student loan reimbursement, and telework, to attract highly qualified candidates from diverse backgrounds and geographic locations;

(v) an assessment of the sources and availability of individuals with needed expertise;

(vi) ways to streamline the hiring process;

(vii) the barriers to recruiting and hiring individuals qualified in cybersecurity and recommendations to overcome the barriers; and

(viii) a training and development plan, consistent with the curriculum developed under section 406, to enhance and improve the knowledge of employees.

(2) FEDERAL AGENCIES WITH SMALL SPECIALIZED WORKFORCE.—In accordance with guidance provided by the Director of the Office of Personnel Management, a Federal agency that needs only a small specialized workforce to fulfill the Federal agency's cybersecurity mission may present the

workforce plan components referred to in paragraph (1)(B) as part of the Federal agency performance plan required under section 1115 of title 31, United States Code.

SEC. 404. CYBERSECURITY OCCUPATION CLASSIFICATIONS.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director of the Office of Personnel Management, in coordination with the Director, shall develop and issue comprehensive occupation classifications for Federal employees engaged in cybersecurity missions.

(b) APPLICABILITY OF CLASSIFICATIONS.—The Director of the Office of Personnel Management shall ensure that the comprehensive occupation classifications issued under subsection (a) may be used throughout the Federal Government.

SEC. 405. MEASURES OF CYBERSECURITY HIRING EFFECTIVENESS.

(a) IN GENERAL.—The head of each Federal agency shall measure, and collect information on, indicators of the effectiveness of the recruitment and hiring by the Federal agency of a workforce needed to fulfill the Federal agency's cybersecurity mission.

(b) TYPES OF INFORMATION.—The indicators of effectiveness measured and subject to collection of informa-

tion under subsection (a) shall include indicators with respect to the following:

(1) RECRUITING AND HIRING.—In relation to recruiting and hiring by the Federal agency—

(A) the ability to reach and recruit well-qualified individuals from diverse talent pools;

(B) the use and impact of special hiring authorities and flexibilities to recruit the most qualified applicants, including the use of student internship and scholarship programs for permanent hires;

(C) the use and impact of special hiring authorities and flexibilities to recruit diverse candidates, including criteria such as the veteran status, race, ethnicity, gender, disability, or national origin of the candidates; and

(D) the educational level, and source of applicants.

(2) SUPERVISORS.—In relation to the supervisors of the positions being filled—

(A) satisfaction with the quality of the applicants interviewed and hired;

(B) satisfaction with the match between the skills of the individuals and the needs of the Federal agency;

(C) satisfaction of the supervisors with the hiring process and hiring outcomes;

(D) whether any mission-critical deficiencies were addressed by the individuals and the connection between the deficiencies and the performance of the Federal agency; and

(E) the satisfaction of the supervisors with the period of time elapsed to fill the positions.

(3) APPLICANTS.—The satisfaction of applicants with the hiring process, including clarity of job announcements, any reasons for withdrawal of an application, the user-friendliness of the application process, communication regarding status of applications, and the timeliness of offers of employment.

(4) HIRED INDIVIDUALS.—In relation to the individuals hired—

(A) satisfaction with the hiring process;

(B) satisfaction with the process of starting employment in the position for which the individual was hired;

(C) attrition; and

(D) the results of exit interviews.

(c) REPORTS.—

(1) IN GENERAL.—The head of each Federal agency shall submit the information collected under

this section to the Director of the Office of Personnel Management on an annual basis and in accordance with the regulations issued under subsection (d).

(2) AVAILABILITY OF RECRUITING AND HIRING INFORMATION.—

(A) IN GENERAL.—The Director of the Office of Personnel Management shall prepare an annual report containing the information received under paragraph (1) in a consistent format to allow for a comparison of hiring effectiveness and experience across demographic groups and Federal agencies.

(B) SUBMISSION.—The Director of the Office of Personnel Management shall—

(i) not later than 90 days after the receipt of all information required to be submitted under paragraph (1), make the report prepared under subparagraph (A) publicly available, including on the website of the Office of Personnel Management; and

(ii) before the date on which the report prepared under subparagraph (A) is

made publicly available, submit the report to Congress.

(d) REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Personnel Management shall issue regulations establishing the methodology, timing, and reporting of the data required to be submitted under this section.

(2) SCOPE AND DETAIL OF REQUIRED INFORMATION.—The regulations under paragraph (1) shall delimit the scope and detail of the information that a Federal agency is required to collect and submit under this section, taking account of the size and complexity of the workforce that the Federal agency needs to fulfill the Federal agency's cybersecurity mission.

SEC. 406. TRAINING AND EDUCATION.

(a) TRAINING.—

(1) FEDERAL GOVERNMENT EMPLOYEES AND FEDERAL CONTRACTORS.—The Director of the Office of Personnel Management, in conjunction with the Director of the National Center for Cybersecurity and Communications, the Director of National Intelligence, the Secretary of Defense, and the Chief

~~Information Officers Council established under section 3603 of title 44, United States Code, shall establish a cybersecurity awareness and education curriculum that shall be required for all Federal employees and contractors engaged in the design, development, or operation of agency information infrastructure, as defined under section 3551 of title 44, United States Code.~~

~~(2) CONTENTS.—The curriculum established under paragraph (1) may include—~~

~~(A) role-based security awareness training;~~

~~(B) recommended cybersecurity practices;~~

~~(C) cybersecurity recommendations for traveling abroad;~~

~~(D) unclassified counterintelligence information;~~

~~(E) information regarding industrial espionage;~~

~~(F) information regarding malicious activity online;~~

~~(G) information regarding cybersecurity and law enforcement;~~

~~(H) identity management information;~~

~~(I) information regarding supply chain security;~~

(J) information security risks associated with the activities of Federal employees; and

(K) the responsibilities of Federal employees in complying with policies and procedures designed to reduce information security risks identified under subparagraph (J).

(3) FEDERAL CYBERSECURITY PROFESSIONALS.—The Director of the Office of Personnel Management in conjunction with the Director of the National Center for Cybersecurity and Communications, the Director of National Intelligence, the Secretary of Defense, the Director of the Office of Management and Budget, and, as appropriate, colleges, universities, and nonprofit organizations with cybersecurity training expertise, shall develop a program, to provide training to improve and enhance the skills and capabilities of Federal employees engaged in the cybersecurity mission, including training specific to the acquisition workforce.

(4) HEADS OF FEDERAL AGENCIES.—Not later than 30 days after the date on which an individual is appointed to a position at level I or II of the Executive Schedule, the Director of the National Center for Cybersecurity and Communications and the Director of National Intelligence, or their designees,

shall provide that individual with a cybersecurity threat briefing.

(5) CERTIFICATION.—The head of each Federal agency shall include in the annual report required under section 3553(c) of title 44, United States Code, a certification regarding whether all officers, employees, and contractors of the Federal agency have completed the training required under this subsection.

(b) EDUCATION.—

(1) FEDERAL EMPLOYEES.—The Director of the Office of Personnel Management, in coordination with the Secretary of Education, the Director of the National Science Foundation, and the Director, shall develop and implement a strategy to provide Federal employees who work in cybersecurity missions with the opportunity to obtain additional education.

(2) K THROUGH 12.—The Secretary of Education, in coordination with the Director of the National Center for Cybersecurity and Communications and State and local governments, shall develop curriculum standards, guidelines, and recommended courses to address cyber safety, cybersecurity, and cyber ethics for students in kindergarten through grade 12.

(3) UNDERGRADUATE, GRADUATE, VOCATIONAL, AND TECHNICAL INSTITUTIONS.—

(A) SECRETARY OF EDUCATION.—The Secretary of Education, in coordination with the Director of the National Center for Cybersecurity and Communications, shall—

(i) develop curriculum standards and guidelines to address cyber safety, cybersecurity, and cyber ethics for all students enrolled in undergraduate, graduate, vocational, and technical institutions in the United States; and

(ii) analyze and develop recommended courses for students interested in pursuing careers in information technology, communications, computer science, engineering, math, and science, as those subjects relate to cybersecurity.

(B) OFFICE OF PERSONNEL MANAGEMENT.—The Director of the Office of Personnel Management, in coordination with the Director, shall develop strategies and programs—

(i) to recruit students from undergraduate, graduate, vocational, and technical institutions in the United States to

serve as Federal employees engaged in cyber missions; and

(ii) that provide internship and part-time work opportunities with the Federal Government for students at the undergraduate, graduate, vocational, and technical institutions in the United States.

(c) CYBER TALENT COMPETITIONS AND CHALLENGES.—

(1) IN GENERAL.—The Director of the National Center for Cybersecurity and Communications shall establish a program to ensure the effective operation of national and statewide competitions and challenges that seek to identify, develop, and recruit talented individuals to work in Federal agencies, State and local government agencies, and the private sector to perform duties relating to the security of the Federal information infrastructure or the national information infrastructure.

(2) GROUPS AND INDIVIDUALS.—The program under this subsection shall include—

(A) high school students;

(B) undergraduate students;

(C) graduate students;

(D) academic and research institutions;

(E) veterans; and

(F) other groups or individuals as the Director may determine.

(3) SUPPORT OF OTHER COMPETITIONS AND CHALLENGES.—The program under this subsection may support other competitions and challenges not established under this subsection through affiliation and cooperative agreements with—

(A) Federal agencies;

(B) regional, State, or community school programs supporting the development of cyber professionals; or

(C) other private sector organizations.

(4) AREAS OF TALENT.—The program under this subsection shall seek to identify, develop, and recruit exceptional talent relating to—

(A) ethical hacking;

(B) penetration testing;

(C) vulnerability Assessment;

(D) continuity of system operations;

(E) cyber forensics; and

(F) offensive and defensive cyber operations.

SEC. 407. CYBERSECURITY INCENTIVES.

(a) AWARDS.—In making cash awards under chapter 45 of title 5, United States Code, the President or the head of a Federal agency, in consultation with the Director, shall consider the success of an employee in fulfilling the objectives of the National Strategy, in a manner consistent with any policies, guidelines, procedures, instructions, or standards established by the President.

(b) OTHER INCENTIVES.—The head of each Federal agency shall adopt best practices, developed by the Director of the National Center for Cybersecurity and Communications and the Office of Management and Budget, regarding effective ways to educate and motivate employees of the Federal Government to demonstrate leadership in cybersecurity, including—

(1) promotions and other nonmonetary awards; and

(2) publicizing information sharing accomplishments by individual employees and, if appropriate, the tangible benefits that resulted.

SEC. 408. RECRUITMENT AND RETENTION PROGRAM FOR THE NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.

(a) DEFINITIONS.—In this section:

(1) CENTER.—The term ''Center'' means the National Center for Cybersecurity and Communications.

(2) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(3) DIRECTOR.—The term ''Director'' means the Director of the Center.

(4) ENTRY LEVEL POSITION.—The term ''entry level position'' means a position that—

(A) is established by the Director in the Center; and

(B) is classified at GS–7, GS–8, or GS–9 of the General Schedule.

(5) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(6) SENIOR POSITION.—The term ''senior position'' means a position that—

(A) is established by the Director in the Center; and

(B) is not established under section 5108 of title 5, United States Code, but is similar in duties and responsibilities for positions established under that section.

(b) RECRUITMENT AND RETENTION PROGRAM.—

~~(1) ESTABLISHMENT.—The Director may establish a program to assist in the recruitment and retention of highly skilled personnel to carry out the functions of the Center.~~

~~(2) CONSULTATION AND CONSIDERATIONS.—In establishing a program under this section, the Director shall—~~

~~(A) consult with the Secretary; and~~

~~(B) consider—~~

~~(i) national and local employment trends;~~

~~(ii) the availability and quality of candidates;~~

~~(iii) any specialized education or certifications required for positions;~~

~~(iv) whether there is a shortage of certain skills; and~~

~~(v) such other factors as the Director determines appropriate.~~

~~(c) HIRING AND SPECIAL PAY AUTHORITIES.—~~

~~(1) DIRECT HIRE AUTHORITY.—Without regard to the civil service laws (other than sections 3303 and 3328 of title 5, United States Code), the Director may appoint not more than 500 employees under~~

this subsection to carry out the functions of the Center.

(2) RATES OF PAY.—

(A) ENTRY LEVEL POSITIONS.—The Director may fix the pay of the employees appointed to entry level positions under this subsection without regard to chapter 51 and subchapter III of chapter 53 of title 5, United States Code, relating to classification of positions and General Schedule pay rates, except that the rate of pay for any such employee may not exceed the maximum rate of basic pay payable for a position at GS–10 of the General Schedule while that employee is in an entry level position.

(B) SENIOR POSITIONS.—

(i) IN GENERAL.—The Director may fix the pay of the employees appointed to senior positions under this subsection without regard to chapter 51 and subchapter III of chapter 53 of title 5, United States Code, relating to classification of positions and General Schedule pay rates, except that the rate of pay for any such employee may not exceed the maximum rate of basic

pay payable under section 5376 of title 5, United States Code.

(ii) HIGHER MAXIMUM RATES.—

(I) IN GENERAL.—Notwithstanding the limitation on rates of pay under clause (i)—

(aa) not more than 20 employees, identified by the Director, may be paid at a rate of pay not to exceed the maximum rate of basic pay payable for a position at level I of the Executive Schedule under section 5312 of title 5, United States Code; and

(bb) not more than 5 employees, identified by the Director with the approval of the Secretary, may be paid at a rate of pay not to exceed the maximum rate of basic pay payable for the Vice President under section 104 of title 3, United States Code.

(II) NONDELEGATION OF AUTHORITY.—The Secretary or the Di-

rector may not delegate any authority under this clause.

(d) CONVERSION TO COMPETITIVE SERVICE.—

(1) DEFINITION.—In this subsection, the term ''qualified employee'' means any individual appointed to an excepted service position in the Department who performs functions relating to the security of the Federal information infrastructure or national information infrastructure.

(2) COMPETITIVE CIVIL SERVICE STATUS.—In consultation with the Director, the Secretary may grant competitive civil service status to a qualified employee if that employee is—

(A) employed in the Center; or

(B) transferring to the Center.

(e) RETENTION BONUSES.—

(1) AUTHORITY.—Notwithstanding section 5754 of title 5, United States Code, the Director may—

(A) pay a retention bonus under that section to any individual appointed under this subsection, if the Director determines that, in the absence of a retention bonus, there is a high risk that the individual would likely leave employment with the Department; and

(B) exercise the authorities of the Office of Personnel Management and the head of an agency under that section with respect to retention bonuses paid under this subsection.

(2) LIMITATIONS ON AMOUNT OF ANNUAL BONUSES.—

(A) DEFINITIONS.—In this paragraph:

(i) MAXIMUM TOTAL PAY.—The term ''maximum total pay'' means—

(I) in the case of an employee described under subsection (c)(2)(B)(i), the total amount of pay paid in a calendar year at the maximum rate of basic pay payable for a position at level I of the Executive Schedule under section 5312 of title 5, United States Code;

(II) in the case of an employee described under subsection (c)(2)(B)(ii)(I)(aa), the total amount of pay paid in a calendar year at the maximum rate of basic pay payable for a position at level I of the Executive Schedule under section 5312 of title 5, United States Code; and

(III) in the case of an employee described under subsection (c)(2)(B)(ii)(I)(bb), the total amount of pay paid in a calendar year at the maximum rate of basic pay payable for the Vice President under section 104 of title 3, United States Code.

(ii) TOTAL COMPENSATION.—The term ''total compensation'' means—

(I) the amount of pay paid to an employee in any calendar year; and

(II) the amount of all retention bonuses paid to an employee in any calendar year.

(B) LIMITATION.—The Director may not pay a retention bonus under this subsection to an employee that would result in the total compensation of that employee exceeding maximum total pay.

(f) TERMINATION OF AUTHORITY.—The authority to make appointments and pay retention bonuses under this section shall terminate 3 years after the date of enactment of this Act.

(g) REPORTS.—

(1) PLAN FOR EXECUTION OF AUTHORITIES.—Not later than 120 days of enactment of this Act, the Director shall submit a report to the appropriate committees of Congress with a plan for the execution of the authorities provided under this section.

(2) ANNUAL REPORT.—Not later than 6 months after the date of enactment of this Act, and every year thereafter, the Director shall submit to the appropriate committees of Congress a detailed report that—

(A) discusses how the actions taken during the period of the report are fulfilling the critical hiring needs of the Center;

(B) assesses metrics relating to individuals hired under the authority of this section, including—

(i) the numbers of individuals hired;

(ii) the turnover in relevant positions;

(iii) with respect to each individual hired—

(I) the position for which hired;

(II) the salary paid;

(III) any retention bonus paid and the amount of the bonus;

(IV) the geographic location from which hired;

(V) the immediate past salary; and

(VI) whether the individual was a noncareer appointee in the Senior Executive Service or an appointee to a position of a confidential or policy-determining character under schedule C of subpart C of part 213 of title 5 of the Code of Federal Regulations before the hiring; and

(iv) whether public notice for recruitment was made, and if so—

(I) the total number of qualified applicants;

(II) the number of veteran preference eligible candidates who applied;

(III) the time from posting to job offer; and

(IV) statistics on diversity, including age, disability, race, gender, and national origin, of individuals hired under the authority of this sec-

tion to the extent such statistics are available; and

(C) includes rates of pay set in accordance with subsection (c).

TITLE V—OTHER PROVISIONS

SEC. 501. CONSULTATION ON CYBERSECURITY MATTERS.

The Chairman of the Federal Trade Commission, the Chairman of the Federal Communications Commission, and the head of any other Federal agency determined appropriate by the President shall consult with the Director of the National Center for Cybersecurity and Communications regarding any regulation, rule, or requirement to be issued or other action to be required by the Federal agency relating to the security and resiliency of the national information infrastructure.

SEC. 502. CYBERSECURITY RESEARCH AND DEVELOPMENT.

Subtitle D of title II of the Homeland Security Act of 2002 (6 U.S.C. 161 et seq.) is amended by adding at the end the following:

"SEC. 238. CYBERSECURITY RESEARCH AND DEVELOPMENT.

"(a) ESTABLISHMENT OF RESEARCH AND DEVELOPMENT PROGRAM.—The Under Secretary for Science and Technology, in coordination with the Director of the National Center for Cybersecurity and Communications, shall

carry out a research and development program for the purpose of improving the security of information infrastructure.

''(b) ELIGIBLE PROJECTS.—The research and development program carried out under subsection (a) may include projects to—

''(1) advance the development and accelerate the deployment of more secure versions of fundamental Internet protocols and architectures, including for the secure domain name addressing system and routing security;

''(2) improve and create technologies for detecting and analyzing attacks or intrusions, including analysis of malicious software;

''(3) improve and create mitigation and recovery methodologies, including techniques for containment of attacks and development of resilient networks and systems;

''(4) develop and support infrastructure and tools to support cybersecurity research and development efforts, including modeling, testbeds, and data sets for assessment of new cybersecurity technologies;

~~"(5) assist the development and support of technologies to reduce vulnerabilities in process control systems;~~

~~"(6) understand human behavioral factors that can affect cybersecurity technology and practices;~~

~~"(7) test, evaluate, and facilitate, with appropriate protections for any proprietary information concerning the technologies, the transfer of technologies associated with the engineering of less vulnerable software and securing the information technology software development lifecycle;~~

~~"(8) assist the development of identity management and attribution technologies;~~

~~"(9) assist the development of technologies designed to increase the security and resiliency of telecommunications networks;~~

~~"(10) advance the protection of privacy and civil liberties in cybersecurity technology and practices; and~~

~~"(11) address other risks identified by the Director of the National Center for Cybersecurity and Communications.~~

~~"(c) COORDINATION WITH OTHER RESEARCH INITIATIVES.—The Under Secretary—~~

"(1) shall ensure that the research and development program carried out under subsection (a) is consistent with the national strategy to increase the security and resilience of cyberspace developed by the Director of Cyberspace Policy under section 101 of the Protecting Cyberspace as a National Asset Act of 2010, or any succeeding strategy;

"(2) shall, to the extent practicable, coordinate the research and development activities of the Department with other ongoing research and development security-related initiatives, including research being conducted by—

"(A) the National Institute of Standards and Technology;

"(B) the National Academy of Sciences;

"(C) other Federal agencies, as defined under section 241;

"(D) other Federal and private research laboratories, research entities, and universities and institutions of higher education, and relevant nonprofit organizations; and

"(E) international partners of the United States;

"(3) shall carry out any research and development project under subsection (a) through a reim-

bursable agreement with an appropriate Federal agency, as defined under section 241, if the Federal agency—

"(A) is sponsoring a research and development project in a similar area; or

"(B) has a unique facility or capability that would be useful in carrying out the project;

"(4) may make grants to, or enter into cooperative agreements, contracts, other transactions, or reimbursable agreements with, the entities described in paragraph (2); and

"(5) shall submit a report to the appropriate committees of Congress on a review of the cybersecurity activities, and the capacity, of the national laboratories and other research entities available to the Department to determine if the establishment of a national laboratory dedicated to cybersecurity research and development is necessary.

"(d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES.—

"(1) CONSULTATION.—In carrying out research and development projects under subsection (a), the Under Secretary shall consult with the Privacy Officer appointed under section 222 and the Officer for

Civil Rights and Civil Liberties of the Department appointed under section 705.

''(2) PRIVACY IMPACT ASSESSMENTS.—In accordance with sections 222 and 705, the Privacy Officer shall conduct privacy impact assessments and the Officer for Civil Rights and Civil Liberties shall conduct reviews, as appropriate, for research and development projects carried out under subsection (a) that the Under Secretary determines could have an impact on privacy, civil rights, or civil liberties.

''SEC. 239. NATIONAL CYBERSECURITY ADVISORY COUNCIL.

''(a) ESTABLISHMENT.—Not later than 90 days after the date of enactment of this section, the Secretary shall establish an advisory committee under section 871 on private sector cybersecurity, to be known as the National Cybersecurity Advisory Council (in this section referred to as the 'Council').

''(b) RESPONSIBILITIES.—

''(1) IN GENERAL.—The Council shall advise the Director of the National Center for Cybersecurity and Communications on the implementation of the cybersecurity provisions affecting the private sector under this subtitle and subtitle E.

''(2) INCENTIVES AND REGULATIONS.—The Council shall advise the Director of the National

Center for Cybersecurity and Communications and appropriate committees of Congress (as defined in section 241) and any other congressional committee with jurisdiction over the particular matter regarding how market incentives and regulations may be implemented to enhance the cybersecurity and economic security of the Nation.

''(c) MEMBERSHIP.—

''(1) IN GENERAL.—The members of the Council shall be appointed the Director of the National Center for Cybersecurity and Communications and shall, to the extent practicable, represent a geographic and substantive cross-section of owners and operators of critical infrastructure and others with expertise in cybersecurity, including, as appropriate—

''(A) representatives of covered critical infrastructure (as defined under section 241);

''(B) academic institutions with expertise in cybersecurity;

''(C) Federal, State, and local government agencies with expertise in cybersecurity;

''(D) a representative of the National Security Telecommunications Advisory Council, as established by Executive Order 12382 (47 Fed.

Reg. 40531; relating to the establishment of the advisory council), as amended by Executive Order 13286 (68 Fed. Reg. 10619), as in effect on August 3, 2009, or any successor entity;

"(E) a representative of the Communications Sector Coordinating Council, or any successor entity;

"(F) a representative of the Information Technology Sector Coordinating Council, or any successor entity;

"(G) individuals, acting in their personal capacity, with demonstrated technical expertise in cybersecurity; and

"(H) such other individuals as the Director determines to be appropriate, including owners of small business concerns (as defined under section 3 of the Small Business Act (15 U.S.C. 632)).

"(2) TERM.—The members of the Council shall be appointed for 2 year terms and may be appointed to consecutive terms.

"(3) LEADERSHIP.—The Chairperson and Vice-Chairperson of the Council shall be selected by members of the Council from among the members of the Council and shall serve 2-year terms.

''(d) APPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Council.''.

SEC. 503. PRIORITIZED CRITICAL INFORMATION INFRASTRUCTURE.

Section 210E(a)(2) of the Homeland Security Act of 2002 (6 U.S.C. 124l(a)(2)) is amended—

(1) by striking ''In accordance'' and inserting the following:

''(A) IN GENERAL.—In accordance''; and

(2) by adding at the end the following:

''(B) CONSIDERATIONS.—In establishing and maintaining a list under subparagraph (A), the Secretary, in coordination with the Director of the National Center for Cybersecurity and Communications and in consultation with the National Cybersecurity Advisory Council, shall—

''(i) consider cyber vulnerabilities and consequences by sector, including—

''(I) the factors listed in section 248(a)(2);

''(II) interdependencies between components of covered critical infra-

structure (as defined under section 241); and

"(III) any other security related factor determined appropriate by the Secretary; and

"(ii) add covered critical infrastructure to or delete covered critical infrastructure from the list based on the factors listed in clause (i) for purposes of sections 248 and 249.

"(C) NOTIFICATION.—The Secretary—

"(i) shall notify the owner or operator of any system or asset added under subparagraph (B)(ii) to the list established and maintained under subparagraph (A) as soon as is practicable;

"(ii) shall develop a mechanism for an owner or operator notified under clause (i) to provide relevant information to the Secretary and the Director of the National Center for Cybersecurity and Communications relating to the inclusion of the system or asset on the list, including any information that the owner or operator be-

lieves may have led to the improper inclusion of the system or asset on the list; and

"(iii) at the sole and unreviewable discretion of the Secretary, may revise the list based on information provided in clause (ii).".

SEC. 504. NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS ACQUISITION AUTHORITIES.

(a) IN GENERAL.—The National Center for Cybersecurity and Communications is authorized to use the authorities under subsections (c)(1) and (d)(1)(B) of section 2304 of title 10, United States Code, instead of the authorities under subsections (c)(1) and (d)(1)(B) of section 303 of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 253), subject to all other requirements of section 303 of the Federal Property and Administrative Services Act of 1949.

(b) GUIDELINES.—Not later than 90 days after the date of enactment of this Act, the chief procurement officer of the Department of Homeland Security shall issue guidelines for use of the authority under subsection (a).

(c) TERMINATION.—The National Center for Cybersecurity and Communications may not use the authority

under subsection (a) on and after the date that is 3 years after the date of enactment of this Act.

(d) REPORTING.—

(1) IN GENERAL.—On a semiannual basis, the Director of the National Center for Cybersecurity and Communications shall submit a report on use of the authority granted by subsection (a) to—

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

(B) the Committee on Homeland Security of the House of Representatives.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include, at a minimum—

(A) the number of contract actions taken under the authority under subsection (a) during the period covered by the report; and

(B) for each contract action described in subparagraph (A)—

(i) the total dollar value of the contract action;

(ii) a summary of the market research conducted by the National Center for Cybersecurity and Communications, including a list of all offerors who were considered and those who actually submitted bids, in

order to determine that use of the authority was appropriate; and

(iii) a copy of the justification and approval documents required by section 303(f) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 253(f)).

(3) CLASSIFIED ANNEX.—A report submitted under this subsection shall be submitted in an unclassified form, but may include a classified annex, if necessary.

SEC. 505. TECHNICAL AND CONFORMING AMENDMENTS.

(a) ELIMINATION OF ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) in section 103(a)(8) (6 U.S.C. 113(a)(8)), by striking ", cybersecurity,";

(2) in section 514 (6 U.S.C. 321c)—

(A) by striking subsection (b); and

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

(3) in section 1801(b) (6 U.S.C. 571(b)), by striking "shall report to the Assistant Secretary for Cybersecurity and Communications" and inserting

"shall report to the Director of the National Center for Cybersecurity and Communications".

(b) CIO COUNCIL.—Section 3603(b) of title 44, United States Code, is amended—

(1) by redesignating paragraph (7) as paragraph (8); and

(2) by inserting after paragraph (6) the following:

"(7) The Director of the National Center for Cybersecurity and Communications.".

(c) REPEAL.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq) is amended—

(1) by striking section 223 (6 U.S.C. 143); and

(2) by redesignating sections 224 and 225 (6 U.S.C. 144 and 145) as sections 223 and 224, respectively.

(d) TECHNICAL CORRECTION.—Section 1802(a) of the Homeland Security Act of 2002 (6 U.S.C. 572(a)) is amended in the matter preceding paragraph (1) by striking "Department of".

(e) EXECUTIVE SCHEDULE POSITION.—Section 5313 of title 5, United States Code, is amended by adding at the end the following:

"Director of the National Center for Cybersecurity and Communications.".

(f) TABLE OF CONTENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by striking the items relating to sections 223, 224, and 225 and inserting the following:

"Sec. 223. NET guard.
"Sec. 224. Cyber Security Enhancements Act of 2002."; and

(2) by inserting after the item relating to section 237 the following:

"Sec. 238. Cybersecurity research and development.
"Sec. 239. National Cybersecurity Advisory Council.

"Subtitle E—Cybersecurity

"Sec. 241. Definitions.
"Sec. 242. National Center for Cybersecurity and Communications.
"Sec. 243. Physical and cyber infrastructure collaboration.
"Sec. 244. United States Computer Emergency Readiness Team.
"Sec. 245. Additional authorities of the Director of the National Center for Cybersecurity and Communications.
"Sec. 246. Information sharing.
"Sec. 247. Private sector assistance.
"Sec. 248. Cyber vulnerabilities to covered critical infrastructure.
"Sec. 249. National cyber emergencies..
"Sec. 250. Enforcement.
"Sec. 251. Protection of information.
"Sec. 252. Sector-specific agencies.
"Sec. 253. Strategy for Federal cybersecurity supply chain management.".

SECTION 1. SHORT TITLE.

This Act may be cited as the "Protecting Cyberspace as a National Asset Act of 2010".

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

SEC. 3. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

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

(B) the Committee on Homeland Security of the House of Representatives;

(C) the Committee on Oversight and Government Reform of the House of Representatives; and

(D) any other congressional committee with jurisdiction over the particular matter.

(2) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given that term in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).

(3) CYBERSPACE.—The term "cyberspace" means the interdependent network of information infrastructure, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

(4) DIRECTOR.—The term "Director" means the Director of Cyberspace Policy established under section 101.

(5) FEDERAL AGENCY.—The term "Federal agency"—

(A) means any executive department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Execu-

tive Office of the President), or any independent regulatory agency; and

(B) does not include the governments of the District of Columbia and of the territories and possessions of the United States and their various subdivisions.

(6) FEDERAL INFORMATION INFRASTRUCTURE.—The term "Federal information infrastructure"—

(A) means information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, any Federal agency, including information systems used or operated by another entity on behalf of a Federal agency; and

(B) does not include—

(i) a national security system; or

(ii) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community.

(7) INCIDENT.—The term "incident" has the meaning given that term in section 3551 of title 44, United States Code, as added by this Act.

(8) INFORMATION INFRASTRUCTURE.—The term "information infrastructure" means the underlying

framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including programmable electronic devices and communications networks and any associated hardware, software, or data.

(9) INFORMATION SECURITY.—The term "information security" means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, by ensuring timely and reliable access to and use of information.

(10) INFORMATION TECHNOLOGY.—The term "information technology" has the meaning given that term in section 11101 of title 40, United States Code.

(11) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given that

term under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(12) KEY RESOURCES.—The term "key resources" has the meaning given that term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)

(13) NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.—The term "National Center for Cybersecurity and Communications" means the National Center for Cybersecurity and Communications established under section 242(a) of the Homeland Security Act of 2002, as added by this Act.

(14) NATIONAL INFORMATION INFRASTRUCTURE.—The term "national information infrastructure" means information infrastructure—

(A) that is owned, operated, or controlled within or from the United States; and

(B) that is not owned, operated, controlled, or licensed for use by a Federal agency.

(15) NATIONAL SECURITY SYSTEM.—The term "national security system" has the meaning given that term in section 3551 of title 44, United States Code, as added by this Act.

(16) NATIONAL STRATEGY.—The term "National Strategy" means the national strategy to increase the

security and resiliency of cyberspace developed under section 101(a)(1).

(17) OFFICE.—The term "Office" means the Office of Cyberspace Policy established under section 101.

(18) RESILIENCY.—The term "resiliency" means the ability to eliminate or reduce the magnitude or duration of a disruptive event, including the ability to prevent, prepare for, respond to, and recover from the event.

(19) RISK.—The term "risk" means the potential for an unwanted outcome resulting from an incident, as determined by the likelihood of the occurrence of the incident and the associated consequences, including potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident.

(20) RISK-BASED SECURITY.—The term "risk-based security" has the meaning given that term in section 3551 of title 44, United States Code, as added by this Act.

TITLE I—OFFICE OF CYBERSPACE POLICY

SEC. 101. ESTABLISHMENT OF THE OFFICE OF CYBERSPACE POLICY.

(a) ESTABLISHMENT OF OFFICE.—There is established in the Executive Office of the President an Office of Cyberspace Policy which shall—

(1) develop, not later than 1 year after the date of enactment of this Act, and update as needed, but not less frequently than once every 2 years, a national strategy to increase the security and resiliency of cyberspace, that includes goals and objectives relating to—

(A) computer network operations, including offensive activities, defensive activities, and other activities;

(B) information assurance;

(C) protection of critical infrastructure and key resources;

(D) research and development priorities;

(E) law enforcement;

(F) diplomacy;

(G) homeland security;

(H) protection of privacy and civil liberties;

(I) military and intelligence activities; and

(J) identity management and authentication;

(2) oversee, coordinate, and integrate all policies and activities of the Federal Government across all instruments of national power relating to ensuring the security and resiliency of cyberspace, including—

(A) diplomatic, economic, military, intelligence, homeland security, and law enforcement policies and activities within and among Federal agencies; and

(B) offensive activities, defensive activities, and other policies and activities necessary to ensure effective capabilities to operate in cyberspace;

(3) ensure that all Federal agencies comply with appropriate guidelines, policies, and directives from the Department of Homeland Security, other Federal agencies with responsibilities relating to cyberspace security or resiliency, and the National Center for Cybersecurity and Communications; and

(4) ensure that Federal agencies have access to, receive, and appropriately disseminate law enforcement information, intelligence information, terrorism information, and any other information (including information relating to incidents provided under sub-

sections (a)(4) and (c) of section 246 of the Homeland Security Act of 2002, as added by this Act) relevant to—

(A) the security of the Federal information infrastructure or the national information infrastructure; and

(B) the security of—

(i) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community; or

(ii) a national security system.

(b) DIRECTOR OF CYBERSPACE POLICY.—

(1) IN GENERAL.—There shall be a Director of Cyberspace Policy, who shall be the head of the Office.

(2) EXECUTIVE SCHEDULE POSITION.—Section 5312 of title 5, United States Code, is amended by adding at the end the following:

"Director of Cyberspace Policy.".

SEC. 102. APPOINTMENT AND RESPONSIBILITIES OF THE DIRECTOR.

(a) APPOINTMENT.—

(1) IN GENERAL.—The Director shall be appointed by the President, by and with the advice and consent of the Senate.

(2) QUALIFICATIONS.—The President shall appoint the Director from among individuals who have demonstrated ability and knowledge in information technology, cybersecurity, and the operations, security, and resiliency of communications networks.

(3) PROHIBITION.—No person shall serve as Director while serving in any other position in the Federal Government.

(b) RESPONSIBILITIES.—The Director shall—

(1) advise the President regarding the establishment of policies, goals, objectives, and priorities for securing the information infrastructure of the Nation;

(2) advise the President and other entities within the Executive Office of the President regarding mechanisms to build, and improve the resiliency and efficiency of, the information and communication industry of the Nation, in collaboration with the private sector, while promoting national economic interests;

(3) work with Federal agencies to—

(A) oversee, coordinate, and integrate the implementation of the National Strategy, including coordination with—

(i) the Department of Homeland Security;

(ii) the Department of Defense;

(iii) the Department of Commerce;

(iv) the Department of State;

(v) the Department of Justice;

(vi) the Department of Energy;

(vii) through the Director of National Intelligence, the intelligence community; and

(viii) and any other Federal agency with responsibilities relating to the National Strategy; and

(B) resolve any disputes that arise between Federal agencies relating to the National Strategy or other matters within the responsibility of the Office;

(4) if the policies or activities of a Federal agency are not in compliance with the responsibilities of the Federal agency under the National Strategy—

(A) notify the Federal agency;

(B) transmit a copy of each notification under subparagraph (A) to the President and the appropriate congressional committees; and

(C) coordinate the efforts to bring the Federal agency into compliance;

(5) ensure the adequacy of protections for privacy and civil liberties in carrying out the responsibilities of the Director under this title, including through consultation with the Privacy and Civil Liberties Oversight Board established under section 1061 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee);

(6) upon reasonable request, appear before any duly constituted committees of the Senate or of the House of Representatives;

(7) recommend to the Office of Management and Budget or the head of a Federal agency actions (including requests to Congress relating to the reprogramming of funds) that the Director determines are necessary to ensure risk-based security of—

(A) the Federal information infrastructure;

(B) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community; or

(C) a national security system;

(8) advise the Administrator of the Office of E-Government and Information Technology and the Administrator of the Office of Information and Regulatory Affairs on the development, and oversee the implementation, of policies, principles, standards, guidelines, and budget priorities for information technology functions and activities of the Federal Government;

(9) coordinate and ensure, to the maximum extent practicable, that the standards and guidelines developed for national security systems and the standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) are complementary and unified;

(10) in consultation with the Administrator of the Office of Information and Regulatory Affairs, coordinate efforts of Federal agencies relating to the development of regulations, rules, requirements, or other actions applicable to the national information infrastructure to ensure, to the maximum extent practicable, that the efforts are complementary;

(11) coordinate the activities of the Office of Science and Technology Policy, the National Economic Council, the Office of Management and Budget, the National Security Council, the Homeland Security Council, and the United States Trade Represent-

ative related to the National Strategy and other matters within the purview of the Office;

(12) carry out the responsibilities for national security and emergency preparedness communications described in section 706 of the Communications Act of 1934 (47 U.S.C. 606) to ensure integration and coordination; and

(13) as assigned by the President, other duties relating to the security and resiliency of cyberspace.

(c) CONFORMING REGULATIONS AND ORDERS.—The President shall amend the regulations and orders issued under section 706 of the Communications Act of 1934 (47 U.S.C. 606) in accordance with subsection (b)(12).

SEC. 103. PROHIBITION ON POLITICAL CAMPAIGNING.

Section 7323(b)(2)(B) of title 5, United States Code, is amended—

(1) in clause (i), by striking "or" at the end;

(2) in clause (ii), by striking the period at the end and inserting "; or"; and

(3) by adding at the end the following:

"(iii) notwithstanding the exception under subparagraph (A) (relating to an appointment made by the President, by and with the advice and consent of the Senate), the Director of Cyberspace Policy.".

SEC. 104. REVIEW OF FEDERAL AGENCY BUDGET REQUESTS RELATING TO THE NATIONAL STRATEGY.

(a) IN GENERAL.—For each fiscal year, the head of each Federal agency shall transmit to the Director a copy of any portion of the budget of the Federal agency intended to implement the National Strategy at the same time as that budget request is submitted to the Office of Management and Budget in the preparation of the budget of the President submitted to Congress under section 1105 (a) of title 31, United States Code.

(b) TIMELY SUBMISSIONS.—The head of each Federal agency shall ensure the timely development and submission to the Director of each proposed budget under this section, in such format as may be designated by the Director with the concurrence of the Director of the Office of Management and Budget.

(c) ADEQUACY OF THE PROPOSED BUDGET REQUESTS.—With the assistance of, and in coordination with, the Office of E-Government and Information Technology and the National Center for Cybersecurity and Communications, the Director shall review each budget submission to assess the adequacy of the proposed request with regard to implementation of the National Strategy, including the overall sufficiency of the requests to implement effectively the National Strategy across all Federal agencies.

(d) INADEQUATE BUDGET REQUESTS.—If the Director concludes that a budget request submitted under subsection (a) is inadequate, in whole or in part, to implement the objectives of the National Strategy, the Director shall submit to the Director of the Office of Management and Budget and the head of the Federal agency submitting the budget request a written description of funding levels and specific initiatives that would, in the determination of the Director, make the request adequate.

SEC. 105. ACCESS TO INTELLIGENCE.

The Director shall have access to law enforcement information, intelligence information, terrorism information, and any other information (including information relating to incidents provided under subsections (a)(4) and (c) of section 246 of the Homeland Security Act of 2002, as added by this Act) that is obtained by, or in the possession of, any Federal agency that the Director determines relevant to the security of—

(1) the Federal information infrastructure;

(2) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community;

(3) a national security system; or

(4) national information infrastructure.

SEC. 106. CONSULTATION.

(a) IN GENERAL.—The Director may consult and obtain recommendations from, as needed, such Presidential and other advisory entities as the Director determines will assist in carrying out the mission of the Office, including—

(1) the National Security Telecommunications Advisory Committee;

(2) the National Infrastructure Advisory Council;

(3) the Privacy and Civil Liberties Oversight Board;

(4) the President's Intelligence Advisory Board;

(5) the Critical Infrastructure Partnership Advisory Council;

(6) the Committee on Foreign Investment in the United States;

(7) the Information Security and Privacy Advisory Board;

(8) the National Cybersecurity Advisory Council established under section 239 of the Homeland Security Act of 2002, as added by this Act; and

(9) any other entity that may provide assistance to the Director.

(b) NATIONAL STRATEGY.—In developing and updating the National Strategy the Director shall consult with

the National Cybersecurity Advisory Council and, as appropriate, State and local governments and private entities.

SEC. 107. REPORTS TO CONGRESS.

(a) IN GENERAL.—The Director shall submit an annual report to the appropriate congressional committees describing the activities, ongoing projects, and plans of the Federal Government designed to meet the goals and objectives of the National Strategy.

(b) CLASSIFIED ANNEX.—A report submitted under this section shall be submitted in an unclassified form, but may include a classified annex, if necessary.

(c) PUBLIC REPORT.—An unclassified version of each report submitted under this section shall be made available to the public.

TITLE II—NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS

SEC. 201. CYBERSECURITY.

Title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following:

"Subtitle E—Cybersecurity

"SEC. 241. DEFINITIONS.

"In this subtitle—

"(1) the term 'agency information infrastructure' means the Federal information infrastructure of a particular Federal agency;

"(2) the term 'appropriate committees of Congress' means the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives;

"(3) the term 'Center' means the National Center for Cybersecurity and Communications established under section 242(a);

"(4) the term 'covered critical infrastructure' means a system or asset identified by the Secretary as covered critical infrastructure under section 254;

"(5) the term 'cyber risk' means any risk to information infrastructure, including physical or personnel risks and security vulnerabilities, that, if exploited or not mitigated, could pose a significant risk of disruption to the operation of information infrastructure essential to the reliable operation of covered critical infrastructure;

"(6) the term 'Director' means the Director of the Center appointed under section 242(b)(1);

"(7) the term 'Federal agency'—

"(A) means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

"(B) does not include the governments of the District of Columbia and of the territories and possessions of the United States and their various subdivisions;

"(8) the term 'Federal information infrastructure'—

"(A) means information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, any Federal agency, including information systems used or operated by another entity on behalf of a Federal agency; and

"(B) does not include—

"(i) a national security system; or

"(ii) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community;

"(9) the term 'incident' has the meaning given that term in section 3551 of title 44, United States Code;

"(10) the term 'information infrastructure' means the underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including—

"(A) programmable electronic devices and communications networks; and

"(B) any associated hardware, software, or data;

"(11) the term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

"(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

"(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

"(C) availability, by ensuring timely and reliable access to and use of information;

"(12) the term 'information sharing and analysis center' means a self-governed forum whose members work together within a specific sector of critical infrastructure to identify, analyze, and share with other members and the Federal Government critical information relating to threats, vulnerabilities, or incidents to the security and resiliency of the critical infrastructure that comprises the specific sector;

"(13) the term 'information system' has the meaning given that term in section 3502 of title 44, United States Code;

"(14) the term 'intelligence community' has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4));

"(15) the term 'management controls' means safeguards or countermeasures for an information system that focus on the management of risk and the management of information system security;

"(16) the term 'National Cybersecurity Advisory Council' means the National Cybersecurity Advisory Council established under section 239;

"(17) the term 'national cyber emergency' means an actual or imminent action by any individual or entity to exploit a cyber risk in a manner that disrupts, attempts to disrupt, or poses a significant risk

of disruption to the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure;

"(18) the term 'national information infrastructure' means information infrastructure—

"(A) that is owned, operated, or controlled within or from the United States; and

"(B) that is not owned, operated, controlled, or licensed for use by a Federal agency;

"(19) the term 'national security system' has the meaning given that term in section 3551 of title 44, United States Code;

"(20) the term 'operational controls' means the safeguards and countermeasures for an information system that are primarily implemented and executed by individuals not systems;

"(21) the term 'sector-specific agency' means the relevant Federal agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category under the National Infrastructure Protection Plan, or any other appropriate Federal agency identified by the President after the date of enactment of this subtitle;

"(22) the term 'sector coordinating councils' means self-governed councils that are composed of rep-

resentatives of key stakeholders within a specific sector of critical infrastructure that serve as the principal private sector policy coordination and planning entities with the Federal Government relating to the security and resiliency of the critical infrastructure that comprise that sector;

"(23) the term 'security controls' means the management, operational, and technical controls prescribed for an information system to protect the information security of the system;

"(24) the term 'small business concern' has the meaning given that term under section 3 of the Small Business Act (15 U.S.C. 632);

"(25) the term 'technical controls' means the safeguards or countermeasures for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system;

"(26) 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);

"(27) the term 'United States person' has the meaning given that term in section 101 of the Foreign

Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and

"(28) the term 'US–CERT' means the United States Computer Emergency Readiness Team established under section 244.

"SEC. 242. NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.

"(a) ESTABLISHMENT.—

"(1) IN GENERAL.—There is established within the Department a National Center for Cybersecurity and Communications.

"(2) OPERATIONAL ENTITY.—The Center may—

"(A) enter into contracts for the procurement of property and services for the Center; and

"(B) appoint employees of the Center in accordance with the civil service laws of the United States.

"(b) DIRECTOR.—

"(1) IN GENERAL.—The Center shall be headed by a Director, who shall be appointed by the President, by and with the advice and consent of the Senate.

"(2) REPORTING TO SECRETARY.—The Director shall report directly to the Secretary and serve as the principal advisor to the Secretary on cybersecurity

and the operations, security, and resiliency of the information infrastructure and communications infrastructure of the United States.

"(3) PRESIDENTIAL ADVICE.—The Director shall regularly advise the President on the exercise of the authorities provided under this subtitle or any other provision of law relating to the security of the Federal information infrastructure or an agency information infrastructure.

"(4) QUALIFICATIONS.—The Director shall be appointed from among individuals who have—

"(A) a demonstrated ability in and knowledge of information technology, cybersecurity, and the operations, security and resiliency of communications networks; and

"(B) significant executive leadership and management experience in the public or private sector.

"(5) LIMITATION ON SERVICE.—

"(A) IN GENERAL.—Subject to subparagraph (B), the individual serving as the Director may not, while so serving, serve in any other capacity in the Federal Government, except to the extent that the individual serving as Director is doing so in an acting capacity.

"(B) EXCEPTION.—The Director may serve on any commission, board, council, or similar entity with responsibilities or duties relating to cybersecurity or the operations, security, and resiliency of the information infrastructure and communications infrastructure of the United States at the direction of the President or as otherwise provided by law.

"(c) DEPUTY DIRECTORS.—

"(1) IN GENERAL.—There shall be not less than 2 Deputy Directors for the Center, who shall report to the Director.

"(2) INFRASTRUCTURE PROTECTION.—

"(A) APPOINTMENT.—There shall be a Deputy Director appointed by the Secretary, who shall have expertise in infrastructure protection.

"(B) RESPONSIBILITIES.—The Deputy Director appointed under subparagraph (A) shall—

"(i) assist the Director and the Assistant Secretary for Infrastructure Protection in coordinating, managing, and directing the information, communications, and physical infrastructure protection responsibilities and activities of the Department,

including activities under Homeland Security Presidential Directive–7, or any successor thereto, and the National Infrastructure Protection Plan, or any successor thereto;

"(ii) review the budget for the Center and the Office of Infrastructure Protection before submission of the budget to the Secretary to ensure that activities are appropriately coordinated;

"(iii) develop, update periodically, and submit to the appropriate committees of Congress a strategic plan detailing how critical infrastructure protection activities will be coordinated between the Center, the Office of Infrastructure Protection, and the private sector;

"(iv) subject to the direction of the Director resolve conflicts between the Center and the Office of Infrastructure Protection relating to the information, communications, and physical infrastructure protection responsibilities of the Center and the Office of Infrastructure Protection; and

"(v) perform such other duties as the Director may assign.

"(C) ANNUAL EVALUATION.—The Assistant Secretary for Infrastructure Protection shall submit annually to the Director an evaluation of the performance of the Deputy Director appointed under subparagraph (A).

"(3) INTELLIGENCE COMMUNITY.—The Director of National Intelligence shall identify an employee of an element of the intelligence community to serve as a Deputy Director of the Center. The employee shall be detailed to the Center on a reimbursable basis for such period as is agreed to by the Director and the Director of National Intelligence, and, while serving as Deputy Director, shall report directly to the Director of the Center.

"(d) LIAISON OFFICERS.—

"(1) IN GENERAL.—The Secretary of Defense, the Attorney General, the Secretary of Commerce, and the Director of National Intelligence shall detail personnel to the Center to act as full-time liaisons with the Department of Defense, the Department of Justice, the National Institute of Standards and Technology, and elements of the intelligence community to assist in coordination between and among the Center, the

Department of Defense, the Department of Justice, the National Institute of Standards and Technology, and elements of the intelligence community.

"(2) PRIVATE SECTOR.—

"(A) IN GENERAL.—Consistent with applicable law and ethics requirements, and except as provided in subparagraph (B), the Director may authorize representatives from private sector entities to participate in the activities of the Center to improve the information sharing, analysis, and coordination of activities of the US–CERT.

"(B) LIMITATION.—A representative from a private sector entity authorized to participate in the activities of the Center under subparagraph (A) may not participate in any activities of the Center under section 248, 249, or 250.

"(e) PRIVACY OFFICER.—

"(1) IN GENERAL.—The Director, in consultation with the Secretary, shall designate a full-time privacy officer, who shall report to the Director.

"(2) DUTIES.—The privacy officer designated under paragraph (1) shall have primary responsibility for implementation by the Center of the privacy policy for the Department established by the Privacy Officer appointed under section 222.

"(f) DUTIES OF DIRECTOR.—

"(1) IN GENERAL.—The Director shall—

"(A) working cooperatively with the private sector, lead the Federal effort to secure, protect, and ensure the resiliency of the Federal information infrastructure, national information infrastructure, and communications infrastructure of the United States, including communications networks;

"(B) assist in the identification, remediation, and mitigation of vulnerabilities to the Federal information infrastructure and the national information infrastructure;

"(C) provide dynamic, comprehensive, and continuous situational awareness of the security status of the Federal information infrastructure, national information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, and information infrastructure located outside the United States the disruption of which could result in national or regional catastrophic damage in the United States by sharing and inte-

grating classified and unclassified information, including information relating to threats, vulnerabilities, traffic, trends, incidents, and other anomalous activities affecting the infrastructure or systems, on a routine and continuous basis with—

"(i) the National Threat Operations Center of the National Security Agency;

"(ii) the United States Cyber Command, including the Joint Task Force-Global Network Operations;

"(iii) the Cyber Crime Center of the Department of Defense;

"(iv) the National Cyber Investigative Joint Task Force;

"(v) the Intelligence Community Incident Response Center;

"(vi) any other Federal agency, or component thereof, identified by the Director; and

"(vii) any non-Federal entity, including, where appropriate, information sharing and analysis centers, identified by the Director, with the concurrence of the owner

or operator of that entity and consistent with applicable law;

"(D) work with the entities described in subparagraph (C) to establish policies and procedures that enable information sharing between and among the entities;

"(E)(i) develop, in coordination with the Assistant Secretary for Infrastructure Protection, other Federal agencies, the private sector, and State and local governments, a national incident response plan that details the roles of Federal agencies, State and local governments, and the private sector, including plans to be executed in response to a declaration of a national cyber emergency by the President under section 249; and

"(ii) establish mechanisms for assisting owners or operators of critical infrastructure, including covered critical infrastructure, in the deployment of emergency measures or other actions, including measures to restore the critical infrastructure in the event of the destruction or a serious disruption of the critical infrastructure;

"(F) conduct risk-based assessments of the Federal information infrastructure with respect to acts of terrorism, natural disasters, and other large-scale disruptions and provide the results of the assessments to the Director of Cyberspace Policy and to affected Federal agencies;

"(G) develop, oversee the implementation of, and enforce policies, principles, and guidelines on information security for the Federal information infrastructure, including timely adoption of and compliance with standards developed by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3);

"(H) provide assistance to the National Institute of Standards and Technology in developing standards under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3);

"(I) provide to Federal agencies mandatory security controls to mitigate and remediate vulnerabilities of and incidents affecting the Federal information infrastructure;

"(J) subject to paragraph (2), and as needed, assist the Director of the Office of Management and Budget and the Director of Cyberspace Policy in conducting analysis and prioritization of budgets, resources, and policies relating to the security of the Federal information infrastructure;

"(K) in accordance with section 253, develop, periodically update, and implement a supply chain risk management strategy to enhance, in a risk-based and cost-effective manner, the security of the communications and information technology products and services purchased by the Federal Government;

"(L) notify the Director of Cyberspace Policy of any incident involving the Federal information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, or the national information infrastructure that could compromise or significantly affect economic or national security;

"(M) consult, in coordination with the Director of Cyberspace Policy, with appropriate international partners to enhance the security of the Federal information infrastructure, national information infrastructure, and information infrastructure located outside the United States the disruption of which could result in national or regional catastrophic damage in the United States;

"(N)(i) coordinate and integrate information to analyze the composite security state of the Federal information infrastructure and information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community;

*"(ii) ensure the information required under clause (i) and section 3553(c)(1)(A) of title 44, United States Code, including the views of the Director on the adequacy and effectiveness of information security throughout the Federal information infrastructure and information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or an-

other element of the intelligence community, is available on an automated and continuous basis through the system maintained under section 3552(a)(3)(D) of title 44, United States Code;

"(iii) in conjunction with the quadrennial homeland security review required under section 707, and at such other times determined appropriate by the Director, analyze the composite security state of the national information infrastructure and submit to the President, Congress, and the Secretary a report regarding actions necessary to enhance the composite security state of the national information infrastructure based on the analysis; and

"(iv) foster collaboration and serve as the primary contact between the Federal Government, State and local governments, and private entities on matters relating to the security of the Federal information infrastructure and the national information infrastructure;

"(O) oversee the development, implementation, and management of security requirements for Federal agencies relating to the external access points to or from the Federal information infrastructure;

"(P) establish, develop, and oversee the capabilities and operations within the US–CERT as required by section 244;

"(Q) oversee the operations of the National Communications System, as described in Executive Order 12472 (49 Fed. Reg. 13471; relating to the assignment of national security and emergency preparedness telecommunications functions), as amended by Executive Order 13286 (68 Fed. Reg. 10619) and Executive Order 13407 (71 Fed. Reg. 36975), or any successor thereto, including planning for and providing communications for the Federal Government under all circumstances, including crises, emergencies, attacks, recoveries, and reconstitutions;

"(R) ensure, in coordination with the privacy officer designated under subsection (e), the Privacy Officer appointed under section 222, and the Director of the Office of Civil Rights and Civil Liberties appointed under section 705, that the activities of the Center comply with all policies, regulations, and laws protecting the privacy and civil liberties of United States persons;

"(S) subject to the availability of resources, in accordance with applicable law relating to the

protection of trade secrets, and at the discretion of the Director, provide voluntary technical assistance—

"(i) at the request of an owner or operator of covered critical infrastructure, to assist the owner or operator in complying with sections 248 and 249, including implementing required security or emergency measures and developing response plans for national cyber emergencies declared under section 249; and

"(ii) at the request of the owner or operator of national information infrastructure that is not covered critical infrastructure, and based on risk, to assist the owner or operator in implementing best practices, and related standards and guidelines, recommended under section 247 and other measures necessary to mitigate or remediate vulnerabilities of the information infrastructure and the consequences of efforts to exploit the vulnerabilities;

"(T)(i) conduct, in consultation with the National Cybersecurity Advisory Council, the head of appropriate sector-specific agencies, and

any private sector entity determined appropriate by the Director, risk-based assessments of national information infrastructure and information infrastructure located outside the United States the disruption of which could result in national or regional catastrophic damage in the United States, on a sector-by-sector basis, with respect to acts of terrorism, natural disasters, and other large-scale disruptions or financial harm, which shall identify and prioritize risks to the national information infrastructure and information infrastructure located outside the United States the disruption of which could result in national or regional catastrophic damage in the United States, including vulnerabilities and associated consequences; and

"(ii) coordinate and evaluate the mitigation or remediation of vulnerabilities and consequences identified under clause (i);

"(U) regularly evaluate and assess technologies designed to enhance the protection of the Federal information infrastructure and national information infrastructure, including an assessment of the cost-effectiveness of the technologies;

"(V) promote the use of the best practices recommended under section 247 to State and local governments and the private sector;

"(W) develop and implement outreach and awareness programs on cybersecurity, including—

"(i) a public education campaign to increase the awareness of cybersecurity, cyber safety, and cyber ethics, which shall include use of the Internet, social media, entertainment, and other media to reach the public;

"(ii) an education campaign to increase the understanding of State and local governments and private sector entities of the costs of failing to ensure effective security of information infrastructure and cost-effective methods to mitigate and remediate vulnerabilities; and

"(iii) outcome-based performance measures to determine the success of the programs;

"(X) develop and implement a national cybersecurity exercise program that includes—

"(i) the participation of State and local governments, international partners of the United States, and the private sector;

"(ii) an after action report analyzing lessons learned from exercises and identifying vulnerabilities to be remediated or mitigated; and

"(iii) oversight, in coordination with the Director of the Office of Cyberspace Policy, of the efforts by Federal agencies to address deficiencies identified in the after action reports required under clause (ii);

"(Y) coordinate with the Assistant Secretary for Infrastructure Protection to ensure that—

"(i) cybersecurity is appropriately addressed in carrying out the infrastructure protection responsibilities described in section 201(d); and

"(ii) the operations of the Center and the Office of Infrastructure Protection avoid duplication and use, to the maximum extent practicable, joint mechanisms for information sharing and coordination with the private sector;

"(Z) oversee the activities of the Office of Emergency Communications established under section 1801;

"(AA) in coordination with the Director of the Office of Cyberspace Policy and the heads of relevant Federal agencies, develop and implement an identity management strategy for cyberspace, which shall include, at a minimum, research and development goals, an analysis of appropriate protections for privacy and civil liberties, and mechanisms to develop and disseminate best practices and standards relating to identity management, including usability and transparency; and

"(BB) perform such other duties as the Secretary may direct relating to the security and resiliency of the information and communications infrastructure of the United States.

"(2) BUDGET ANALYSIS.—In conducting analysis and prioritization of budgets under paragraph (1)(J), the Director—

"(A) in coordination with the Director of the Office of Management and Budget, may access information from any Federal agency regarding the finances, budget, and programs of

the Federal agency relevant to the security of the Federal information infrastructure;

"(B) may make recommendations to the Director of the Office of Management and Budget and the Director of Cyberspace Policy regarding the budget for each Federal agency to ensure that adequate funding is devoted to securing the Federal information infrastructure, in accordance with policies, principles, and guidelines established by the Director under this subtitle; and

"(C) shall provide copies of any recommendations made under subparagraph (B) to—

"(i) the Committee on Appropriations of the Senate;

"(ii) the Committee on Appropriations of the House of Representatives; and

"(iii) the appropriate committees of Congress.

"(g) USE OF MECHANISMS FOR COLLABORATION.—In carrying out the responsibilities and authorities of the Director under this subtitle, to the maximum extent practicable, the Director shall use mechanisms for collaboration and information sharing (including mechanisms relating to the identification and communication of threats,

vulnerabilities, and associated consequences) established by other components of the Department or other Federal agencies to avoid unnecessary duplication or waste.

"(h) SUFFICIENCY OF RESOURCES PLAN.—

"(1) REPORT.—Not later than 120 days after the date of enactment of this subtitle, the Director of the Office of Management and Budget shall submit to the appropriate committees of Congress and the Comptroller General of the United States a report on the resources and staff necessary to carry out fully the responsibilities under this subtitle.

"(2) COMPTROLLER GENERAL REVIEW.—

"(A) IN GENERAL.—The Comptroller General of the United States shall evaluate the reasonableness and adequacy of the report submitted by the Director under paragraph (1).

"(B) REPORT.—Not later than 60 days after the date on which the report is submitted under paragraph (1), the Comptroller General shall submit to the appropriate committees of Congress a report containing the findings of the review under subparagraph (A).

"(i) FUNCTIONS TRANSFERRED.—There are transferred to the Center the National Cyber Security Division, the Office of Emergency Communications, and the National

Communications System, including all the functions, personnel, assets, authorities, and liabilities of the National Cyber Security Division, the Office of Emergency Communications, and the National Communications System.

"(j) ASSISTANT TO THE DIRECTOR FOR STATE, LOCAL, AND PRIVATE SECTOR OUTREACH.—The Director shall identify a senior official in the Center who—

"(1) shall report directly to the Director; and

"(2) in coordination with the Special Assistant to the Secretary appointed under section 102(f), shall—

"(A) advise the Director on policies and regulations, rules, requirements or other actions affecting the private sector, including the economic impact;

"(B) work with individual businesses and other nongovernmental organizations to foster dialogue with the Center;

"(C) foster partnerships and facilitate communication between the Center and State and local governments and private sector entities;

"(D) coordinate and maintain communication and interaction with State and local governments and private sector entities on matters relating to the security of the Federal informa-

tion infrastructure and the national information infrastructure;

"(E) assist the Director in sharing best practices, guidelines, and other important information relating to the policies, goals, and activities of the Center;

"(F) assist the Director in developing and implementing the national cybersecurity exercise program under subsection (f)(1)(X) as it relates to State and local governments and private sector entities;

"(G) assist the Director in developing the national incident response plan under subsection (f)(1)(E) as it relates to State and local governments and private sector entities;

"(H) assist the Director in information sharing activities of the Center as it relates to State and local governments and private sector entities; and

"(I) perform any other duties, as directed by the Director.

"SEC. 243. PHYSICAL AND CYBER INFRASTRUCTURE COLLABORATION.

"(a) IN GENERAL.—The Director and the Assistant Secretary for Infrastructure Protection shall coordinate the

information, communications, and physical infrastructure protection responsibilities and activities of the Center and the Office of Infrastructure Protection.

"(b) OVERSIGHT.—The Secretary shall ensure that the coordination described in subsection (a) occurs.

"SEC. 244. UNITED STATES COMPUTER EMERGENCY READINESS TEAM.

"(a) ESTABLISHMENT OF OFFICE.—There is established within the Center, the United States Computer Emergency Readiness Team, which shall be headed by a Director, who shall be selected from the Senior Executive Service by the Secretary.

"(b) RESPONSIBILITIES.—The US–CERT shall—

"(1) collect, coordinate, and disseminate information on—

"(A) risks to the Federal information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, or the national information infrastructure; and

"(B) security controls to enhance the security of the Federal information infrastructure or

the national information infrastructure against the risks identified in subparagraph (A); and

"(2) establish a mechanism for engagement with the private sector.

"(c) MONITORING, ANALYSIS, WARNING, AND RESPONSE.—

"(1) DUTIES.—Subject to paragraph (2), the US–CERT shall—

"(A) provide analysis and reports to Federal agencies on the security of the Federal information infrastructure;

"(B) provide continuous, automated monitoring of the Federal information infrastructure at external Internet access points, which shall include detection and warning of threats, vulnerabilities, traffic, trends, incidents, and other anomalous activities affecting the information security of the Federal information infrastructure;

"(C) warn Federal agencies of threats, vulnerabilities, incidents, and anomalous activities that could affect the Federal information infrastructure;

"(D) develop, recommend, and deploy security controls to mitigate or remediate vulnerabilities;

"(E) support Federal agencies in conducting risk assessments of the agency information infrastructure;

"(F) disseminate to Federal agencies risk analyses of incidents that could impair the risk-based security of the Federal information infrastructure;

"(G) develop and acquire predictive analytic tools to evaluate threats, vulnerabilities, traffic, trends, incidents, and anomalous activities;

"(H) aid in the detection of, and warn owners or operators of national information infrastructure regarding, threats, vulnerabilities, and incidents, affecting the national information infrastructure, including providing—

"(i) timely, targeted, and actionable notifications of threats, vulnerabilities, and incidents;

"(ii) notifications under this subparagraph; and

"(iii) recommended security controls to mitigate or remediate vulnerabilities; and

"(I) respond to assistance requests from Federal agencies and, subject to the availability of resources, owners or operators of the national information infrastructure to—

"(i) isolate, mitigate, or remediate incidents;

"(ii) recover from damages and mitigate or remediate vulnerabilities; and

"(iii) evaluate security controls and other actions taken to secure information infrastructure and incorporate lessons learned into best practices, policies, principles, and guidelines.

"(2) REQUIREMENT.—With respect to the Federal information infrastructure, the US–CERT shall conduct the activities described in paragraph (1) in a manner consistent with the responsibilities of the head of a Federal agency described in section 3553 of title 44, United States Code.

"(3) REPORT.—Not later than 1 year after the date of enactment of this subtitle, and every year thereafter, the Secretary shall—

"(A) in conjunction with the Inspector General of the Department, conduct an independent audit or review of the activities of the US–CERT under paragraph (1)(B)), which shall include, at a minimum, an assessment of whether and to what extent the activities authorized under paragraph (1)(B) have monitored communications other than communications to or from a Federal agency; and

"(B) submit to the appropriate committees of Congress and the President a report regarding the audit or review under subparagraph (A).

"(4) CLASSIFIED ANNEX.—A report submitted under paragraph (3) shall be submitted in an unclassified form, but may include a classified annex, if necessary.

"(d) PROCEDURES FOR FEDERAL GOVERNMENT.—Not later than 90 days after the date of enactment of this subtitle, the head of each Federal agency shall establish procedures for the Federal agency that ensure that the US–CERT can perform the functions described in subsection (c) in relation to the Federal agency.

"(e) OPERATIONAL UPDATES.—The US–CERT shall provide unclassified and, as appropriate, classified updates regarding the composite security state of the Federal infor-

mation infrastructure to the Federal Information Security Taskforce.

"(f) FEDERAL POINTS OF CONTACT.—The Director of the US–CERT shall designate a principal point of contact within the US–CERT for each Federal agency to—

"(1) maintain communication;

"(2) ensure cooperative engagement and information sharing; and

"(3) respond to inquiries or requests.

"(g) REQUESTS FOR INFORMATION OR PHYSICAL ACCESS.—

"(1) INFORMATION ACCESS.—Upon request of the Director of the US–CERT, the head of a Federal agency or an Inspector General for a Federal agency shall provide any law enforcement information, intelligence information, terrorism information, or any other information (including information relating to incidents provided under subsections (a)(4) and (c) of section 246) relevant to the security of the Federal information infrastructure or the national information infrastructure necessary to carry out the duties, responsibilities, and authorities under this subtitle.

"(2) PHYSICAL ACCESS.—Upon request of the Director, and in consultation with the head of a Federal agency, the Federal agency shall provide physical

access to any facility of the Federal agency necessary to determine whether the Federal agency is in compliance with any policies, principles, and guidelines established by the Director under this subtitle, or otherwise necessary to carry out the duties, responsibilities, and authorities of the Director applicable to the Federal information infrastructure.

"SEC. 245. ADDITIONAL AUTHORITIES OF THE DIRECTOR OF THE NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.

"(a) ACCESS TO INFORMATION.—Unless otherwise directed by the President—

"(1) the Director shall access, receive, and analyze law enforcement information, intelligence information, terrorism information, and any other information (including information relating to incidents provided under subsections (a)(4) and (c) of section 246) relevant to the security of the Federal information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, or national information infrastructure from Federal agencies and, consistent with applicable law, State and local governments (including law en-

forcement agencies), and private entities, including information provided by any contractor to a Federal agency regarding the security of the agency information infrastructure;

"(2) any Federal agency in possession of law enforcement information, intelligence information, terrorism information, or any other information (including information relating to incidents provided under subsections (a)(4) and (c) of section 246) relevant to the security of the Federal information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, or national information infrastructure shall provide that information to the Director in a timely manner; and

"(3) the Director, in coordination with the Director of the Office of Management and Budget, the Attorney General, the Privacy and Civil Liberties Oversight Board established under section 1061 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee), the Director of National Intelligence, and the Archivist of the United States, shall establish

guidelines to ensure that information is transferred, stored, and preserved—

"(A) in accordance with applicable laws relating to the protection of trade secrets and other applicable laws; and

"(B) in a manner that protects the privacy and civil liberties of United States persons and intelligence sources and methods.

"(b) OPERATIONAL EVALUATIONS.—

"(1) IN GENERAL.—The Director—

"(A) subject to paragraph (2), shall develop, maintain, and enhance capabilities to evaluate the security of the Federal information infrastructure as described in section 3554(a)(3) of title 44, United States Code, including the ability to conduct risk-based penetration testing and vulnerability assessments;

"(B) in carrying out subparagraph (A), may request technical assistance from the Director of the Federal Bureau of Investigation, the Director of the National Security Agency, the head of any other Federal agency that may provide support, and any nongovernmental entity contracting with the Department or another Federal agency; and

"(C) in consultation with the Attorney General and the Privacy and Civil Liberties Oversight Board established under section 1061 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee), shall develop guidelines to ensure compliance with all applicable laws relating to the privacy of United States persons in carrying out the operational evaluations under subparagraph (A).

"(2) OPERATIONAL EVALUATIONS.—

"(A) IN GENERAL.—The Director may conduct risk-based operational evaluations of the agency information infrastructure of any Federal agency, at a time determined by the Director, in consultation with the head of the Federal agency, using the capabilities developed under paragraph (1)(A).

"(B) ANNUAL EVALUATION REQUIREMENT.—If the Director conducts an operational evaluation under subparagraph (A) or an operational evaluation at the request of a Federal agency to meet the requirements of section 3554 of title 44, United States Code, the operational evaluation shall satisfy the requirements of section 3554 for the Federal agency for the year of

the evaluation, unless otherwise specified by the Director.

"(c) CORRECTIVE MEASURES AND MITIGATION PLANS.—If the Director determines that a Federal agency is not in compliance with applicable policies, principles, standards, and guidelines applicable to the Federal information infrastructure—

"(1) the Director, in consultation with the Director of the Office of Management and Budget, may direct the head of the Federal agency to—

"(A) take corrective measures to meet the policies, principles, standards, and guidelines; and

"(B) develop a plan to remediate or mitigate any vulnerabilities addressed by the policies, principles, standards, and guidelines;

"(2) within such time period as the Director shall prescribe, the head of the Federal agency shall—

"(A) implement a corrective measure or develop a mitigation plan in accordance with paragraph (1); or

"(B) submit to the Director, the Director of the Office of Management and Budget, the Inspector General for the Federal agency, and the appropriate committees of Congress a report in-

dicating why the Federal agency has not implemented the corrective measure or developed a mitigation plan; and

"(3) after providing notice to the head of the affected Federal agency, the Director may direct the isolation of any component of the agency information infrastructure, consistent with the contingency or continuity of operation plans applicable to the agency information infrastructure, until corrective measures are taken or mitigation plans approved by the Director are put in place, if—

"(A) the head of the Federal agency has failed to comply with the corrective measures prescribed under paragraph (1); and

"(B) the failure to comply presents a significant danger to the Federal information infrastructure.

"SEC. 246. INFORMATION SHARING.

"(a) FEDERAL AGENCIES.—

"(1) INFORMATION SHARING PROGRAM.—Consistent with the responsibilities described in section 242 and 244, the Director, in consultation with the other members of the Chief Information Officers Council established under section 3603 of title 44, United States Code, and the Federal Information Se-

curity Taskforce, shall establish a program for sharing information with and between the Center and other Federal agencies that includes processes and procedures, including standard operating procedures—

"(A) under which the Director regularly shares with each Federal agency—

"(i) analysis and reports on the composite security state of the Federal information infrastructure and information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, which shall include information relating to threats, vulnerabilities, incidents, or anomalous activities;

"(ii) any available analysis and reports regarding the security of the agency information infrastructure; and

"(iii) means and methods of preventing, responding to, mitigating, and remediating vulnerabilities; and

"(B) under which the Director may request information from Federal agencies concerning the security of the Federal information infrastructure, information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community, or the national information infrastructure necessary to carry out the duties of the Director under this subtitle or any other provision of law.

"(2) CONTENTS.—The program established under this section shall include—

"(A) timeframes for the sharing of information under paragraph (1);

"(B) guidance on what information shall be shared, including information regarding incidents;

"(C) a tiered structure that provides guidance for the sharing of urgent information; and

"(D) processes and procedures under which the Director or the head of a Federal agency may report noncompliance with the program to the Director of Cyberspace Policy.

"(3) US–CERT.—The Director of the US–CERT shall ensure that the head of each Federal agency has continual access to data collected by the US–CERT regarding the agency information infrastructure of the Federal agency.

"(4) FEDERAL AGENCIES.—

"(A) IN GENERAL.—The head of a Federal agency shall comply with all processes and procedures established under this subsection regarding notification to the Director relating to incidents.

"(B) IMMEDIATE NOTIFICATION REQUIRED.—Unless otherwise directed by the President, any Federal agency with a national security system shall immediately notify the Director regarding any incident affecting the risk-based security of the national security system.

"(b) STATE AND LOCAL GOVERNMENTS, PRIVATE SECTOR, AND INTERNATIONAL PARTNERS.—

"(1) IN GENERAL.—The Director shall establish processes and procedures, including standard operating procedures, to ensure bidirectional information sharing with State and local governments, private entities, and international partners of the United States on—

"(A) threats, vulnerabilities, incidents, and anomalous activities affecting the national information infrastructure; and

"(B) means and methods of preventing, responding to, and mitigating and remediating vulnerabilities.

"(2) CONTENTS.—The processes and procedures established under paragraph (1) shall include—

"(A) means or methods of accessing classified or unclassified information, as appropriate and in accordance with applicable laws regarding trade secrets, that will provide situational awareness of the security of the Federal information infrastructure and the national information infrastructure relating to threats, vulnerabilities, traffic, trends, incidents, and other anomalous activities affecting the Federal information infrastructure or the national information infrastructure;

"(B) a mechanism, established in consultation with the heads of the relevant sector-specific agencies, sector coordinating councils, and information sharing and analysis centers, by which owners and operators of covered critical infrastructure shall report incidents in the informa-

tion infrastructure for covered critical infrastructure under subsection (c)(1)(A);

"(C) guidance on the form, content, and priority of incident reports that shall be submitted under subsection (c)(1)(A), which shall—

"(i) include appropriate mechanisms to protect—

"(I) information in accordance with section 251;

"(II) personally identifiable information; and

"(III) trade secrets; and

"(ii) prioritize the reporting of incidents based on the risk the incident poses to the disruption of the reliable operation of the covered critical infrastructure;

"(D) a procedure for notifying an information technology provider if a vulnerability is detected in the product or service produced by the information technology provider and, where possible, working with the information technology provider to remediate the vulnerability before any public disclosure of the vulnerability so as to minimize the opportunity for the vulnerability to be exploited; and

"(E) an evaluation of the need to provide security clearances to employees of State and local governments, private entities, and international partners to carry out this subsection.

"(3) GUIDELINES.—The Director, in consultation with the Attorney General, the Director of National Intelligence, and the Privacy Officer established under section 242(e), shall develop guidelines to protect the privacy and civil liberties of United States persons and intelligence sources and methods, while carrying out this subsection.

"(c) INCIDENTS.—

"(1) NON-FEDERAL ENTITIES.—

"(A) IN GENERAL.—

"(i) MANDATORY REPORTING.—Subject to clause (ii), the owner or operator of covered critical infrastructure shall report any incident affecting the information infrastructure of covered critical infrastructure to the extent the incident might indicate an actual or potential cyber risk, or exploitation of a cyber risk, in accordance with the policies and procedures for the mechanism established under subsection (b)(2)(B)

and guidelines developed under subsection (b)(3).

"(ii) LIMITATION.—Clause (i) shall not authorize the Director, the Center, the Department, or any other Federal entity to—

"(I) compel the disclosure of information relating to an incident unless otherwise authorized by law; or

"(II) intercept a wire, oral, or electronic communication (as those terms are defined in section 2510 of title 18, United States Code), access a stored electronic or wire communication, install or use a pen register or trap and trace device, or conduct electronic surveillance (as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.1801)) relating to an incident unless otherwise authorized under chapter 119, chapter 121, or chapter 206 of title 18, United States Code, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(B) REPORTING PROCEDURES.—The Director shall establish procedures that enable and encourage the owner or operator of national information infrastructure to report to the Director regarding incidents affecting such information infrastructure.

"(2) INFORMATION PROTECTION.—Notwithstanding any other provision of law, information reported under paragraph (1) shall be protected from unauthorized disclosure, in accordance with section 251.

"(d) ADDITIONAL RESPONSIBILITIES.—The Director shall—

"(1) share data collected on the Federal information infrastructure with the National Science Foundation and other accredited research institutions for the sole purpose of cybersecurity research in a manner that protects privacy and civil liberties of United States persons and intelligence sources and methods;

"(2) establish a website to provide an opportunity for the public to provide—

"(A) input about the operations of the Center; and

"(B) recommendations for improvements of the Center; and

"(3) in coordination with the Secretary of Defense, the Director of National Intelligence, the Secretary of State, and the Attorney General, develop information sharing pilot programs with international partners of the United States.

"SEC. 247. PRIVATE SECTOR ASSISTANCE.

"(a) IN GENERAL.—The Director, in consultation with the Director of the National Institute of Standards and Technology, the Director of the National Security Agency, the head of any relevant sector-specific agency, the National Cybersecurity Advisory Council, State and local governments, and any private entities the Director determines appropriate, shall establish a program to promote, and provide technical assistance authorized under section 242(f)(1)(S) relating to the implementation of, best practices and related standards and guidelines for securing the national information infrastructure, including the costs and benefits associated with the implementation of the best practices and related standards and guidelines.

"(b) ANALYSIS AND IMPROVEMENT OF STANDARDS AND GUIDELINES.—For purposes of the program established under subsection (a), the Director shall—

"(1) regularly assess and evaluate cybersecurity standards and guidelines issued by private sector organizations, recognized international and domestic

standards setting organizations, and Federal agencies; and

"(2) in coordination with the National Institute of Standards and Technology, encourage the development of, and recommend changes to, the standards and guidelines described in paragraph (1) for securing the national information infrastructure.

"(c) GUIDANCE AND TECHNICAL ASSISTANCE.—

"(1) IN GENERAL.—The Director shall promote best practices and related standards and guidelines to assist owners and operators of national information infrastructure in increasing the security of the national information infrastructure and protecting against and mitigating or remediating known vulnerabilities.

"(2) REQUIREMENT.—Technical assistance provided under section 242(f)(1)(S) and best practices promoted under this section shall be prioritized based on risk.

"(d) CRITERIA.—In promoting best practices or recommending changes to standards and guidelines under this section, the Director shall ensure that best practices, and related standards and guidelines—

"(1) address cybersecurity in a comprehensive, risk-based manner;

"(2) include consideration of the cost of implementing such best practices or of implementing recommended changes to standards and guidelines;

"(3) increase the ability of the owners or operators of national information infrastructure to protect against and mitigate or remediate known vulnerabilities;

"(4) are suitable, as appropriate, for implementation by small business concerns;

"(5) as necessary and appropriate, are sector specific;

"(6) to the maximum extent possible, incorporate standards and guidelines established by private sector organizations, recognized international and domestic standards setting organizations, and Federal agencies;

"(7) consider voluntary programs by internet service providers to assist individuals using the internet service providers in the identification and mitigation of cyber threats and vulnerabilities, with the consent of the individual users; and

"(8) provide sufficient flexibility to permit a range of security solutions.

"SEC. 248. CYBER RISKS TO COVERED CRITICAL INFRASTRUCTURE.

"(a) IDENTIFICATION OF CYBER RISKS.—

"(1) IN GENERAL.—Based on the risk-based assessments conducted under section 242(f)(1)(T)(i), the Director, in coordination with the head of the sector-specific agency with responsibility for covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure, and in consultation with the National Cybersecurity Advisory Council and any private sector entity determined appropriate by the Director, shall, on a continuous and sector-by-sector basis, identify and evaluate the cyber risks to covered critical infrastructure.

"(2) FACTORS TO BE CONSIDERED.—In identifying and evaluating cyber risks under paragraph (1), the Director shall consider—

"(A) the actual or assessed threat, including a consideration of adversary capabilities and intent, preparedness, target attractiveness, and deterrence capabilities;

"(B) the extent and likelihood of death, injury, or serious adverse effects to human health and safety caused by a disruption of the reliable operation of covered critical infrastructure;

"(C) the threat to or impact on national security caused by a disruption of the reliable operation of covered critical infrastructure;

"(D) the extent to which the disruption of the reliable operation of covered critical infrastructure will disrupt the reliable operation of other covered critical infrastructure;

"(E) the harm to the economy that would result from a disruption of the reliable operation of covered critical infrastructure; and

"(F) other risk-based security factors that the Director, in consultation with the head of the sector-specific agency with responsibility for the covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure, determine to be appropriate and necessary to protect public health and safety, critical infrastructure, or national and economic security.

"(3) REPORT.—

"(A) IN GENERAL.—Not later than 180 days after the date of enactment of this subtitle, and annually thereafter, the Director, in coordination with the head of the sector-specific agency

with responsibility for the covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure, shall submit to the appropriate committees of Congress a report on the findings of the identification and evaluation of cyber risks under this subsection. Each report submitted under this paragraph shall be submitted in an unclassified form, but may include a classified annex.

"(B) INPUT.—For purposes of the reports required under subparagraph (A), the Director shall create a process under which owners and operators of covered critical infrastructure may provide input on the findings of the reports.

"(b) RISK-BASED SECURITY PERFORMANCE REQUIREMENTS.—

"(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this subtitle, in coordination with the heads of the sector-specific agencies with responsibility for covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure, and in con-

sultation with the National Cybersecurity Advisory Council and any private sector entity determined appropriate by the Director, the Director shall issue interim final regulations establishing risk-based security performance requirements to secure covered critical infrastructure against cyber risks through the adoption of security measures that satisfy the security performance requirements identified by the Director.

"(2) PROCEDURES.—The regulations issued under this subsection shall—

"(A) include a process under which owners and operators of covered critical infrastructure are informed of identified cyber risks and security performance requirements designed to remediate or mitigate the cyber risks, in combination with best practices recommended under section 247;

"(B) establish a process for owners and operators of covered critical infrastructure to select security measures, including any best practices recommended under section 247, that, in combination, satisfy the security performance requirements established by the Director under this subsection;

"(C) establish a process for owners and operators of covered critical infrastructure to develop response plans for a national cyber emergency declared under section 249;

"(D) establish a process under which the Director—

"(i) is notified of the security measures selected by the owner or operator of covered critical infrastructure under subparagraph (B); and

"(ii) may determine whether the proposed security measures satisfy the security performance requirements established by the Director under this subsection; and

"(E) establish a process under which the Director—

"(i) identifies to owners and operators of covered critical infrastructure cyber risks that are not capable of effective remediation or mitigation using available best practices or security measures;

"(ii) provides owners and operators of covered critical infrastructure the opportunity to develop best practices or security measures to remediate or mitigate the cyber

risks identified in clause (i) without the prior approval of the Director and without affecting the compliance of the covered critical infrastructure with the requirements under this section;

"(iii) in accordance with applicable law relating to the protection of trade secrets, permits owners and operators of covered critical infrastructure to report to the Center the development of effective best practices or security measures to remediate or mitigate the cyber risks identified under clause (i); and

"(iv) incorporates the best practices and security measures developed into the risk-based security performance requirements under this section.

"(3) INTERNATIONAL COOPERATION ON SECURING COVERED CRITICAL INFRASTRUCTURE.—

"(A) IN GENERAL.—The Director, in coordination with the head of the sector-specific agency with responsibility for covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with respon-

sibilities for regulating the covered critical infrastructure, shall—

"(i) consistent with the protection of intelligence sources and methods and other sensitive matters, inform the owner or operator of information infrastructure located outside the United States the disruption of which could result in national or regional catastrophic damage in the United States and the government of the country in which the information infrastructure is located of any cyber risks to the information infrastructure; and

"(ii) coordinate with the government of the country in which the information infrastructure is located and, as appropriate, the owner or operator of the information infrastructure, regarding the implementation of security measures or other measures to the information infrastructure to mitigate or remediate cyber risks.

"(B) INTERNATIONAL AGREEMENTS.—The Director shall carry out this paragraph in a manner consistent with applicable international agreements.

"(4) RISK-BASED SECURITY PERFORMANCE REQUIREMENTS.—

"(A) IN GENERAL.—The security performance requirements established by the Director under this subsection shall be—

"(i) based on the factors listed in subsection (a)(2); and

"(ii) designed to remediate or mitigate identified cyber risks and any associated consequences of an exploitation based on such risks.

"(B) CONSULTATION.—In establishing security performance requirements under this subsection, the Director shall, to the maximum extent practicable, consult with—

"(i) the Director of the National Security Agency;

"(ii) the Director of the National Institute of Standards and Technology;

"(iii) the National Cybersecurity Advisory Council;

"(iv) the heads of sector-specific agencies; and

"(v) the heads of Federal agencies that are not sector-specific agencies with respon-

sibilities for regulating the covered critical infrastructure.

"(C) ALTERNATIVE MEASURES.—

"(i) IN GENERAL.—The owners and operators of covered critical infrastructure shall have flexibility to implement any security measure, or combination thereof, to satisfy the security performance requirements described in subparagraph (A) and the Director may not disapprove under this section any proposed security measures, or combination thereof, based on the presence or absence of any particular security measure if the proposed security measures, or combination thereof, satisfy the security performance requirements established by the Director under this section or are consistent with the process for addressing new or evolving cyber risks established under paragraph (2)(E).

"(ii) RECOMMENDED SECURITY MEASURES.—The Director may recommend to an owner and operator of covered critical infrastructure a specific security measure, or combination thereof, that will satisfy the se-

curity performance requirements established by the Director. The absence of the recommended security measures, or combination thereof, may not serve as the basis for a disapproval of the security measure, or combination thereof, proposed by the owner or operator of covered critical infrastructure if the proposed security measure, or combination thereof, otherwise satisfies the security performance requirements established by the Director under this section.

"SEC. 249. NATIONAL CYBER EMERGENCIES.

"(a) DECLARATION.—

"(1) IN GENERAL.—The President may issue a declaration of a national cyber emergency to covered critical infrastructure if there is an ongoing or imminent action by any individual or entity to exploit a cyber risk in a manner that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure. Any declaration under this section shall specify the covered critical infrastructure subject to the national cyber emergency.

"(2) NOTIFICATION.—Upon issuing a declaration under paragraph (1), the President shall, consistent with the protection of intelligence sources and methods, notify the owners and operators of the specified covered critical infrastructure and any other relevant private sector entity of the nature of the national cyber emergency.

"(3) AUTHORITIES.—If the President issues a declaration under paragraph (1), the Director shall—

"(A) immediately direct the owners and operators of covered critical infrastructure subject to the declaration under paragraph (1) to implement response plans required under section 248(b)(2)(C);

"(B) develop and coordinate emergency measures or actions necessary to preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption, of covered critical infrastructure;

"(C) ensure that emergency measures or actions directed under this section represent the least disruptive means feasible to the operations of the covered critical infrastructure and to the national information infrastructure;

"(D) subject to subsection (g), direct actions by other Federal agencies to respond to the national cyber emergency;

"(E) coordinate with officials of State and local governments, international partners of the United States, owners and operators of covered critical infrastructure specified in the declaration, and other relevant private section entities to respond to the national cyber emergency;

"(F) initiate a process under section 248 to address the cyber risk that may be exploited by the national cyber emergency; and

"(G) provide voluntary technical assistance, if requested, under section 242(f)(1)(S).

"(4) REIMBURSEMENT.—A Federal agency shall be reimbursed for expenditures under this section from funds appropriated for the purposes of this section. Any funds received by a Federal agency as reimbursement for services or supplies furnished under the authority of this section shall be deposited to the credit of the appropriation or appropriations available on the date of the deposit for the services or supplies.

"(5) CONSULTATION.—In carrying out this section, the Director shall consult with the Secretary, the Secretary of Defense, the Director of the National Se-

curity Agency, the Director of the National Institute of Standards and Technology, and any other official, as directed by the President.

"(6) PROHIBITED ACTIONS.—The authority to direct compliance with an emergency measure or action under this section shall not authorize the Director, the Center, the Department, or any other Federal entity to—

"(A) restrict or prohibit communications carried by, or over, covered critical infrastructure and not specifically directed to or from the covered critical infrastructure unless the Director determines that no other emergency measure or action will preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption, of the covered critical infrastructure or the national information infrastructure;

"(B) control covered critical infrastructure;

"(C) compel the disclosure of information unless specifically authorized by law; or

"(D) intercept a wire, oral, or electronic communication (as those terms are defined in section 2510 of title 18, United States Code), access a stored electronic or wire communication,

install or use a pen register or trap and trace device, or conduct electronic surveillance (as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.1801)) relating to an incident unless otherwise authorized under chapter 119, chapter 121, or chapter 206 of title 18, United States Code, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(7) PRIVACY.—In carrying out this section, the Director shall ensure that the privacy and civil liberties of United States persons are protected.

"(b) DISCONTINUANCE OF EMERGENCY MEASURES.—

"(1) IN GENERAL.—Any emergency measure or action developed under this section shall cease to have effect not later than 30 days after the date on which the President issued the declaration of a national cyber emergency, unless—

"(A) the Director details in writing why the emergency measure or action remains necessary to address the identified national cyber emergency; and

"(B) the President issues a written order or directive reaffirming the national cyber emergency, the continuing nature of the national

cyber emergency, or the need to continue the adoption of the emergency measure or action.

"(2) EXTENSIONS.—An emergency measure or action extended in accordance with paragraph (1) may—

"(A) remain in effect for not more than 30 days after the date on which the emergency measure or action was to cease to have effect; and

"(B) unless a joint resolution described in subsection (f)(1) is enacted, be extended for not more than 3 additional 30-day periods, if the requirements of paragraph (1) and subsection (d) are met.

"(c) COMPLIANCE WITH EMERGENCY MEASURES.—

"(1) IN GENERAL.—Subject to paragraph (2), the owner or operator of covered critical infrastructure shall immediately comply with any emergency measure or action developed by the Director under this section during the pendency of any declaration by the President under subsection (a)(1) or an extension under subsection (b)(2).

"(2) ALTERNATIVE MEASURES.—

"(A) IN GENERAL.—If the Director determines that a proposed security measure, or any

combination thereof, submitted by the owner or operator of covered critical infrastructure in accordance with the process established under section 248(b)(2) will effectively mitigate or remediate the cyber risk associated with the national cyber emergency that is the subject of the declaration under this section, or effectively mitigate or remediate the consequences of the potential disruption of the covered critical infrastructure based on the cyber risk at least as effectively as the emergency measures or actions directed by the Director under this section, the owner or operator may comply with paragraph (1) of this subsection by implementing the proposed security measure, or combination thereof, approved by the Director under the process established under section 248.

"(B) COMPLIANCE PENDING SUBMISSION OR APPROVAL.—Before submission of a proposed security measure, or combination thereof, and during the pendency of any review by the Director under the process established under section 248, the owner or operator of covered critical infrastructure shall remain in compliance with any emergency measure or action developed by the

Director under this section during the pendency of any declaration by the President under subsection (a)(1) or an extension under subsection (b)(2), until such time as the Director has approved an alternative proposed security measure, or combination thereof, under this paragraph.

"(3) INTERNATIONAL COOPERATION ON NATIONAL CYBER EMERGENCIES.—

"(A) IN GENERAL.—The Director, in coordination with the head of the sector-specific agency with responsibility for covered critical infrastructure and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure, shall—

"(i) consistent with the protection of intelligence sources and methods and other sensitive matters, inform the owner or operator of information infrastructure located outside the United States the disruption of which could result in national or regional catastrophic damage in the United States and the government of the country in which the information infrastructure is located of any cyber risks to the information infra-

structure that led to the declaration of a national cyber emergency; and

"(ii) coordinate with the government of the country in which the information infrastructure is located and, as appropriate, the owner or operator of the information infrastructure, regarding the implementation of emergency measures or actions necessary to preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption, of covered critical infrastructure that is the subject of the national cyber emergency.

"(B) INTERNATIONAL AGREEMENTS.—The Director shall carry out this paragraph in a manner consistent with applicable international agreements.

"(d) REPORTING.—

"(1) IN GENERAL.—Except as provided in paragraph (2), the President shall ensure that any declaration under subsection (a)(1) or any extension under subsection (b)(2) is reported to the appropriate committees of Congress before the Director mandates any emergency measure or actions under subsection (a)(3).

"(2) EXCEPTION.—If notice cannot be given under paragraph (1) before mandating any emergency measure or actions under subsection (a)(3), the President shall provide the report required under paragraph (1) as soon as possible, along with a statement of the reasons for not providing notice in accordance with paragraph (1).

"(3) CONTENTS.—Each report under this subsection shall describe—

"(A) the nature of the national cyber emergency;

"(B) the reasons that risk-based security requirements under section 248 are not sufficient to address the national cyber emergency;

"(C) the actions necessary to preserve the reliable operation and mitigate the consequences of the potential disruption of covered critical infrastructure; and

"(D) in the case of an extension of a national cyber emergency under subsection (b)(2)—

"(i) why the emergency measures or actions continue to be necessary to address the national cyber emergency; and

"(ii) when the President expects the national cyber emergency to abate.

"(e) STATUTORY DEFENSES AND CIVIL LIABILITY LIMITATIONS FOR COMPLIANCE WITH EMERGENCY MEASURES.—

"(1) DEFINITIONS.—In this subsection—

"(A) the term 'covered civil action'—

"(i) means a civil action filed in a Federal or State court against a covered entity; and

"(ii) does not include an action brought under section 2520 or 2707 of title 18, United States Code, or section 110 or 308 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1810 and 1828);

"(B) the term 'covered entity' means any entity that owns or operates covered critical infrastructure, including any owner, operator, officer, employee, agent, landlord, custodian, provider of information technology, or other person acting for or on behalf of that entity with respect to the covered critical infrastructure; and

"(C) the term 'noneconomic damages' means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companion-

ship, loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.

"(2) APPLICATION OF LIMITATIONS ON CIVIL LIABILITY.—The limitations on civil liability under paragraph (3) apply if—

"(A) the President has issued a declaration of national cyber emergency under subsection (a)(1);

"(B) the Director has—

"(i) issued emergency measures or actions for which compliance is required under subsection (c)(1); or

"(ii) approved security measures under subsection (c)(2);

"(C) the covered entity is in compliance with—

"(i) the emergency measures or actions required under subsection (c)(1); or

"(ii) security measures which the Director has approved under subsection (c)(2); and

"(D)(i) the Director certifies to the court in which the covered civil action is pending that the actions taken by the covered entity during the

period covered by the declaration under subsection (a)(1) were consistent with—

"(I) emergency measures or actions for which compliance is required under subsection (c)(1); or

"(II) security measures which the Director has approved under subsection (c)(2); or

"(ii) notwithstanding the lack of a certification, the covered entity demonstrates by a preponderance of the evidence that the actions taken during the period covered by the declaration under subsection (a)(1) are consistent with the implementation of—

"(I) emergency measures or actions for which compliance is required under subsection (c)(1); or

"(II) security measures which the Director has approved under subsection (c)(2).

"(3) LIMITATIONS ON CIVIL LIABILITY.—In any covered civil action that is related to any incident associated with a cyber risk covered by a declaration of a national cyber emergency and for which Director has issued emergency measures or actions for which compliance is required under subsection (c)(1) or for

which the Director has approved security measures under subsection (c)(2), or that is the direct consequence of actions taken in good faith for the purpose of implementing security measures or actions which the Director has approved under subsection (c)(2)—

"(A) the covered entity shall not be liable for any punitive damages intended to punish or deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses; and

"(B) noneconomic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff, and no plaintiff may recover noneconomic damages unless the plaintiff suffered physical harm.

"(4) CIVIL ACTIONS ARISING OUT OF IMPLEMENTATION OF EMERGENCY MEASURES OR ACTIONS.—A covered civil action may not be maintained against a covered entity that is the direct consequence of actions taken in good faith for the purpose of implementing specific emergency measures or actions for which compliance is required under subsection (c)(1), if—

"(A) the President has issued a declaration of national cyber emergency under subsection (a)(1) and the action was taken during the period covered by that declaration;

"(B) the Director has issued emergency measures or actions for which compliance is required under subsection (c)(1) or that the Director has approved under subsection (c)(2);

"(C) the covered entity is in compliance with the emergency measures required under subsection (c)(1) or that the Director has approved under subsection (c)(2); and

"(D)(i) the Director certifies to the court in which the covered civil action is pending that the actions taken by the entity during the period covered by the declaration under subsection (a)(1) were consistent with the implementation of emergency measures or actions for which compliance is required under subsection (c)(1) or that the Director has approved under subsection (c)(2); or

"(ii) notwithstanding the lack of a certification, the entity demonstrates by a preponderance of the evidence that the actions taken during the period covered by the declaration under

subsection (a)(1) are consistent with the implementation of emergency measures or actions for which compliance is required under subsection (c)(1) or that the Director has approved under subsection (c)(2).

"(5) CERTAIN ACTIONS NOT SUBJECT TO LIMITATIONS ON LIABILITY.—

"(A) ADDITIONAL OR INTERVENING ACTS.—Paragraphs (2) through (4) shall not apply to a civil action relating to any additional or intervening acts or omissions by any covered entity.

"(B) SERIOUS OR SUBSTANTIAL DAMAGE.—Paragraph (4) shall not apply to any civil action brought by an individual—

"(i) whose recovery is otherwise precluded by application of paragraph (4); and

"(ii) who has suffered—

"(I) serious physical injury or death; or

"(II) substantial damage or destruction to his primary residence.

"(C) RULE OF CONSTRUCTION.—Recovery available under subparagraph (B) shall be limited to those damages available under subparagraphs (A) and (B) of paragraph (3), except that

neither reasonable and necessary medical benefits nor lifetime total benefits for lost employment income due to permanent and total disability shall be limited herein.

"(D) INDEMNIFICATION.—In any civil action brought under subparagraph (B), the United States shall defend and indemnify any covered entity. Any covered entity defended and indemnified under this subparagraph shall fully cooperate with the United States in the defense by the United States in any proceeding and shall be reimbursed the reasonable costs associated with such cooperation.

"(f) JOINT RESOLUTION TO EXTEND CYBER EMERGENCY.—

"(1) IN GENERAL.—For purposes of subsection (b)(2)(B), a joint resolution described in this paragraph means only a joint resolution—

"(A) the title of which is as follows: 'Joint resolution approving the extension of a cyber emergency'; and

"(B) the matter after the resolving clause of which is as follows: 'That Congress approves the continuation of the emergency measure or action issued by the Director of the National Center for

Cybersecurity and Communications on _____ for not longer than an additional 120-day period.', the blank space being filled in with the date on which the emergency measure or action to which the joint resolution applies was issued.

"(2) PROCEDURE.—

"(A) NO REFERRAL.—A joint resolution described in paragraph (1) shall not be referred to a committee in either House of Congress and shall immediately be placed on the calendar.

"(B) CONSIDERATION.—

"(i) DEBATE LIMITATION.—A motion to proceed to a joint resolution described in paragraph (1) is highly privileged in the House of Representatives and is privileged in the Senate and is not debatable. The motion is not subject to a motion to postpone. In the Senate, consideration of the joint resolution, and on all debatable motions and appeals in connection therewith, shall be limited to not more than 10 hours, which shall be divided equally between the majority leader and the minority leader, or their designees. A motion further to limit debate

is in order and not debatable. All points of order against the joint resolution (and against consideration of the joint resolution) are waived. An amendment to, or a motion to postpone, or a motion to proceed to the consideration of other business, or a motion to recommit the joint resolution is not in order.

"(ii) PASSAGE.—In the Senate, immediately following the conclusion of the debate on a joint resolution described in paragraph (1), and a single quorum call at the conclusion of the debate if requested in accordance with the rules of the Senate, the vote on passage of the joint resolution shall occur.

"(iii) APPEALS.—Appeals from the decisions of the Chair relating to the application of the rules of the Senate to the procedure relating to a joint resolution described in paragraph (1) shall be decided without debate.

"(C) OTHER HOUSE ACTS FIRST.—If, before the passage by 1 House of a joint resolution of that House described in paragraph (1), that

House receives from the other House a joint resolution described in paragraph (1)—

"(i) the procedure in that House shall be the same as if no joint resolution had been received from the other House; and

"(ii) the vote on final passage shall be on the joint resolution of the other House.

"(D) MAJORITY REQUIRED FOR ADOPTION.—A joint resolution considered under this subsection shall require an affirmative vote of a majority of the Members, duly chosen and sworn, for adoption.

"(3) RULEMAKING.—This subsection is enacted by Congress—

"(A) as an exercise of the rulemaking power of the Senate and the House of Representatives, respectively, and is deemed to be part of the rules of each House, respectively but applicable only with respect to the procedure to be followed in that House in the case of a joint resolution described in paragraph (1), and it supersedes other rules only to the extent that it is inconsistent with such rules; and

"(B) with full recognition of the constitutional right of either House to change the rules

(so far as they relate to the procedure of that House) at any time, in the same manner, and to the same extent as in the case of any other rule of that House.

"(g) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to—

"(1) alter or supersede the authority of the Secretary of Defense, the Attorney General, or the Director of National Intelligence in responding to a national cyber emergency; or

"(2) limit the authority of the Director under section 248, after a declaration issued under this section expires.

"SEC. 250. ENFORCEMENT.

"(a) ANNUAL CERTIFICATION OF COMPLIANCE.—

"(1) IN GENERAL.—Not later than 6 months after the date on which the Director promulgates regulations under section 248(b), and every year thereafter, each owner or operator of covered critical infrastructure shall certify in writing to the Director whether the owner or operator has developed and implemented, or is implementing, security measures approved by the Director under section 248 and any applicable emergency measures or actions required

under section 249 for any cyber risks and national cyber emergencies.

"(2) FAILURE TO COMPLY.—If an owner or operator of covered critical infrastructure fails to submit a certification in accordance with paragraph (1), or if the certification indicates the owner or operator is not in compliance, the Director may issue an order requiring the owner or operator to submit proposed security measures under section 248 or comply with specific emergency measures or actions under section 249.

"(b) RISK-BASED EVALUATIONS.—

"(1) IN GENERAL.—Consistent with the factors described in paragraph (3), the Director may perform an evaluation of the information infrastructure of any specific system or asset constituting covered critical infrastructure to assess the validity of a certification of compliance submitted under subsection (a)(1).

"(2) DOCUMENT REVIEW AND INSPECTION.—An evaluation performed under paragraph (1) may include—

"(A) a review of all documentation submitted to justify an annual certification of compliance submitted under subsection (a)(1); and

"(B) a physical or electronic inspection of relevant information infrastructure to which the security measures required under section 248 or the emergency measures or actions required under section 249 apply.

"(3) EVALUATION SELECTION FACTORS.—In determining whether sufficient risk exists to justify an evaluation under this subsection, the Director shall consider—

"(A) the specific cyber risks affecting or potentially affecting the information infrastructure of the specific system or asset constituting covered critical infrastructure;

"(B) any reliable intelligence or other information indicating a cyber risk or credible national cyber emergency to the information infrastructure of the specific system or asset constituting covered critical infrastructure;

"(C) actual knowledge or reasonable suspicion that the certification of compliance submitted by a specific owner or operator of covered critical infrastructure is false or otherwise inaccurate;

"(D) a request by a specific owner or operator of covered critical infrastructure for such an evaluation; and

"(E) such other risk-based factors as identified by the Director.

"(4) SECTOR-SPECIFIC AGENCIES.—To carry out the risk-based evaluation authorized under this subsection, the Director may use the resources of a sector-specific agency with responsibility for the covered critical infrastructure or any Federal agency that is not a sector-specific agency with responsibilities for regulating the covered critical infrastructure with the concurrence of the head of the agency.

"(5) INFORMATION PROTECTION.—Information provided to the Director during the course of an evaluation under this subsection shall be protected from disclosure in accordance with section 251.

"(c) CIVIL PENALTIES.—

"(1) IN GENERAL.—Any person who violates section 248 or 249 shall be liable for a civil penalty.

"(2) NO PRIVATE RIGHT OF ACTION.—Nothing in this section confers upon any person, except the Director, a right of action against an owner or operator of covered critical infrastructure to enforce any provision of this subtitle.

"(d) LIMITATION ON CIVIL LIABILITY.—

"(1) DEFINITION.—In this subsection—

"(A) the term 'covered civil action'—

"(i) means a civil action filed in a Federal or State court against a covered entity; and

"(ii) does not include an action brought under section 2520 or 2707 of title 18, United States Code, or section 110 or 308 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1810 and 1828);

"(B) the term 'covered entity' means any entity that owns or operates covered critical infrastructure, including any owner, operator, officer, employee, agent, landlord, custodian, provider of information technology, or other person acting for or on behalf of that entity with respect to the covered critical infrastructure; and

"(C) the term 'noneconomic damages' means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium, hedonic damages, injury

to reputation, and any other nonpecuniary losses.

"(2) LIMITATIONS ON CIVIL LIABILITY.—If a covered entity experiences an incident related to a cyber risk identified under section 248(a), in any covered civil action for damages directly caused by the incident related to that cyber risk—

"(A) the covered entity shall not be liable for any punitive damages intended to punish or deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses; and

"(B) noneconomic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff, and no plaintiff may recover noneconomic damages unless the plaintiff suffered physical harm.

"(3) APPLICATION.—This subsection shall apply to claims made by any individual or nongovernmental entity, including claims made by a State or local government agency on behalf of such individuals or nongovernmental entities, against a covered entity—

"(A) whose proposed security measures, or combination thereof, satisfy the security performance requirements established under subsection 248(b) and have been approved by the Director;

"(B) that has been evaluated under subsection (b) and has been found by the Director to have implemented the proposed security measures approved under section 248; and

"(C) that is in actual compliance with the approved security measures at the time of the incident related to that cyber risk.

"(4) LIMITATION.—This subsection shall only apply to harm directly caused by the incident related to the cyber risk and shall not apply to damages caused by any additional or intervening acts or omissions by the covered entity.

"(5) RULE OF CONSTRUCTION.—Except as provided under paragraph (3), nothing in this subsection shall be construed to abrogate or limit any right, remedy, or authority that the Federal Government or any State or local government, or any entity or agency thereof, may possess under any law, or that any individual is authorized by law to bring on behalf of the government.

"(e) REPORT TO CONGRESS.—The Director shall submit an annual report to the appropriate committees of Congress on the implementation and enforcement of the risk-based performance requirements of covered critical infrastructure under subsection 248(b) and this section including—

"(1) the level of compliance of covered critical infrastructure with the risk-based security performance requirements issued under section 248(b);

"(2) how frequently the evaluation authority under subsection (b) was utilized and a summary of the aggregate results of the evaluations; and

"(3) any civil penalties imposed on covered critical infrastructure.

"SEC. 251. PROTECTION OF INFORMATION.

"(a) DEFINITION.—In this section, the term 'covered information'—

"(1) means—

"(A) any information required to be submitted under sections 246, 248, and 249 to the Center by the owners and operators of covered critical infrastructure; and

"(B) any information submitted to the Center under the processes and procedures established under section 246 by State and local gov-

ernments, private entities, and international partners of the United States regarding threats, vulnerabilities, and incidents affecting—

"(i) the Federal information infrastructure;

"(ii) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community; or

"(iii) the national information infrastructure; and

"(2) shall not include any information described under paragraph (1), if that information is submitted to—

"(A) conceal violations of law, inefficiency, or administrative error;

"(B) prevent embarrassment to a person, organization, or agency; or

"(C) interfere with competition in the private sector.

"(b) VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.—Covered information submitted in accordance with this section shall be treated as voluntarily shared critical infrastructure information under section

214, except that the requirement of section 214 that the information be voluntarily submitted, including the requirement for an express statement, shall not be required for submissions of covered information.

"(c) GUIDELINES.—

"(1) IN GENERAL.—Subject to paragraph (2), the Director shall develop and issue guidelines, in consultation with the Secretary, Attorney General, and the National Cybersecurity Advisory Council, as necessary to implement this section.

"(2) REQUIREMENTS.—The guidelines developed under this section shall—

"(A) consistent with section 214(e)(2)(D) and (g) and the processes, procedures, and guidelines developed under section 246(b), include provisions for information sharing among Federal, State, and local and officials, private entities, or international partners of the United States necessary to carry out the authorities and responsibilities of the Director;

"(B) be consistent, to the maximum extent possible, with policy guidance and implementation standards developed by the National Archives and Records Administration for controlled unclassified information, including with respect

to marking, safeguarding, dissemination and dispute resolution; and

"(C) describe, with as much detail as possible, the categories and type of information entities should voluntarily submit under subsections (b) and (c)(1)(B) of section 246.

"(d) PROCESS FOR REPORTING SECURITY PROBLEMS.—

"(1) ESTABLISHMENT OF PROCESS.—The Director shall establish through regulation, and provide information to the public regarding, a process by which any person may submit a report to the Secretary regarding cybersecurity threats, vulnerabilities, and incidents affecting—

"(A) the Federal information infrastructure;

"(B) information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community; or

"(C) national information infrastructure.

"(2) ACKNOWLEDGMENT OF RECEIPT.—If a report submitted under paragraph (1) identifies the person making the report, the Director shall respond

promptly to such person and acknowledge receipt of the report.

"(3) STEPS TO ADDRESS PROBLEM.—The Director shall review and consider the information provided in any report submitted under paragraph (1) and, at the sole, unreviewable discretion of the Director, determine what, if any, steps are necessary or appropriate to address any problems or deficiencies identified.

"(4) DISCLOSURE OF IDENTITY.—

"(A) IN GENERAL.—Except as provided in subparagraph (B), or with the written consent of the person, the Secretary may not disclose the identity of a person who has provided information described in paragraph (1).

"(B) REFERRAL TO THE ATTORNEY GENERAL.—The Secretary shall disclose to the Attorney General the identity of a person described under subparagraph (A) if the matter is referred to the Attorney General for enforcement. The Director shall provide reasonable advance notice to the affected person if disclosure of that person's identity is to occur, unless such notice would risk compromising a criminal or civil enforcement investigation or proceeding.

"(e) RULES OF CONSTRUCTION.—Nothing in this section shall be construed to—

"(1) limit or otherwise affect the right, ability, duty, or obligation of any entity to use or disclose any information of that entity, including in the conduct of any judicial or other proceeding;

"(2) prevent the classification of information submitted under this section if that information meets the standards for classification under Executive Order 12958 or any successor of that order or affect measures and controls relating to the protection of classified information as prescribed by Federal statute or under Executive Order 12958, or any successor of that order;

"(3) limit the right of an individual to make any disclosure—

"(A) protected or authorized under section 2302(b)(8) or 7211 of title 5, United States Code;

"(B) to an appropriate official of information that the individual reasonably believes evidences a violation of any law, rule, or regulation, gross mismanagement, or substantial and specific danger to public health, safety, or security, and that is protected under any Federal or State law (other than those referenced in sub-

paragraph (A)) that shields the disclosing individual against retaliation or discrimination for having made the disclosure if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs; or

"(C) to the Special Counsel, the inspector general of an agency, or any other employee designated by the head of an agency to receive similar disclosures;

"(4) prevent the Director from using information required to be submitted under sections 246, 248, or 249 for enforcement of this subtitle, including enforcement proceedings subject to appropriate safeguards;

"(5) authorize information to be withheld from Congress, the Government Accountability Office, or Inspector General of the Department;

"(6) affect protections afforded to trade secrets under any other provision of law; or

"(7) create a private right of action for enforcement of any provision of this section.

"(f) AUDIT.—

"(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Protecting Cyberspace as

a National Asset Act of 2010, the Inspector General of the Department shall conduct an audit of the management of information submitted under subsection (b) and report the findings to appropriate committees of Congress.

"(2) CONTENTS.—The audit under paragraph (1) shall include assessments of—

"(A) whether the information is adequately safeguarded against inappropriate disclosure;

"(B) the processes for marking and disseminating the information and resolving any disputes;

"(C) how the information is used for the purposes of this section, and whether that use is effective;

"(D) whether information sharing has been effective to fulfill the purposes of this section;

"(E) whether the kinds of information submitted have been appropriate and useful, or overbroad or overnarrow;

"(F) whether the information protections allow for adequate accountability and transparency of the regulatory, enforcement, and other aspects of implementing this subtitle; and

"(G) any other factors at the discretion of the Inspector General.

"SEC. 252. SECTOR-SPECIFIC AGENCIES.

"(a) IN GENERAL.—The head of each sector-specific agency and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating covered critical infrastructure shall coordinate with the Director on any activities of the sector-specific agency or Federal agency that relate to the efforts of the agency regarding security or resiliency of the national information infrastructure, including critical infrastructure and covered critical infrastructure, within or under the supervision of the agency.

"(b) DUPLICATIVE REPORTING REQUIREMENTS.—The head of each sector-specific agency and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating covered critical infrastructure shall coordinate with the Director to eliminate and avoid the creation of duplicate reporting or compliance requirements relating to the security or resiliency of the national information infrastructure, including critical infrastructure and covered critical infrastructure, within or under the supervision of the agency.

"(c) REQUIREMENTS.—

"(1) IN GENERAL.—To the extent that the head of each sector-specific agency and the head of any Federal agency that is not a sector-specific agency with responsibilities for regulating covered critical infrastructure has the authority to establish regulations, rules, or requirements or other required actions that are applicable to the security of national information infrastructure, including critical infrastructure and covered critical infrastructure, the head of that agency shall—

"(A) notify the Director in a timely fashion of the intent to establish the regulations, rules, requirements, or other required actions;

"(B) coordinate with the Director to ensure that the regulations, rules, requirements, or other required actions are consistent with, and do not conflict or impede, the activities of the Director under sections 247, 248, and 249; and

"(C) in coordination with the Director, ensure that the regulations, rules, requirements, or other required actions are implemented, as they relate to covered critical infrastructure, in accordance with subsection (a).

"(2) COORDINATION.—Coordination under paragraph (1)(B) shall include the active participation of

the Director in the process for developing regulations, rules, requirements, or other required actions.

"(3) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide additional authority for any sector-specific agency or any Federal agency that is not a sector-specific agency with responsibilities for regulating national information infrastructure, including critical infrastructure or covered critical infrastructure, to establish standards or other measures that are applicable to the security of national information infrastructure not otherwise authorized by law.

"SEC. 253. STRATEGY FOR FEDERAL CYBERSECURITY SUPPLY CHAIN MANAGEMENT.

"(a) IN GENERAL.—The Secretary, in consultation with the Director of Cyberspace Policy, the Director, the Secretary of Defense, the Secretary of Commerce, the Secretary of State, the Director of National Intelligence, the Administrator of General Services, the Administrator for Federal Procurement Policy, the other members of the Chief Information Officers Council established under section 3603 of title 44, United States Code, the Chief Acquisition Officers Council established under section 16A of the Office of Federal Procurement Policy Act (41 U.S.C. 414b), the Chief Financial Officers Council established under section 302 of

the Chief Financial Officers Act of 1990 (31 U.S.C. 901 note), and the private sector, shall develop, periodically update, and implement a supply chain risk management strategy designed to ensure, based on mission criticality and cost effectiveness, the security of the Federal information infrastructure, including protection against unauthorized access to, alteration of information in, disruption of operations of, interruption of communications or services of, and insertion of malicious software, engineering vulnerabilities, or otherwise corrupting software, hardware, services, or products intended for use in Federal information infrastructure.

"(b) CONTENTS.—The supply chain risk management strategy developed under subsection (a) shall—

"(1) address risks in the supply chain during the entire life cycle of any part of the Federal information infrastructure;

"(2) place particular emphasis on—

"(A) securing critical information systems and the Federal information infrastructure;

"(B) developing processes that—

"(i) incorporate all-source intelligence analysis into assessments of the supply chain for the Federal information infrastructure;

"(ii) assess risks from potential suppliers providing critical components or services of the Federal information infrastructure;

"(iii) assess risks from individual components, including all subcomponents, or software used in or affecting the Federal information infrastructure;

"(iv) manage the quality, configuration, and security of software, hardware, and systems of the Federal information infrastructure throughout the life cycle of the software, hardware, or system, including components or subcomponents from secondary and tertiary sources;

"(v) detect the occurrence, reduce the likelihood of occurrence, and mitigate or remediate the risks associated with products containing counterfeit components or malicious functions;

"(vi) enhance developmental and operational test and evaluation capabilities, including software vulnerability detection methods and automated methods and tools that shall be integrated into acquisition pol-

icy practices by Federal agencies and, where appropriate, make the capabilities available for use by the private sector; and

"(vii) protect the intellectual property and trade secrets of suppliers of information and communications technology products and services;

"(C) the use of internationally-recognized standards and standards developed by the private sector and developing a process, with the National Institute for Standards and Technology, to make recommendations for improvements of the standards;

"(D) identifying acquisition practices of Federal agencies that increase risks in the supply chain and developing a process to provide recommendations for revisions to those processes; and

"(E) sharing with the private sector, to the fullest extent possible, the threats identified in the supply chain and working with the private sector to develop responses to those threats as identified; and

"(3) to the maximum extent practicable, promote the ability of Federal agencies to procure authentic

commercial off the shelf information and communications technology products and services from a diverse pool of suppliers.

"(c) IMPLEMENTATION.—The Federal Acquisition Regulatory Council established under section 25(a) of the Office of Federal Procurement Policy Act (41 U.S.C. 421(a)) shall—

"(1) amend the Federal Acquisition Regulation issued under section 25 of that Act to—

"(A) incorporate, where relevant, the supply chain risk management strategy developed under subsection (a) to improve security throughout the acquisition process; and

"(B) direct that all software and hardware purchased by the Federal Government shall comply with standards developed or be interoperable with automated tools approved by the National Institute of Standards and Technology, to continually enhance security; and

"(2) develop a clause or set of clauses for inclusion in solicitations, contracts, and task and delivery orders that sets forth the responsibility of the contractor under the Federal Acquisition Regulation provisions implemented under this subsection.

"(d) PREFERENCES FOR ACQUISITION OF COMMERCIAL ITEMS.—The strategy developed under this section, and any actions taken under subsection (c), shall be consistent with the preferences for the acquisition of commercial items under section 2377 of title 10, United States Code, and section 314B of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 264b).".

TITLE III—FEDERAL INFORMATION SECURITY MANAGEMENT

SEC. 301. COORDINATION OF FEDERAL INFORMATION POLICY.

(a) FINDINGS.—Congress finds that—

(1) since 2002 the Federal Government has experienced multiple high-profile incidents that resulted in the theft of sensitive information amounting to more than the entire print collection contained in the Library of Congress, including personally identifiable information, advanced scientific research, and prenegotiated United States diplomatic positions; and

(2) chapter 35 of title 44, United States Code, must be amended to increase the coordination of Federal agency activities and to enhance situational awareness throughout the Federal Government using

more effective enterprise-wide automated monitoring, detection, and response capabilities.

(b) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

"SUBCHAPTER II—INFORMATION SECURITY

"§ 3550. Purposes

"The purposes of this subchapter are to—

"(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support the Federal information infrastructure and the operations and assets of agencies;

"(2) recognize the highly networked nature of the current Federal information infrastructure and provide effective Government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

"(3) provide for development and maintenance of prioritized and risk-based security controls required to protect Federal information infrastructure and information systems; and

"(4) provide a mechanism for improved oversight of Federal agency information security programs.

"(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the Nation that are designed, built, and operated by the private sector; and

"(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

"§ 3551. Definitions

"(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

"(b) ADDITIONAL DEFINITIONS.—In this subchapter:

"(1) The term 'agency information infrastructure'—

"(A) means information infrastructure that is owned, operated, controlled, or licensed for use by, or on behalf of, an agency, including infor-

mation systems used or operated by another entity on behalf of the agency; and

"(B) does not include national security systems.

"(2) The term 'automated and continuous monitoring' means monitoring at a frequency and sufficiency such that the data exchange requires little to no human involvement and is not interrupted;

"(3) The term 'incident' means an occurrence that—

"(A) actually or imminently jeopardizes—

"(i) the information security of information infrastructure; or

"(ii) the information that information infrastructure processes, stores, receives, or transmits; or

"(B) constitutes a violation of security policies, security procedures, or acceptable use policies applicable to information infrastructure.

"(4) The term 'information infrastructure' means the underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including programmable electronic devices and communications

networks and any associated hardware, software, or data.

"(5) The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

"(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

"(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

"(C) availability, by ensuring timely and reliable access to and use of information.

"(6) The term 'information technology' has the meaning given that term in section 11101 of title 40.

"(7) The term 'management controls' means safeguards or countermeasures for an information system that focus on the management of risk and the management of information system security.

"(8)(A) The term 'national security system' means any information system (including any telecommunications system) used or operated by an agen-

cy or by a contractor of an agency, or other organization on behalf of an agency—

"(i) the function, operation, or use of which—

"(I) involves intelligence activities;

"(II) involves cryptologic activities related to national security;

"(III) involves command and control of military forces;

"(IV) involves equipment that is an integral part of a weapon or weapons system; or

"(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

"(ii) that is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

"(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

"(9) The term 'operational controls' means the safeguards and countermeasures for an information system that are primarily implemented and executed by individuals, not systems.

"(10) The term 'risk' means the potential for an unwanted outcome resulting from an incident, as determined by the likelihood of the occurrence of the incident and the associated consequences, including potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident

"(11) The term 'risk-based security' means security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification, of information, including assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability.

"(12) The term 'security controls' means the management, operational, and technical controls prescribed for an information system to protect the information security of the system.

"(13) The term 'technical controls' means the safeguards or countermeasures for an information system that are primarily implemented and executed

by the information system through mechanism contained in the hardware, software, or firmware components of the system.

"§ 3552. Authority and functions of the National Center for Cybersecurity and Communications

"(a) IN GENERAL.—The Director of the National Center for Cybersecurity and Communications shall—

"(1) develop, oversee the implementation of, and enforce policies, principles, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and subtitle E of title II of the Homeland Security Act of 2002;

"(2) provide to agencies security controls that agencies shall be required to be implemented to mitigate and remediate vulnerabilities, attacks, and exploitations discovered as a result of activities required under this subchapter or subtitle E of title II of the Homeland Security Act of 2002;

"(3) to the extent practicable—

"(A) prioritize the policies, principles, standards, and guidelines promulgated under section 20 of the National Institute of Standards

and Technology Act (15 U.S.C. 278g–3), paragraph (1), and subtitle E of title II of the Homeland Security Act of 2002, based upon the risk of an incident; and

"(B) develop guidance that requires agencies to monitor, including automated and continuous monitoring of, the effective implementation of policies, principles, standards, and guidelines developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), paragraph (1), and subtitle E of title II of the Homeland Security Act of 2002;

"(C) ensure the effective operation of technical capabilities within the National Center for Cybersecurity and Communications to enable automated and continuous monitoring of any information collected as a result of the guidance developed under subparagraph (B) and use the information to enhance the risk-based security of the Federal information infrastructure; and

"(D) ensure the effective operation of a secure system that satisfies information reporting requirements under sections 3553(c) and 3556(c);

"(4) require agencies, consistent with the standards developed under section 20 of the National Insti-

tute of Standards and Technology Act (15 U.S.C. 278g–3) or paragraph (1) and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk resulting from the disruption or unauthorized access, use, disclosure, modification, or destruction of—

"(A) information collected or maintained by or on behalf of an agency; or

"(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

"(5) oversee agency compliance with the requirements of this subchapter, including coordinating with the Office of Management and Budget to use any authorized action under section 11303 of title 40 to enforce accountability for compliance with such requirements;

"(6) review, at least annually, and approve or disapprove, agency information security programs required under section 3553(b); and

"(7) coordinate information security policies and procedures with the Administrator for Electronic Government and the Administrator for the Office of Information and Regulatory Affairs with related infor-

mation resources management policies and procedures.

"(b) NATIONAL SECURITY SYSTEMS.—The authorities of the Director of the National Center for Cybersecurity and Communications under this section shall not apply to national security systems.

"§ 3553. Agency responsibilities

"(a) IN GENERAL.—The head of each agency shall—

"(1) be responsible for—

"(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

"(i) information collected or maintained by or on behalf of the agency; and

"(ii) agency information infrastructure;

"(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

"(i) information security requirements, including security controls, developed by the Director of the National Center for Cybersecurity and Communications under section

3552, subtitle E of title II of the Homeland Security Act of 2002, or any other provision of law;

"(ii) information security policies, principles, standards, and guidelines promulgated under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and section 3552(a)(1);

"(iii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

"(iv) ensuring the standards implemented for information systems and national security systems of the agency are complementary and uniform, to the extent practicable;

"(C) ensuring that information security management processes are integrated with agency strategic and operational planning and budget processes, including policies, procedures, and practices described in subsection (c)(1)(C);

"(D) as appropriate, maintaining secure facilities that have the capability of accessing,

sending, receiving, and storing classified information;

"(E) maintaining a sufficient number of personnel with security clearances, at the appropriate levels, to access, send, receive and analyze classified information to carry out the responsibilities of this subchapter; and

"(F) ensuring that information security performance indicators and measures are included in the annual performance evaluations of all managers, senior managers, senior executive service personnel, and political appointees;

"(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under the control of those officials, including through—

"(A) assessing the risk and magnitude of the harm that could result from the disruption or unauthorized access, use, disclosure, modification, or destruction of such information or information systems;

"(B) determining the levels of information security appropriate to protect such information and information systems in accordance with

policies, principles, standards, and guidelines promulgated under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), section 3552(a)(1), and subtitle E of title II of the Homeland Security Act of 2002, for information security categorizations and related requirements;

"(C) implementing policies and procedures to cost effectively reduce risks to an acceptable level;

"(D) periodically testing and evaluating information security controls and techniques to ensure that such controls and techniques are operating effectively; and

"(E) withholding all bonus and cash awards to senior agency officials accountable for the operation of such agency information infrastructure that are recognized by the Chief Information Security Officer as impairing the risk-based security information, information system, or agency information infrastructure;

"(3) delegate to a senior agency officer designated as the Chief Information Security Officer the authority and budget necessary to ensure and enforce compliance with the requirements imposed on the

agency under this subchapter, subtitle E of title II of the Homeland Security Act of 2002, or any other provision of law, including—

"(A) overseeing the establishment, maintenance, and management of a security operations center that has technical capabilities that can, through automated and continuous monitoring—

"(i) detect, report, respond to, contain, remediate, and mitigate incidents that impair risk-based security of the information, information systems, and agency information infrastructure, in accordance with policy provided by the Director of the National Center for Cybersecurity and Communications;

"(ii) monitor and, on a risk-based basis, mitigate and remediate the vulnerabilities of every information system within the agency information infrastructure;

"(iii) continually evaluate risks posed to information collected or maintained by or on behalf of the agency and information systems and hold senior agency officials accountable for ensuring the risk-based secu-

rity of such information and information systems;

"(iv) collaborate with the Director of the National Center for Cybersecurity and Communications and appropriate public and private sector security operations centers to address incidents that impact the security of information and information systems that extend beyond the control of the agency; and

"(v) report any incident described under clauses (i) and (ii), as directed by the policy of the Director of the National Center for Cybersecurity and Communications and the Inspector General of the agency;

"(B) collaborating with the Administrator for E–Government and the Chief Information Officer to establish, maintain, and update an enterprise network, system, storage, and security architecture, that can be accessed by the National Cybersecurity Communications Center and includes—

"(i) information on how security controls are implemented throughout the agency information infrastructure; and

"(ii) information on how the controls described under subparagraph (A) maintain the appropriate level of confidentiality, integrity, and availability of information and information systems based on—

"(I) the policy of the Director of the National Center for Cybersecurity and Communications; and

"(II) the standards or guidance developed by the National Institute of Standards and Technology;

"(C) developing, maintaining, and overseeing an agency-wide information security program as required by subsection (b);

"(D) developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3552;

"(E) training, consistent with the requirements of section 406 of the Protecting Cyberspace as a National Asset Act of 2010, and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

"(F) assisting senior agency officers concerning their responsibilities under paragraph (2);

"(4) ensure that the Chief Information Security Officer has a sufficient number of cleared and trained personnel with technical skills identified by the Director of the National Center for Cybersecurity and Communications as critical to maintaining the risk-based security of agency information infrastructure as required by the subchapter and other applicable laws;

"(5) ensure that the agency Chief Information Security Officer, in coordination with appropriate senior agency officials, reports not less than annually to the head of the agency on the effectiveness of the agency information security program, including progress of remedial actions;

"(6) ensure that the Chief Information Security Officer—

"(A) possesses necessary qualifications, including education, professional certifications, training, experience, and the security clearance required to administer the functions described under this subchapter; and

"(B) has information security duties as the primary duty of that officer; and

"(7) ensure that components of that agency establish and maintain an automated reporting mechanism that allows the Chief Information Security Officer with responsibility for the entire agency, and all components thereof, to implement, monitor, and hold senior agency officers accountable for the implementation of appropriate security policies, procedures, and controls of agency components.

"(b) AGENCY-WIDE INFORMATION SECURITY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program, approved by the Director of the National Center for Cybersecurity and Communications under section 3552(a)(6) and consistent with components across and within agencies, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

"(1) frequent assessments, at least twice each month—

"(A) of the risk and magnitude of the harm that could result from the disruption or unauthorized access, use, disclosure, modification, or destruction of information and information sys-

tems that support the operations and assets of the agency; and

"(B) that assess whether information or information systems should be removed or migrated to more secure networks or standards and make recommendations to the head of the agency and the Director of the National Center for Cybersecurity and Communications based on that assessment;

"(2) consistent with guidance developed under section 3554, vulnerability assessments and penetration tests commensurate with the risk posed to an agency information infrastructure;

"(3) ensure that information security vulnerabilities are remediated or mitigated based on the risk posed to the agency;

"(4) policies and procedures that—

"(A) are informed and revised by the assessments required under paragraphs (1) and (2);

"(B) cost effectively reduce information security risks to an acceptable level;

"(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

"(D) ensure compliance with—

"(i) the requirements of this subchapter;

"(ii) policies and procedures prescribed by the Director of the National Center for Cybersecurity and Communications;

"(iii) minimally acceptable system configuration requirements, as determined by the Director of the National Center for Cybersecurity and Communications; and

"(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

"(5) subordinate plans for providing risk-based information security for networks, facilities, and systems or groups of information systems, as appropriate;

"(6) role-based security awareness training, consistent with the requirements of section 406 of the Protecting Cyberspace as a National Asset Act of 2010, to inform personnel with access to the agency network, including contractors and other users of information systems that support the operations and assets of the agency, of—

"(A) information security risks associated with agency activities; and

"(B) agency responsibilities in complying with agency policies and procedures designed to reduce those risks;

"(7) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a rigor and frequency depending on risk, which shall include—

"(A) testing and evaluation not less than twice each year of security controls of information collected or maintained by or on behalf of the agency and every information system identified in the inventory required under section 3505(c);

"(B) the effectiveness of ongoing monitoring, including automated and continuous monitoring, vulnerability scanning, and intrusion detection and prevention of incidents posed to the risk-based security of information and information systems as required under subsection (a)(3); and

"(C) testing relied on in—

"(i) an operational evaluation under section 3554;

"(ii) an independent assessment under section 3556; or

"(iii) another evaluation, to the extent specified by the Director of the National Center for Cybersecurity and Communications;

"(8) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

"(9) procedures for detecting, reporting, and responding to incidents, consistent with requirements issued under section 3552, that include—

"(A) to the extent practicable, automated and continuous monitoring of the use of information and information systems;

"(B) requirements for mitigating risks and remediating vulnerabilities associated with such incidents systemically within the agency information infrastructure before substantial damage is done; and

"(C) notifying and coordinating with the Director of the National Center for Cybersecurity and Communications, as required by this subchapter, subtitle E of title II of the Homeland

Security Act of 2002, and any other provision of law; and

"(10) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

"(c) AGENCY REPORTING.—

"(1) IN GENERAL.—Each agency shall—

"(A) ensure that information relating to the adequacy and effectiveness of information security policies, procedures, and practices, is available to the entities identified under paragraph (2) through the system developed under section 3552(a)(3), including information relating to—

"(i) compliance with the requirements of this subchapter;

"(ii) the effectiveness of the information security policies, procedures, and practices of the agency based on a determination of the aggregate effect of identified deficiencies and vulnerabilities;

"(iii) an identification and analysis of any significant deficiencies identified in such policies, procedures, and practices;

"(iv) an identification of any vulnerability that could impair the risk-based se-

curity of the agency information infrastructure; and

"(v) results of any operational evaluation conducted under section 3554 and plans of action to address the deficiencies and vulnerabilities identified as a result of such operational evaluation;

"(B) follow the policy, guidance, and standards of the Director of the National Center for Cybersecurity and Communications, in consultation with the Federal Information Security Taskforce, to continually update, and ensure the electronic availability of both a classified and unclassified version of the information required under subparagraph (A);

"(C) ensure the information under subparagraph (A) addresses the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

"(i) annual agency budgets;

"(ii) information resources management of this subchapter;

"(iii) information technology management and procurement under this chapter or any other applicable provision of law;

"(iv) subtitle E of title II of the Homeland Security Act of 2002;

"(v) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

"(vi) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

"(vii) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note);

"(viii) internal accounting and administrative controls under section 3512 of title 31; and

"(ix) performance ratings, salaries, and bonuses provided to the senior managers and supporting personnel taking into account program performance as it relates to complying with this subchapter; and

"(D) report any significant deficiency in a policy, procedure, or practice identified under subparagraph (A) or (B)—

"(i) as a material weakness in reporting under section 3512 of title 31; and

"(ii) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

"(2) ADEQUACY AND EFFECTIVENESS INFORMATION.—Information required under paragraph (1)(A) shall, to the extent possible and in accordance with applicable law, policy, guidance, and standards, be available on an automated and continuous basis to—

"(A) the Director of the National Center for Cybersecurity and Communications;

"(B) the Office of Management and Budget;

"(C) the Committee on Homeland Security and Governmental Affairs of the Senate;

"(D) the Committee on Government Oversight and Reform of the House of Representatives;

"(E) the Committee on Homeland Security of the House of Representatives;

"(F) other appropriate authorization and appropriations committees of Congress;

"(G) the Inspector General of the Federal agency; and

"(H) the Comptroller General.

"(d) INCLUSIONS IN PERFORMANCE PLANS.—

"(1) IN GENERAL.—In addition to the requirements of subsection (c), each agency, in consultation with the Director of the National Center for Cybersecurity and Communications, shall include as part of the performance plan required under section 1115 of title 31 a description of the time periods the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

"(2) RISK ASSESSMENTS.—The description under paragraph (1) shall be based on the risk and vulnerability assessments required under subsection (b) and evaluations required under section 3554.

"(e) NOTICE AND COMMENT.—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

"(f) MORE STRINGENT STANDARDS.—The head of an agency may employ standards for the cost effective information security for information systems within or under the

supervision of that agency that are more stringent than the standards the Director of the National Center for Cybersecurity and Communications prescribes under this subchapter, subtitle E of title II of the Homeland Security Act of 2002, or any other provision of law, if the more stringent standards—

"(1) contain at least the applicable standards made compulsory and binding by the Director of the National Center for Cybersecurity and Communications; and

"(2) are otherwise consistent with policies and guidelines issued under section 3552.

"§ 3554. Annual operational evaluation

"(a) GUIDANCE.—

"(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Protecting Cyberspace as a National Asset Act of 2010 and each year thereafter, the Director of the National Center for Cybersecurity and Communications shall oversee, coordinate, and develop guidance for the effective implementation of operational evaluations of the Federal information infrastructure and agency information security programs and practices to determine the effectiveness of such program and practices.

"(2) COLLABORATION IN DEVELOPMENT.—In developing guidance for the operational evaluations described under this section, the Director of the National Center for Cybersecurity and Communications shall collaborate with the Federal Information Security Taskforce and the Council of Inspectors General on Integrity and Efficiency, and other agencies as necessary, to develop and update risk-based performance indicators and measures that assess the adequacy and effectiveness of information security of an agency and the Federal information infrastructure.

"(3) CONTENTS OF OPERATIONAL EVALUATION.—Each operational evaluation under this section—

"(A) shall be prioritized based on risk; and

"(B) shall—

"(i) test the effectiveness of agency information security policies, procedures, and practices of the information systems of the agency, or a representative subset of those information systems;

"(ii) assess (based on the results of the testing) compliance with—

"(I) the requirements of this subchapter; and

"(II) related information security policies, procedures, standards, and guidelines;

"(iii) evaluate whether agencies—

"(I) effectively monitor, detect, analyze, protect, report, and respond to vulnerabilities and incidents;

"(II) report to and collaborate with the appropriate public and private security operation centers, the Director of the National Center for Cybersecurity and Communications, and law enforcement agencies; and

"(III) remediate or mitigate the risk posed by attacks and exploitations in a timely fashion in order to prevent future vulnerabilities and incidents; and

"(iv) identify deficiencies of agency information security policies, procedures, and controls on the agency information infrastructure.

"(b) CONDUCT AN OPERATIONAL EVALUATION.—

"(1) IN GENERAL.—Except as provided under paragraph (2), and in consultation with the Chief In-

formation Officer and senior officials responsible for the affected systems, the Chief Information Security Officer of each agency shall not less than annually—

"(A) conduct an operational evaluation of the agency information infrastructure for vulnerabilities, attacks, and exploitations of the agency information infrastructure;

"(B) evaluate the ability of the agency to monitor, detect, correlate, analyze, report, and respond to incidents; and

"(C) report to the head of the agency, the Director of the National Center for Cybersecurity and Communications, the Chief Information Officer, and the Inspector General for the agency the findings of the operational evaluation.

"(2) SATISFACTION OF REQUIREMENTS BY OTHER EVALUATION.—Unless otherwise specified by the Director of the National Center for Cybersecurity and Communications, if the Director of the National Center for Cybersecurity and Communications conducts an operational evaluation of the agency information infrastructure under section 245(b)(2)(A) of the Homeland Security Act of 2002, the Chief Information Security Officer may deem the requirements of paragraph (1) satisfied for the year in which the

operational evaluation described under this paragraph is conducted.

"(c) CORRECTIVE MEASURES MITIGATION AND REMEDIATION PLANS.—

"(1) IN GENERAL.—In consultation with the Director of the National Center for Cybersecurity and Communications and the Chief Information Officer, Chief Information Security Officers shall remediate or mitigate vulnerabilities in accordance with this subsection.

"(2) RISK-BASED PLAN.—After an operational evaluation is conducted under this section or under section 245(b) of the Homeland Security Act of 2002, the agency shall submit to the Director of the National Center for Cybersecurity and Communications in a timely fashion a risk-based plan for addressing recommendations and mitigating and remediating vulnerabilities identified as a result of such operational evaluation, including a timeline and budget for implementing such plan.

"(3) APPROVAL OR DISAPPROVAL.—Not later than 15 days after receiving a plan submitted under paragraph (2), the Director of the National Center for Cybersecurity and Communications shall—

"(A) approve or disprove the agency plan; and

"(B) comment on the adequacy and effectiveness of the plan.

"(4) ISOLATION FROM INFRASTRUCTURE.—

"(A) IN GENERAL.—The Director of the National Center for Cybersecurity and Communications may, consistent with the contingency or continuity of operation plans applicable to such agency information infrastructure, order the isolation of any component of the Federal information infrastructure from any other Federal information infrastructure, if—

"(i) an agency does not implement measures in a risk-based plan approved under this subsection; and

"(ii) the failure to comply presents a significant danger to the Federal information infrastructure.

"(B) DURATION.—An isolation under subparagraph (A) shall remain in effect until—

"(i) the Director of the National Center for Cybersecurity and Communications determines that corrective measures have been implemented; or

"(ii) an updated risk-based plan is approved by the Director of the National Center for Cybersecurity and Communications and implemented by the agency.

"(d) OPERATIONAL GUIDANCE.—The Director of the National Center for Cybersecurity and Communications shall—

"(1) not later than 180 days after the date of enactment of the Protecting Cyberspace as a National Asset Act of 2010, develop operational guidance for operational evaluations as required under this section that are risk-based and cost effective; and

"(2) periodically evaluate and ensure information is available on an automated and continuous basis through the system required under section 3552(a)(3)(D) to Congress on—

"(A) the adequacy and effectiveness of the operational evaluations conducted under this section or section 245(b) of the Homeland Security Act of 2002; and

"(B) possible executive and legislative actions for cost-effectively managing the risks to the Federal information infrastructure.

"§ 3555. Federal Information Security Taskforce

"(a) ESTABLISHMENT.—There is established in the executive branch a Federal Information Security Taskforce.

"(b) MEMBERSHIP.—The members of the Federal Information Security Taskforce shall be full-time senior Government employees and shall be as follows:

"(1) The Director of the National Center for Cybersecurity and Communications.

"(2) The Administrator of the Office of Electronic Government of the Office of Management and Budget.

"(3) The Chief Information Security Officer of each agency described under section 901(b) of title 31.

"(4) The Chief Information Security Officer of the Department of the Army, the Department of the Navy, and the Department of the Air Force.

"(5) A representative from the Office of Cyberspace Policy.

"(6) A representative from the Office of the Director of National Intelligence.

"(7) A representative from the United States Cyber Command.

"(8) A representative from the National Security Agency.

"(9) A representative from the United States Computer Emergency Readiness Team.

"(10) A representative from the Intelligence Community Incident Response Center.

"(11) A representative from the Committee on National Security Systems.

"(12) A representative from the National Institute for Standards and Technology.

"(13) A representative from the Council of Inspectors General on Integrity and Efficiency.

"(14) A representative from State and local government.

"(15) Any other officer or employee of the United States designated by the chairperson.

"(c) CHAIRPERSON AND VICE-CHAIRPERSON.—

"(1) CHAIRPERSON.—The Director of the National Center for Cybersecurity and Communications shall act as chairperson of the Federal Information Security Taskforce.

"(2) VICE-CHAIRPERSON.—The vice chairperson of the Federal Information Security Taskforce shall—

"(A) be selected by the Federal Information Security Taskforce from among its members;

"(B) serve a 1-year term and may serve multiple terms; and

"(C) serve as a liaison to the Chief Information Officer, Council of the Inspectors General on

Integrity and Efficiency, Committee on National Security Systems, and other councils or committees as appointed by the chairperson.

"(d) FUNCTIONS.—The Federal Information Security Taskforce shall—

"(1) be the principal interagency forum for collaboration regarding best practices and recommendations for agency information security and the security of the Federal information infrastructure;

"(2) assist in the development of and annually evaluate guidance to fulfill the requirements under sections 3554 and 3556;

"(3) share experiences and innovative approaches relating to threats against the Federal information infrastructure, information sharing and information security best practices, penetration testing regimes, and incident response, mitigation, and remediation;

"(4) promote the development and use of standard performance indicators and measures for agency information security that—

"(A) are outcome-based;

"(B) focus on risk management;

"(C) align with the business and program goals of the agency;

"(D) measure improvements in the agency security posture over time; and

"(E) reduce burdensome and inefficient performance indicators and measures;

"(5) recommend to the Office of Personnel Management the necessary qualifications to be established for Chief Information Security Officers to be capable of administering the functions described under this subchapter including education, training, and experience;

"(6) enhance information system processes by establishing a prioritized baseline of information security measures and controls that can be continuously monitored through automated mechanisms; and

"(7) evaluate the effectiveness and efficiency of any reporting and compliance requirements that are required by law related to the information security of Federal information infrastructure; and

"(8) submit proposed enhancements developed under paragraphs (1) through (7) to the Director of the National Center for Cybersecurity and Communications.

"(e) TERMINATION.—

"(1) IN GENERAL.—Except as provided under paragraph (2), the Federal Information Security

Taskforce shall terminate 4 years after the date of enactment of the Protecting Cyberspace as a National Asset Act of 2010.

"(2) EXTENSION.—The President may—

"(A) extend the Federal Information Security Taskforce by executive order; and

"(B) make more than 1 extension under this paragraph for any period as the President may determine.

"§ 3556. Independent Assessments

"(a) IN GENERAL.—

"(1) INSPECTORS GENERAL ASSESSMENTS.—Not less than every 2 years, each agency with an Inspector General appointed under the Inspector General Act of 1978 (5 U.S.C. App.) or any other law shall assess the adequacy and effectiveness of the information security program developed under section 3553(b) and (c), and evaluations conducted under section 3554.

"(2) INDEPENDENT ASSESSMENTS.—For each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the assessment.

"(b) STANDARDS.—The assessments required under subsection (a) shall be performed in accordance with stand-

ards developed by the Government Accountability Office, in collaboration with the Council of Inspectors General on Integrity and Efficiency and with assistance from the Federal Information Security Taskforce.

"(c) EXISTING ASSESSMENTS.—The assessments required under this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

"(d) REPORTING OF INFORMATION.—

"(1) INSPECTORS GENERAL REPORTING.—Each Inspector General shall ensure information obtained as a result of the assessment required under this section, or any other relevant information, is—

"(A) provided to the head of the agency, the agency Chief Information Security Officer, and the agency Chief Information Officer; and

"(B) available through the system required under section 3552(a)(3)(D) to Congress and the Director of the National Center for Cybersecurity and Communications.

"(2) HEADS OF AGENCIES REPORTING.—If an assessment described under subsection (a)(2) is performed, the head of the agency shall comply with the requirements of paragraph (1)(A) and (B).

"§ 3557. Protection of Information

"In complying with this subchapter, agencies, evaluators, and Inspectors General shall take appropriate actions to ensure the protection of information which, if disclosed, may adversely affect information security. Protections under this chapter shall be commensurate with the risk and comply with all applicable laws and regulations.

"§ 3558. Department of Defense and Central Intelligence Agency systems

"(a) IN GENERAL.—The authorities of the Director of the National Center for Cybersecurity and Communications under this subchapter shall be delegated to—

"(1) the Secretary of Defense in the case of systems described under subsection (b); and

"(2) the Director of the Central Intelligence Agency in the case of systems described under subsection (c).

"(b) DEPARTMENT OF DEFENSE SYSTEMS.—The systems described under this subsection are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

"(c) CENTRAL INTELLIGENCE AGENCY SYSTEMS.—The systems described under this subsection are systems that are operated by the Central Intelligence Agency, a contractor of the Central Intelligence Agency, or another entity on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Central Intelligence Agency.".

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TABLE OF SECTIONS.—The table of sections for chapter 35 of title 44, United States Code, is amended by striking the matter relating to subchapters II and III and inserting the following:

"SUBCHAPTER II—INFORMATION SECURITY

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(c)(1)(A)) is amended by striking "section 3532(3)" and inserting "section 3551(b)".

(B) Section 2222(j)(6) of title 10, United States Code, is amended by striking "section 3542(b)(2))" and inserting "section 3551(b)".

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking "section 3542(b)(2))" and inserting "section 3551(b)".

(D) Section 2315 of title 10, United States Code, is amended by striking "section 3542(b)(2))" and inserting "section 3551(b)".

(E) Section 20(a)(2) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by striking "section 3532(b)(2)" and inserting "section 3551(b)".

(F) Section 21(b)(2) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)(2)) is amended by striking "Institute and" and inserting "Institute, the Director of the National Center on Cybersecurity and Communications, and".

(G) Section 21(b)(3) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)(3)) is amended by inserting "the Director of the National Center on Cybersecurity and Communications," after "the Director of the National Security Agency,".

(H) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking "section 3534(b)" and inserting "section 3553(b)".

(3) HOMELAND SECURITY ACT OF 2002.—

(A) TITLE X.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by striking title X.

(B) TABLE OF CONTENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by striking the matter relating to title X.

(d) REPEAL OF OTHER STANDARDS.—

(1) IN GENERAL.—Section 11331 of title 40, United States Code, is repealed.

(2) TECHNICAL AND CONFORMING AMENDMENTS.—

(A) Section 20(c)(3) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(c)(3)) is amended by striking "under section 11331 of title 40, United States Code".

(B) Section 20(d)(1) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(d)(1)) is amended by striking "the Director of the Office of Management and Budget for

promulgation under section 11331 of title 40, United States Code" and inserting "the Secretary of Commerce for promulgation".

(C) Section 11302(d) of title 40, United States Code, is amended by striking "under section 11331 of this title and".

(D) Section 1874A (e)(2)(A)(ii) of the Social Security Act (42 U.S.C.1395kk-1 (e)(2)(A)(ii)) is amended by striking "section 11331 of title 40, United States Code" and inserting "section 3552 of title 44, United States Code".

(E) Section 3504(g)(2) of title 44, United States Code, is amended by striking "section 11331 of title 40" and inserting "section 3552 of title 44".

(F) Section 3504(h)(1) of title 44, United States Code, is amended by inserting ", the Director of the National Center for Cybersecurity and Communications," after "the National Institute of Standards and Technology".

(G) Section 3504(h)(1)(B) of title 44, United States Code, is amended by striking "under section 11331 of title 40" and inserting "section 3552 of title 44".

(H) Section 3518(d) of title 44, United States Code, is amended by striking "sections 11331 and 11332" and inserting "section 11332".

(I) Section 3602(f)(8) of title 44, United States Code, is amended by striking "under section 11331 of title 40.

(J) Section 3603(f)(5) of title 44, United States Code, is amended by striking "and promulgated under section 11331 of title 40,".

TITLE IV—RECRUITMENT AND PROFESSIONAL DEVELOPMENT

SEC. 401. DEFINITIONS.

In this title:

(1) CYBERSECURITY MISSION.—The term "cybersecurity mission" means the activities of the Federal Government that encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as such activities relate to the security and stability of cyberspace.

(2) FEDERAL AGENCY'S CYBERSECURITY MISSION.—The term "Federal agency's cybersecurity mission" means, with respect to any Federal agency, the portion of the cybersecurity mission that is the responsibility of the Federal agency.

SEC. 402. ASSESSMENT OF CYBERSECURITY WORKFORCE.

(a) IN GENERAL.—The Director of the Office of Personnel Management and the Director shall assess the readiness and capacity of the Federal workforce to meet the needs of the cybersecurity mission of the Federal Government.

(b) STRATEGY.—

(1) IN GENERAL.—The Director of the Office of Personnel Management, in consultation with the Director and the Director of the Office of Management and Budget, shall develop a comprehensive workforce strategy that enhances the readiness, capacity, training, and recruitment and retention of Federal cybersecurity personnel.

(2) CONTENTS.—The strategy developed under paragraph (1) shall include—

(A) a 5-year plan on recruitment of personnel for the Federal workforce; and

(B) 10-year and 20-year projections of workforce needs.

(3) DATES FOR COMPLETION.—The strategy under this subsection shall be—

(A) completed not later than 180 days after the date of enactment of this Act; and

(B) updated as needed.

SEC. 403. STRATEGIC CYBERSECURITY WORKFORCE PLANNING.

(a) FEDERAL AGENCY DEVELOPMENT OF STRATEGIC CYBERSECURITY WORKFORCE PLANS.—Not later than 180 days after the date of enactment of this Act and in every subsequent year, and subject to subsection (c)(2), the head of each Federal agency shall develop a strategic cybersecurity workforce plan as part of the Federal agency performance plan required under section 1115 of title 31, United States Code.

(b) BASIS AND GUIDANCE FOR PLANS.—Each Federal agency shall develop a plan prepared under subsection (a) on the basis of the assessment developed under section 402 and any subsequent guidance issued by the Director of the Office of Personnel Management, in consultation with the Director and the Director of the Office of Management and Budget.

(c) CONTENTS OF THE PLAN.—

(1) IN GENERAL.—Subject to paragraph (2), each plan prepared under subsection (a) shall include—

(A) a description of the Federal agency's cybersecurity mission;

(B) a description and analysis, relating to the specialized workforce needed by the Federal agency to fulfill the Federal agency's cybersecurity mission, including—

(i) the workforce needs of the Federal agency on the date of the report, and 10-year and 20-year projections of workforce needs;

(ii) hiring projections to meet workforce needs, including, for at least a 2-year period, specific occupation and grade levels;

(iii) long-term and short-term strategic goals to address critical skills deficiencies, including analysis of the numbers of and reasons for attrition of employees;

(iv) recruitment strategies, including the use of student internships, part-time employment, student loan reimbursement, and telework, to attract highly qualified

candidates from diverse backgrounds and geographic locations;

(v) an assessment of the sources and availability of individuals with needed expertise;

(vi) ways to streamline the hiring process;

(vii) the barriers to recruiting and hiring individuals qualified in cybersecurity and recommendations to overcome the barriers; and

(viii) a training and development plan, consistent with the curriculum developed under section 406, to enhance and improve the knowledge of employees.

(2) FEDERAL AGENCIES WITH SMALL SPECIALIZED WORKFORCE.—In accordance with guidance issued under subsection (b), a Federal agency that needs only a small specialized workforce to fulfill the Federal agency's cybersecurity mission may, in lieu of developing a separate strategic cybersecurity workforce plan, present the workforce plan component referred to in paragraph (1)(A) and those components referred to in paragraph (1)(B) that are relevant and appropriate to the circumstances of the agency as

part of the Federal agency performance plan required under section 1115 of title 31, United States Code.

SEC. 404. CYBERSECURITY OCCUPATION CLASSIFICATIONS.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director of the Office of Personnel Management, in coordination with the Director, shall develop and issue comprehensive occupation classifications for Federal employees engaged in cybersecurity missions.

(b) APPLICABILITY OF CLASSIFICATIONS.—The Director of the Office of Personnel Management shall ensure that the comprehensive occupation classifications issued under subsection (a) may be used throughout the Federal Government.

SEC. 405. MEASURES OF CYBERSECURITY HIRING EFFECTIVENESS.

(a) IN GENERAL.—The head of each Federal agency shall measure, and collect information on, indicators of the effectiveness of the recruitment and hiring by the Federal agency of a workforce needed to fulfill the Federal agency's cybersecurity mission.

(b) TYPES OF INFORMATION.—The indicators of effectiveness measured and subject to collection of information under subsection (a) shall include indicators with respect to the following:

(1) RECRUITING AND HIRING.—In relation to recruiting and hiring by the Federal agency—

(A) the ability to reach and recruit well-qualified individuals from diverse talent pools;

(B) the use and impact of special hiring authorities and flexibilities to recruit the most qualified applicants, including the use of student internship and scholarship programs for permanent hires;

(C) the use and impact of special hiring authorities and flexibilities to recruit diverse candidates, including criteria such as the veteran status, race, ethnicity, gender, disability, or national origin of the candidates; and

(D) the educational level, and source of applicants.

(2) SUPERVISORS.—In relation to the supervisors of the positions being filled—

(A) satisfaction with the quality of the applicants interviewed and hired;

(B) satisfaction with the match between the skills of the individuals and the needs of the Federal agency;

(C) satisfaction of the supervisors with the hiring process and hiring outcomes;

(D) whether any mission-critical deficiencies were addressed by the individuals and the connection between the deficiencies and the performance of the Federal agency; and

(E) the satisfaction of the supervisors with the period of time elapsed to fill the positions.

(3) APPLICANTS.—The satisfaction of applicants with the hiring process, including clarity of job announcements, any reasons for withdrawal of an application, the user-friendliness of the application process, communication regarding status of applications, and the timeliness of offers of employment.

(4) HIRED INDIVIDUALS.—In relation to the individuals hired—

(A) satisfaction with the hiring process;

(B) satisfaction with the process of starting employment in the position for which the individual was hired;

(C) attrition; and

(D) the results of exit interviews.

(c) REPORTS.—

(1) IN GENERAL.—The head of each Federal agency shall submit the information collected under this section to the Director of the Office of Personnel

Management on an annual basis and in accordance with the regulations issued under subsection (d).

(2) AVAILABILITY OF RECRUITING AND HIRING INFORMATION.—

(A) IN GENERAL.—The Director of the Office of Personnel Management shall prepare an annual report containing the information received under paragraph (1) in a consistent format to allow for a comparison of hiring effectiveness and experience across demographic groups and Federal agencies.

(B) SUBMISSION.—The Director of the Office of Personnel Management shall—

(i) not later than 90 days after the receipt of all information required to be submitted under paragraph (1), make the report prepared under subparagraph (A) publicly available, including on the website of the Office of Personnel Management; and

(ii) before the date on which the report prepared under subparagraph (A) is made publicly available, submit the report to Congress.

(d) REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Personnel Management shall issue regulations establishing the methodology, timing, and reporting of the data required to be submitted under this section.

(2) SCOPE AND DETAIL OF REQUIRED INFORMATION.—The regulations under paragraph (1) shall delimit the scope and detail of the information that a Federal agency is required to collect and submit under this section, taking account of the size and complexity of the workforce that the Federal agency needs to fulfill the Federal agency's cybersecurity mission.

SEC. 406. TRAINING AND EDUCATION.

(a) TRAINING.—

(1) FEDERAL GOVERNMENT EMPLOYEES AND FEDERAL CONTRACTORS.—The Director of the Office of Personnel Management, in conjunction with the Director of the National Center for Cybersecurity and Communications, the Director of National Intelligence, the Secretary of Defense, and the Chief Information Officers Council established under section 3603 of title 44, United States Code, shall establish a cybersecurity awareness and education curriculum

that shall be required for all Federal employees and contractors engaged in the design, development, or operation of agency information infrastructure, as defined under section 3551 of title 44, United States Code.

(2) CONTENTS.—The curriculum established under paragraph (1) may include—

(A) role-based security awareness training;

(B) recommended cybersecurity practices;

(C) cybersecurity recommendations for traveling abroad;

(D) unclassified counterintelligence information;

(E) information regarding industrial espionage;

(F) information regarding malicious activity online;

(G) information regarding cybersecurity and law enforcement;

(H) identity management information;

(I) information regarding supply chain security;

(J) information security risks associated with the activities of Federal employees; and

(K) the responsibilities of Federal employees in complying with policies and procedures designed to reduce information security risks identified under subparagraph (J).

(3) FEDERAL CYBERSECURITY PROFESSIONALS.—The Director of the Office of Personnel Management in conjunction with the Director of the National Center for Cybersecurity and Communications, the Director of National Intelligence, the Secretary of Defense, the Director of the Office of Management and Budget, and, as appropriate, colleges, universities, and nonprofit organizations with cybersecurity training expertise, shall develop a program, to provide training to improve and enhance the skills and capabilities of Federal employees engaged in the cybersecurity mission, including training specific to the acquisition workforce.

(4) HEADS OF FEDERAL AGENCIES.—Not later than 30 days after the date on which an individual is appointed to a position at level I or II of the Executive Schedule, the Director of the National Center for Cybersecurity and Communications and the Director of National Intelligence, or their designees, shall provide that individual with a cybersecurity threat briefing.

(5) CERTIFICATION.—The head of each Federal agency shall include in the annual report required under section 3553(c) of title 44, United States Code, a certification regarding whether all officers, employees, and contractors of the Federal agency have completed the training required under this subsection.

(b) EDUCATION.—

(1) FEDERAL EMPLOYEES.—The Director of the Office of Personnel Management, in coordination with the Secretary of Education, the Director of the National Science Foundation, and the Director, shall develop and implement a strategy to provide Federal employees who work in cybersecurity missions with the opportunity to obtain additional education.

(2) K THROUGH 12.—The Secretary of Education, in coordination with the Director of the National Center for Cybersecurity and Communications and State and local governments, shall develop curriculum standards, guidelines, and recommended courses to address cyber safety, cybersecurity, and cyber ethics for students in kindergarten through grade 12.

(3) UNDERGRADUATE, GRADUATE, VOCATIONAL, AND TECHNICAL INSTITUTIONS.—

(A) SECRETARY OF EDUCATION.—The Secretary of Education, in coordination with the Director of the National Center for Cybersecurity and Communications, shall—

(i) develop curriculum standards and guidelines to address cyber safety, cybersecurity, and cyber ethics for all students enrolled in undergraduate, graduate, vocational, and technical institutions in the United States; and

(ii) analyze and develop recommended courses for students interested in pursuing careers in information technology, communications, computer science, engineering, math, and science, as those subjects relate to cybersecurity.

(B) OFFICE OF PERSONNEL MANAGEMENT.—The Director of the Office of Personnel Management, in coordination with the Director, shall develop strategies and programs—

(i) to recruit students from undergraduate, graduate, vocational, and technical institutions in the United States to serve as Federal employees engaged in cyber missions; and

(ii) that provide internship and part-time work opportunities with the Federal Government for students at the undergraduate, graduate, vocational, and technical institutions in the United States.

(c) CYBER TALENT COMPETITIONS AND CHALLENGES.—

(1) IN GENERAL.—The Director of the National Center for Cybersecurity and Communications shall establish a program to ensure the effective operation of national and statewide competitions and challenges that seek to identify, develop, and recruit talented individuals to work in Federal agencies, State and local government agencies, and the private sector to perform duties relating to the security of the Federal information infrastructure or the national information infrastructure.

(2) GROUPS AND INDIVIDUALS.—The program under this subsection shall include—

(A) high school students;

(B) undergraduate students;

(C) graduate students;

(D) academic and research institutions;

(E) veterans; and

(F) other groups or individuals as the Director may determine.

(3) SUPPORT OF OTHER COMPETITIONS AND CHALLENGES.—The program under this subsection may support other competitions and challenges not established under this subsection through affiliation and cooperative agreements with—

(A) Federal agencies;

(B) regional, State, or community school programs supporting the development of cyber professionals; or

(C) other private sector organizations.

(4) AREAS OF TALENT.—The program under this subsection shall seek to identify, develop, and recruit exceptional talent relating to—

(A) ethical hacking;

(B) penetration testing;

(C) vulnerability Assessment;

(D) continuity of system operations;

(E) cyber forensics; and

(F) offensive and defensive cyber operations.

SEC. 407. CYBERSECURITY INCENTIVES.

(a) AWARDS.—In making cash awards under chapter 45 of title 5, United States Code, the President or the head of a Federal agency, in consultation with the Director, shall

consider the success of an employee in fulfilling the objectives of the National Strategy, in a manner consistent with any policies, guidelines, procedures, instructions, or standards established by the President.

(b) OTHER INCENTIVES.—The head of each Federal agency shall adopt best practices, developed by the Director of the National Center for Cybersecurity and Communications and the Office of Management and Budget, regarding effective ways to educate and motivate employees of the Federal Government to demonstrate leadership in cybersecurity, including—

(1) promotions and other nonmonetary awards; and

(2) publicizing information sharing accomplishments by individual employees and, if appropriate, the tangible benefits that resulted.

SEC. 408. RECRUITMENT AND RETENTION PROGRAM FOR THE NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.

(a) DEFINITIONS.—In this section:

(1) CENTER.—The term "Center" means the National Center for Cybersecurity and Communications.

(2) DEPARTMENT.—The term "Department" means the Department of Homeland Security.

(3) DIRECTOR.—The term "Director" means the Director of the Center.

(4) ENTRY LEVEL POSITION.—The term "entry level position" means a position that—

(A) is established by the Director in the Center; and

(B) is classified at GS–7, GS–8, or GS–9 of the General Schedule.

(5) SECRETARY.—The term "Secretary" means the Secretary of Homeland Security.

(6) SENIOR POSITION.—The term "senior position" means a position that—

(A) is established by the Director in the Center; and

(B) is not established under section 5108 of title 5, United States Code, but is similar in duties and responsibilities for positions established under that section.

(b) RECRUITMENT AND RETENTION PROGRAM.—

(1) ESTABLISHMENT.—The Director may establish a program to assist in the recruitment and retention of highly skilled personnel to carry out the functions of the Center.

(2) CONSULTATION AND CONSIDERATIONS.—In establishing a program under this section, the Director shall—

(A) consult with the Secretary; and

(B) consider—

(i) national and local employment trends;

(ii) the availability and quality of candidates;

(iii) any specialized education or certifications required for positions;

(iv) whether there is a shortage of certain skills; and

(v) such other factors as the Director determines appropriate.

(c) HIRING AND SPECIAL PAY AUTHORITIES.—

(1) DIRECT HIRE AUTHORITY.—Without regard to the civil service laws (other than sections 3303 and 3328 of title 5, United States Code), the Director may appoint not more than 500 employees under this subsection to carry out the functions of the Center.

(2) RATES OF PAY.—

(A) ENTRY LEVEL POSITIONS.—The Director may fix the pay of the employees appointed to entry level positions under this subsection

without regard to chapter 51 and subchapter III of chapter 53 of title 5, United States Code, relating to classification of positions and General Schedule pay rates, except that the rate of pay for any such employee may not exceed the maximum rate of basic pay payable for a position at GS–10 of the General Schedule while that employee is in an entry level position.

(B) SENIOR POSITIONS.—

(i) IN GENERAL.—The Director may fix the pay of the employees appointed to senior positions under this subsection without regard to chapter 51 and subchapter III of chapter 53 of title 5, United States Code, relating to classification of positions and General Schedule pay rates, except that the rate of pay for any such employee may not exceed the maximum rate of basic pay payable under section 5376 of title 5, United States Code.

(ii) HIGHER MAXIMUM RATES.—

(I) IN GENERAL.—Notwithstanding the limitation on rates of pay under clause (i)—

(aa) not more than 20 employees, identified by the Director, may be paid at a rate of pay not to exceed the maximum rate of basic pay payable for a position at level I of the Executive Schedule under section 5312 of title 5, United States Code; and

(bb) not more than 5 employees, identified by the Director with the approval of the Secretary, may be paid at a rate of pay not to exceed the maximum rate of basic pay payable for the Vice President under section 104 of title 3, United States Code.

(II) NONDELEGATION OF AUTHORITY.—The Secretary or the Director may not delegate any authority under this clause.

(d) CONVERSION TO COMPETITIVE SERVICE.—

(1) DEFINITION.—In this subsection, the term "qualified employee" means any individual appointed to an excepted service position in the Department who performs functions relating to the security

of the Federal information infrastructure or national information infrastructure.

(2) COMPETITIVE CIVIL SERVICE STATUS.—In consultation with the Director, the Secretary may grant competitive civil service status to a qualified employee if that employee is —

(A) employed in the Center; or

(B) transferring to the Center.

(e) RETENTION BONUSES.—

(1) AUTHORITY.—Notwithstanding section 5754 of title 5, United States Code, the Director may—

(A) pay a retention bonus under that section to any individual appointed under this subsection, if the Director determines that, in the absence of a retention bonus, there is a high risk that the individual would likely leave employment with the Department; and

(B) exercise the authorities of the Office of Personnel Management and the head of an agency under that section with respect to retention bonuses paid under this subsection.

(2) LIMITATIONS ON AMOUNT OF ANNUAL BONUSES.—

(A) DEFINITIONS.—In this paragraph:

(i) MAXIMUM TOTAL PAY.—The term "maximum total pay" means—

(I) in the case of an employee described under subsection(c)(2)(B)(i), the total amount of pay paid in a calendar year at the maximum rate of basic pay payable for a position at level I of the Executive Schedule under section 5312 of title 5, United States Code;

(II) in the case of an employee described under subsection(c)(2)(B)(ii)(I)(aa), the total amount of pay paid in a calendar year at the maximum rate of basic pay payable for a position at level I of the Executive Schedule under section 5312 of title 5, United States Code; and

(III) in the case of an employee described under subsection(c)(2)(B)(ii)(I)(bb), the total amount of pay paid in a calendar year at the maximum rate of basic pay payable for the Vice President under

section 104 of title 3, United States Code.

(ii) TOTAL COMPENSATION.—The term "total compensation" means—

(I) the amount of pay paid to an employee in any calendar year; and

(II) the amount of all retention bonuses paid to an employee in any calendar year.

(B) LIMITATION.—The Director may not pay a retention bonus under this subsection to an employee that would result in the total compensation of that employee exceeding maximum total pay.

(f) TERMINATION OF AUTHORITY.—The authority to make appointments and pay retention bonuses under this section shall terminate 3 years after the date of enactment of this Act.

(g) REPORTS.—

(1) PLAN FOR EXECUTION OF AUTHORITIES.—Not later than 120 days of enactment of this Act, the Director shall submit a report to the appropriate committees of Congress with a plan for the execution of the authorities provided under this section.

(2) ANNUAL REPORT.—Not later than 6 months after the date of enactment of this Act, and every year thereafter, the Director shall submit to the appropriate committees of Congress a detailed report that—

(A) discusses how the actions taken during the period of the report are fulfilling the critical hiring needs of the Center;

(B) assesses metrics relating to individuals hired under the authority of this section, including—

(i) the numbers of individuals hired;

(ii) the turnover in relevant positions;

(iii) with respect to each individual hired—

(I) the position for which hired;

(II) the salary paid;

(III) any retention bonus paid and the amount of the bonus;

(IV) the geographic location from which hired;

(V) the immediate past salary; and

(VI) whether the individual was a noncareer appointee in the Senior Executive Service or an appointee to a

position of a confidential or policy-determining character under schedule C of subpart C of part 213 of title 5 of the Code of Federal Regulations before the hiring; and

(iv) whether public notice for recruitment was made, and if so—

(I) the total number of qualified applicants;

(II) the number of veteran preference eligible candidates who applied;

(III) the time from posting to job offer; and

(IV) statistics on diversity, including age, disability, race, gender, and national origin, of individuals hired under the authority of this section to the extent such statistics are available; and

(C) includes rates of pay set in accordance with subsection (c).

TITLE V—OTHER PROVISIONS

SEC. 501. CYBERSECURITY RESEARCH AND DEVELOPMENT.

Subtitle D of title II of the Homeland Security Act of 2002 (6 U.S.C. 161 et seq.) is amended by adding at the end the following:

"SEC. 238. CYBERSECURITY RESEARCH AND DEVELOPMENT.

"(a) ESTABLISHMENT OF RESEARCH AND DEVELOPMENT PROGRAM.—The Under Secretary for Science and Technology, in coordination with the Director of the National Center for Cybersecurity and Communications, shall carry out a research and development program for the purpose of improving the security of information infrastructure.

"(b) ELIGIBLE PROJECTS.—The research and development program carried out under subsection (a) may include projects to—

"(1) advance the development and accelerate the deployment of more secure versions of fundamental Internet protocols and architectures, including for the secure domain name addressing system and routing security;

"(2) improve and create technologies for detecting and analyzing attacks or intrusions, including analysis of malicious software;

"(3) improve and create mitigation and recovery methodologies, including techniques for containment of attacks and development of resilient networks and systems;

"(4) develop and support infrastructure and tools to support cybersecurity research and development efforts, including modeling, testbeds, and data sets for assessment of new cybersecurity technologies;

"(5) assist the development and support of technologies to reduce vulnerabilities in process control systems;

"(6) understand human behavioral factors that can affect cybersecurity technology and practices;

"(7) test, evaluate, and facilitate, with appropriate protections for any proprietary information concerning the technologies, the transfer of technologies associated with the engineering of less vulnerable software and securing the information technology software development lifecycle;

"(8) assist the development of identity management and attribution technologies;

"(9) assist the development of technologies designed to increase the security and resiliency of telecommunications networks;

"(10) advance the protection of privacy and civil liberties in cybersecurity technology and practices; and

"(11) address other risks identified by the Director of the National Center for Cybersecurity and Communications.

"(c) COORDINATION WITH OTHER RESEARCH INITIATIVES.—The Under Secretary—

"(1) shall ensure that the research and development program carried out under subsection (a) is consistent with the national strategy to increase the security and resilience of cyberspace developed by the Director of Cyberspace Policy under section 101 of the Protecting Cyberspace as a National Asset Act of 2010, or any succeeding strategy;

"(2) shall, to the extent practicable, coordinate the research and development activities of the Department with other ongoing research and development security-related initiatives, including research being conducted by—

"(A) the National Institute of Standards and Technology;

"(B) the National Science Foundation;

"(C) the National Academy of Sciences;

"(D) other Federal agencies, as defined under section 241;

"(E) other Federal and private research laboratories, research entities, and universities and institutions of higher education, and relevant nonprofit organizations; and

"(F) international partners of the United States;

"(3) shall carry out any research and development project under subsection (a) through a reimbursable agreement with an appropriate Federal agency, as defined under section 241, if the Federal agency—

"(A) is sponsoring a research and development project in a similar area; or

"(B) has a unique facility or capability that would be useful in carrying out the project;

"(4) may make grants to, or enter into cooperative agreements, contracts, other transactions, or reimbursable agreements with, the entities described in paragraph (2); and

"(5) shall submit a report to the appropriate committees of Congress on a review of the cybersecurity activities, and the capacity, of the national laboratories and other research entities available to the Department to determine if the establishment of a na-

tional laboratory dedicated to cybersecurity research and development is necessary.

"(d) PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES.—

"(1) CONSULTATION.—In carrying out research and development projects under subsection (a), the Under Secretary shall consult with the Privacy Officer appointed under section 222 and the Officer for Civil Rights and Civil Liberties of the Department appointed under section 705.

"(2) PRIVACY IMPACT ASSESSMENTS.—In accordance with sections 222 and 705, the Privacy Officer shall conduct privacy impact assessments and the Officer for Civil Rights and Civil Liberties shall conduct reviews, as appropriate, for research and development projects carried out under subsection (a) that the Under Secretary determines could have an impact on privacy, civil rights, or civil liberties.

"SEC. 239. NATIONAL CYBERSECURITY ADVISORY COUNCIL.

"(a) ESTABLISHMENT.—Not later than 90 days after the date of enactment of this section, the Secretary shall establish an advisory committee under section 871 on private sector cybersecurity, to be known as the National Cybersecurity Advisory Council (in this section referred to as the 'Council').

"(b) RESPONSIBILITIES.—

"(1) IN GENERAL.—The Council shall advise the Director of the National Center for Cybersecurity and Communications on the implementation of the cybersecurity provisions affecting the private sector under this subtitle and subtitle E.

"(2) INCENTIVES AND REGULATIONS.—The Council shall advise the Director of the National Center for Cybersecurity and Communications and appropriate committees of Congress (as defined in section 241) and any other congressional committee with jurisdiction over the particular matter regarding how market incentives and regulations may be implemented to enhance the cybersecurity and economic security of the Nation.

"(c) MEMBERSHIP.—

"(1) IN GENERAL.—The members of the Council shall be appointed the Director of the National Center for Cybersecurity and Communications and shall, to the extent practicable, represent a geographic and substantive cross-section of owners and operators of critical infrastructure and others with expertise in cybersecurity, including, as appropriate—

"(A) representatives of covered critical infrastructure (as defined under section 241);

"(B) academic institutions with expertise in cybersecurity;

"(C) Federal, State, and local government agencies with expertise in cybersecurity;

"(D) a representative of the National Security Telecommunications Advisory Council, as established by Executive Order 12382 (47 Fed. Reg. 40531; relating to the establishment of the advisory council), as amended by Executive Order 13286 (68 Fed. Reg. 10619), as in effect on August 3, 2009, or any successor entity;

"(E) a representative of the Communications Sector Coordinating Council, or any successor entity;

"(F) a representative of the Information Technology Sector Coordinating Council, or any successor entity;

"(G) individuals, acting in their personal capacity, with demonstrated technical expertise in cybersecurity; and

"(H) such other individuals as the Director determines to be appropriate, including owners of small business concerns (as defined under section 3 of the Small Business Act (15 U.S.C. 632)).

"(2) TERM.—The members of the Council shall be appointed for 2 year terms and may be appointed to consecutive terms.

"(3) LEADERSHIP.—The Chairperson and Vice-Chairperson of the Council shall be selected by members of the Council from among the members of the Council and shall serve 2-year terms.

"(d) APPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Council.".

SEC. 502. PRIORITIZED CRITICAL INFORMATION INFRASTRUCTURE.

(a) IN GENERAL.—Section 210E(a)(2) of the Homeland Security Act of 2002 (6 U.S.C. 124l(a)(2)) is amended—

(1) by striking "In accordance" and inserting the following:

"(A) IN GENERAL.—In accordance"; and

(2) by adding at the end the following:

"(B) CONSIDERATIONS.—In establishing and maintaining a list under subparagraph (A), the Secretary, in coordination with the Director of the National Center for Cybersecurity and Communications, shall consider cyber risks and consequences by sector, including—

"(i) the factors listed in section 248(a)(2);

"(ii) interdependencies between components of covered critical infrastructure (as defined under section 241); and

"(iii) the potential for the destruction or disruption of the system or asset to cause—

"(I) a mass casualty event which includes an extraordinary number of fatalities;

"(II) severe economic consequences;

"(III) mass evacuations with a prolonged absence; or

"(IV) severe degradation of national security capabilities, including intelligence and defense functions.".

(b) COVERED CRITICAL INFRASTRUCTURE.—Title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) (as amended by section 201 of this Act) is further amended by adding at the end the following:

"SEC. 254. COVERED CRITICAL INFRASTRUCTURE.

"(a) IDENTIFICATION OF COVERED CRITICAL INFRASTRUCTURE.—

"(1) IN GENERAL.—Subject to paragraphs (2) and (3), the Secretary, in coordination with sector-specific agencies and in consultation with the National Cybersecurity Advisory Council and other appropriate representatives of State and local governments and the private sector, shall establish and maintain a list of systems or assets that constitute covered critical infrastructure for purposes of this subtitle.

"(2) REQUIREMENTS.—

"(A) IN GENERAL.—A system or asset may not be identified as covered critical infrastructure under this section unless such system or asset meets each of the requirements under subparagraph (B)(i), (ii), and (iii).

"(B) REQUIREMENTS.—The requirements referred to under subparagraph (A) are that—

"(i) the destruction or the disruption of the reliable operation of the system or asset would cause national or regional catastrophic effects identified under section 210E(a)(2)(B)(iii);

"(ii) the system or asset is on the prioritized critical infrastructure list estab-

lished by the Secretary under section 210E(a)(2); and

"(iii)(I) the system or asset is a component of the national information infrastructure; or

"(II) the national information infrastructure is essential to the reliable operation of the system or asset.

"(3) LIMITATION.—A system or asset may not be identified as covered critical infrastructure under this section based solely on activities protected by the first amendment to the United States Constitution.

"(b) NOTIFICATION.—

"(1) IDENTIFICATION OF SYSTEM OR ASSET.—If the Secretary identifies any system or asset as covered critical infrastructure under subsection (a), the Secretary shall promptly notify the owner or operator of that system or asset of that identification.

"(2) SYSTEM OR ASSET NO LONGER COVERED CRITICAL INFRASTRUCTURE.—If the Secretary determines that any system or asset that was identified as covered critical infrastructure under subsection (a) no longer constitutes covered critical infrastructure, the Secretary shall promptly notify the owner or operator of that system or asset of that determination.

"(c) REDRESS.—

"(1) IN GENERAL.—Subject to paragraphs (2), (3), and (4), the Secretary shall develop a mechanism, consistent with subchapter II of chapter 5 of title 5, United States Code, for an owner or operator notified under subsection (b)(1) to appeal the identification of a system or asset as covered critical infrastructure under this section.

"(2) COMPLIANCE.—The owner or operator of a system or asset identified as covered critical infrastructure shall comply with any requirement of this subtitle relating to covered critical infrastructure until such time as the system or asset is no longer identified as covered critical infrastructure by the Secretary, based on—

"(A) an appeal under this subsection; or

"(B) a determination of the Secretary unrelated to an appeal.

"(3) ABUSE OF DISCRETION.—In order to prevail in any appeal under this subsection, the owner or operator of the system or asset identified as covered critical infrastructure shall be required to demonstrate an abuse of discretion by the Secretary.

"(4) FINAL APPEAL.—A final decision in any appeal under this subsection shall be a final agency action that shall not be subject to judicial review.

"(d) ADDITION OF SYSTEMS OR ASSETS.—

"(1) IN GENERAL.—The Secretary shall develop a process under which any owner or operator of a system or asset that may constitute covered critical infrastructure may—

"(A) request that such system or asset be identified by the Secretary as covered critical infrastructure under this section; and

"(B) submit material supporting such a request to the Director of the Center for consideration by the Secretary in carrying out this section.

"(2) FINAL DECISION.—A decision to identify any system or asset as covered critical infrastructure based on a request submitted under this subsection—

"(A) is committed to the sole, unreviewable discretion of the Secretary; and

"(B) shall not be subject to—

"(i) an appeal under subsection (c); or

"(ii) judicial review.".

SEC. 503. NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS ACQUISITION AUTHORITIES.

(a) IN GENERAL.—The National Center for Cybersecurity and Communications is authorized to use the authorities under subsections (c)(1) and (d)(1)(B) of section 2304 of title 10, United States Code, instead of the authorities under subsections (c)(1) and (d)(1)(B) of section 303 of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 253), subject to all other requirements of section 303 of the Federal Property and Administrative Services Act of 1949.

(b) GUIDELINES.—Not later than 90 days after the date of enactment of this Act, the chief procurement officer of the Department of Homeland Security shall issue guidelines for use of the authority under subsection (a).

(c) TERMINATION.—The National Center for Cybersecurity and Communications may not use the authority under subsection (a) on and after the date that is 3 years after the date of enactment of this Act.

(d) REPORTING.—

(1) IN GENERAL.—On a semiannual basis, the Director of the National Center for Cybersecurity and Communications shall submit a report on use of the authority granted by subsection (a) to—

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

(B) the Committee on Homeland Security of the House of Representatives.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include, at a minimum—

(A) the number of contract actions taken under the authority under subsection (a) during the period covered by the report; and

(B) for each contract action described in subparagraph (A)—

(i) the total dollar value of the contract action;

(ii) a summary of the market research conducted by the National Center for Cybersecurity and Communications, including a list of all offerors who were considered and those who actually submitted bids, in order to determine that use of the authority was appropriate; and

(iii) a copy of the justification and approval documents required by section 303(f) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 253(f)).

(3) CLASSIFIED ANNEX.—A report submitted under this subsection shall be submitted in an unclassified form, but may include a classified annex, if necessary.

SEC. 504. EVALUATION OF THE EFFECTIVE IMPLEMENTATION OF OFFICE OF MANAGEMENT AND BUDGET INFORMATION SECURITY RELATED POLICIES AND DIRECTIVES.

(a) IN GENERAL.—The Administrator for Electronic Government and Information Technology, in coordination with the Chief Information Officers Council, the Federal Information Security Taskforce, and Council on Inspectors General on Integrity and Efficiency, shall evaluate agency adoption and effective implementation of appropriate information security related policies, memoranda, and directives issued by the Office of Management and Budget including—

(1) OMB Memorandum M–10–15, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, issued April 21, 2010;

(2) OMB Memorandum M–09–32, Update on the Trusted Internet Connections Initiative, issued September 17, 2009;

(3) OMB Memorandum M–09–02, Information Technology Management Structure and Governance Framework, issued October 21, 2008;

(4) OMB Memorandum M–08–23, Securing the Federal Government's Domain Name System Infrastructure, issued April 22, 2008;

(5) OMB Memorandum M–08–22, Guidance on the Federal Desktop Core Configuration (FDCC), issued August 11, 2008;

(6) OMB Memorandum M–07–16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, issued May 22, 2007;

(7) OMB Memorandum M–07–06, Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials, issued January 11, 2007;

(8) OMB Memorandum M–04–26, Personal Use Policies and "File Sharing" Technology, issued September 8, 2004; and

(9) OMB Memorandum M–03–22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, issued September 26, 2003.

(b) REPORT.—Not later than 1 year after the date of enactment of this Act, the Office of Management and Budget shall submit a report on the evaluation required under sub-

section (a) to the appropriate congressional committees which shall include—

(1) an examination of whether Federal agencies have effectively implemented information security policies;

(2) identification of and reasons why Federal agencies are not in compliance with information security policies;

(3) the extent to which contractors working on behalf of Federal agencies are in compliance and effectively implementing information security policies; and

(4) recommended legislative and executive branch actions.

SEC. 505. TECHNICAL AND CONFORMING AMENDMENTS.

(a) ELIMINATION OF ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) in section 103(a)(8) (6 U.S.C. 113(a)(8)), by striking ", cybersecurity,";

(2) in section 514 (6 U.S.C. 321c)—

(A) by striking subsection (b); and

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

(3) in section 1801(b) (6 U.S.C. 571(b)), by striking "shall report to the Assistant Secretary for Cybersecurity and Communications" and inserting "shall report to the Director of the National Center for Cybersecurity and Communications".

(b) CIO COUNCIL.—Section 3603(b) of title 44, United States Code, is amended—

(1) by redesignating paragraph (7) as paragraph (8); and

(2) by inserting after paragraph (6) the following:

"(7) The Director of the National Center for Cybersecurity and Communications.".

(c) REPEAL.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq) is amended—

(1) by striking section 223 (6 U.S.C. 143); and

(2) by redesignating sections 224 and 225 (6 U.S.C. 144 and 145) as sections 223 and 224, respectively.

(d) TECHNICAL CORRECTION.—Section 1802(a) of the Homeland Security Act of 2002 (6 U.S.C. 572(a)) is amended in the matter preceding paragraph (1) by striking "Department of".

(e) EXECUTIVE SCHEDULE POSITION.—Section 5313 of title 5, United States Code, is amended by adding at the end the following:

"Director of the National Center for Cybersecurity and Communications.".

(f) TABLE OF CONTENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by striking the items relating to sections 223, 224, and 225 and inserting the following:

"Sec. 223. NET guard.
"Sec. 224. Cyber Security Enhancements Act of 2002."; and

(2) by inserting after the item relating to section 237 the following:

"Sec. 238. Cybersecurity research and development.
"Sec. 239. National Cybersecurity Advisory Council.

"Subtitle E—Cybersecurity

"Sec. 241. Definitions.
"Sec. 242. National Center for Cybersecurity and Communications.
"Sec. 243. Physical and cyber infrastructure collaboration.
"Sec. 244. United States Computer Emergency Readiness Team.
"Sec. 245. Additional authorities of the Director of the National Center for Cybersecurity and Communications.
"Sec. 246. Information sharing.
"Sec. 247. Private sector assistance.
"Sec. 248. Cyber risks to covered critical infrastructure.
"Sec. 249. National cyber emergencies..
"Sec. 250. Enforcement.
"Sec. 251. Protection of information.
"Sec. 252. Sector-specific agencies.
"Sec. 253. Strategy for Federal cybersecurity supply chain management.
"Sec. 254. Covered critical infrastructure.".

Calendar No. 698

111TH CONGRESS
2D SESSION

S. 3480

[Report No. 111–368]

A BILL

To amend the Homeland Security Act of 2002 and other laws to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

DECEMBER 15, 2010

Reported with an amendment