AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 470

112TH CONGRESS
2D SESSION

S. 3414

To enhance the security and resiliency of the cyber and communications infrastructure of the United States.

IN THE SENATE OF THE UNITED STATES

JULY 19, 2012

Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEINSTEIN, and Mr. CARPER) introduced the following bill; which was read the first time

JULY 23, 2012

Read the second time and placed on the calendar

A BILL

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; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Cybersecurity Act of 2012'' or the ''CSA2012''.

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

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

TITLE I—PUBLIC-PRIVATE PARTNERSHIP TO PROTECT CRITICAL INFRASTRUCTURE

Sec. 101. National Cybersecurity Council.
Sec. 102. Inventory of critical infrastructure.
Sec. 103. Voluntary cybersecurity practices.
Sec. 104. Voluntary cybersecurity program for critical infrastructure.
Sec. 105. Rules of construction.
Sec. 106. Protection of information.
Sec. 107. Annual assessment of cybersecurity.
Sec. 108. International cooperation.
Sec. 109. Effect on other laws.
Sec. 110. Definitions.

TITLE II—FEDERAL INFORMATION SECURITY MANAGEMENT AND CONSOLIDATING RESOURCES

Sec. 201. FISMA Reform.
Sec. 202. Management of information technology.
Sec. 203. Savings provisions.
Sec. 204. Consolidation of existing departmental cyber resources and authorities.

TITLE III—RESEARCH AND DEVELOPMENT

Sec. 301. Federal cybersecurity research and development.
Sec. 302. Homeland security cybersecurity research and development.
Sec. 303. Research centers for cybersecurity.
Sec. 304. Centers of excellence.

TITLE IV—EDUCATION, WORKFORCE, AND AWARENESS

Sec. 401. Definitions.
Sec. 402. Education and awareness.
Sec. 403. National cybersecurity competition and challenge.
Sec. 404. Federal Cyber Scholarship-for-Service program.
Sec. 405. Assessment of cybersecurity Federal workforce.
Sec. 406. Federal cybersecurity occupation classifications.
Sec. 407. Training and education of Federal employees.
Sec. 408. National Center for Cybersecurity and Communications acquisition authorities.
Sec. 409. Reports on cyber incidents against Government networks.
Sec. 410. Reports on prosecution for cybercrime.
Sec. 411. Report on research relating to secure domain.
Sec. 412. Report on preparedness of Federal courts to promote cybersecurity.
Sec. 413. Report on impediments to public awareness.
Sec. 414. Report on protecting the electrical grid of the United States.
Sec. 415. Marketplace information.

TITLE V—FEDERAL ACQUISITION RISK MANAGEMENT STRATEGY

Sec. 501. Federal acquisition risk management strategy.
Sec. 502. Amendments to Clinger-Cohen provisions to enhance agency planning for information security needs.

TITLE VI—INTERNATIONAL COOPERATION

Sec. 601. Definitions.
Sec. 602. Findings.
Sec. 603. Sense of Congress.
Sec. 604. Coordination of international cyber issues within the United States Government.
Sec. 605. Consideration of cybercrime in foreign policy and foreign assistance programs.

TITLE VII—INFORMATION SHARING

Sec. 701. Affirmative authority to monitor and defend against cybersecurity threats.
Sec. 702. Voluntary disclosure of cybersecurity threat indicators among private entities.
Sec. 703. Cybersecurity exchanges.
Sec. 704. Voluntary disclosure of cybersecurity threat indicators to a cybersecurity exchange.
Sec. 705. Sharing of classified cybersecurity threat indicators.
Sec. 706. Limitation on liability and good faith defense for cybersecurity activities.
Sec. 707. Construction and federal preemption.
Sec. 708. Definitions.

SEC. 2. DEFINITIONS.

In this Act:

(1) CATEGORY OF CRITICAL CYBER INFRASTRUCTURE.—The term ''category of critical cyber infrastructure'' means a category identified by the Council as critical cyber infrastructure in accordance with the procedure established under section 102.

(2) COMMERCIAL INFORMATION TECHNOLOGY PRODUCT.—The term ''commercial information technology product'' means a commercial item that organizes or communicates information electronically.

(3) COMMERCIAL ITEM.—The term ''commercial item'' has the meaning given the term in section 103 of title 41, United States Code.

(4) COUNCIL.—The term ''Council'' means the National Cybersecurity Council established under section 101.

(5) CRITICAL CYBER INFRASTRUCTURE.—The term ''critical cyber infrastructure'' means critical infrastructure identified by the Council under section 102(b)(3)(A).

(6) 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)).

(7) CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL.—The term ''Critical Infrastructure Partnership Advisory Council'' means the Critical Infrastructure Partnership Advisory Council established by the Department under section 871 of the Homeland Security Act of 2002 (6 U.S.C. 451) to coordinate critical infrastructure protection activities within the Federal Government and with the private sector and State, local, territorial, and tribal governments.

(8) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(9) FEDERAL AGENCY.—The term ''Federal agency'' has the meaning given the term ''agency'' in section 3502 of title 44, United States Code.

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

(A) means information and information systems that are 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 and information systems that are owned, operated, controlled, or licensed solely for use by, or on behalf of, the Department of Defense, a military department, or an element of the intelligence community.

(11) INCIDENT.—The term ''incident'' has the meaning given that term in section 3552 of title 44, United States Code, as added by section 201 of this Act.

(12) 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, communications networks, and industrial or supervisory control systems and any associated hardware, software, or data.

(13) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ''Information Sharing and Analysis Organization'' has the meaning given that term in section 212 of the Homeland Security Act of 2002 (6 U.S.C. 131).

(14) INFORMATION SYSTEM.—The term ''information system'' has the meaning given that term in section 3502 of title 44, United States Code.

(15) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given that term in section 102 of the Higher Education Act of 1965 (20 U.S.C. 1002).

(16) 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)).

(17) MEMBER AGENCY.—The term ''member agency'' means a Federal agency from which a member of the Council is appointed.

(18) NATIONAL INFORMATION INFRASTRUCTURE.—The term ''national information infrastructure'' means information and information systems—

(A) that are owned, operated, or controlled, in whole or in part, within or from the United States; and

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

(19) NATIONAL LABORATORY.—The term ''national laboratory'' has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(20) NATIONAL SECURITY SYSTEM.—The term ''national security system'' has the meaning given that term in section 3552 of title 44, United States Code, as added by section 201 of this Act.

(21) OWNER.—The term ''owner''—

(A) means an entity that owns critical infrastructure; and

(B) does not include a company contracted by the owner to manage, run, or operate that critical infrastructure, or to provide a specific

information technology product or service that is used or incorporated into that critical infrastructure.

(22) OPERATOR.—The term ''operator''—

(A) means an entity that manages, runs, or operates, in whole or in part, the day-to-day operations of critical infrastructure; and

(B) may include the owner of critical infrastructure.

(23) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(24) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means an incident resulting in, or an attempted to cause an incident that, if successful, would have resulted in—

(A) the exfiltration of data that is essential to the operation of critical cyber infrastructure; or

(B) the defeat of an operational control or technical control, as those terms are defined in section 708, essential to the security or operation of critical cyber infrastructure.

TITLE I—PUBLIC-PRIVATE PARTNERSHIP TO PROTECT CRITICAL INFRASTRUCTURE

SEC. 101. NATIONAL CYBERSECURITY COUNCIL.

(a) IN GENERAL.—There is established a National Cybersecurity Council.

(b) RESPONSIBILITIES.—The Council shall—

(1) conduct sector-by-sector risk assessments in partnership with owners and operators, private sector entities, relevant Federal agencies, and appropriate non-governmental entities and institutions of higher education;

(2) identify categories of critical cyber infrastructure, in partnership with relevant Federal agencies, owners and operators, other appropriate private sector entities, and appropriate non-governmental entities and institutions of higher education;

(3) coordinate the adoption of private-sector recommended voluntary outcome-based cybersecurity practices with owners and operators, private sector entities, relevant Federal agencies, the Critical Infrastructure Partnership Advisory Council, institutions of higher education, and appropriate non-governmental cybersecurity experts, in accordance with this title;

(4) establish an incentives-based voluntary cybersecurity program for critical infrastructure to encourage owners to adopt voluntary outcome-based cybersecurity practices under section 103;

(5) develop procedures to inform owners and operators of cyber threats, vulnerabilities, and consequences; and

(6) upon request and to the maximum extent possible, provide any technical guidance or assistance to owners and operators consistent with this title.

(c) PROCEDURES.—The President shall establish procedures, consistent with this section, for the operation of the Council, which shall include procedures that—

(1) prescribe the responsibilities of the Council and the member agencies;

(2) ensure the timely implementation of decisions of the Council;

(3) delegate authority to the Chairperson to take action to fulfill the responsibilities of the Council if—

(A) the Council is not fulfilling the responsibilities of the Council in a timely fashion; or

(B) necessary to prevent or mitigate an imminent cybersecurity threat.

(d) MEMBERSHIP.—The Council shall be comprised of appropriate representatives appointed by the President from—

(1) the Department of Commerce;

(2) the Department of Defense;

(3) the Department of Justice;

(4) the intelligence community;

(5) sector-specific Federal agencies, as appropriate;

(6) Federal agencies with responsibility for regulating the security of critical cyber infrastructure, as appropriate; and

(7) the Department.

(e) COORDINATION.—The Council shall coordinate the activities of the Council with—

(1) appropriate representatives of the private sector; and

(2) owners and operators.

(f) CHAIRPERSON.—

(1) IN GENERAL.—The Secretary shall serve as Chairperson of the Council (referred to in this section as the ''Chairperson'').

(2) RESPONSIBILITIES OF THE CHAIRPERSON.—The Chairperson shall—

(A) ensure the responsibilities of the Council are expeditiously fulfilled;

(B) provide expertise and support to the Council; and

(C) provide recommendations to the Council.

(g) PARTICIPATION OF SECTOR-SPECIFIC FEDERAL AGENCIES AND FEDERAL REGULATORY AGENCIES.—A sector-specific Federal agency and a Federal agency with responsibility for regulating the security of critical cyber infrastructure shall participate on the Council on matters directly relating to the sector of critical infrastructure for which the Federal agency has responsibility to ensure that any cybersecurity practice adopted by the Council under section 103—

(1) does not contradict any regulation or compulsory standard in effect before the adoption of the cybersecurity practice; and

(2) to the extent possible, complements or otherwise improves the regulation or compulsory standard described in paragraph (1).

SEC. 102. INVENTORY OF CRITICAL INFRASTRUCTURE.

(a) RISK ASSESSMENTS.—

(1) IN GENERAL.—

(A) DESIGNATION OF MEMBER AGENCY.—The Council shall designate a member agency to conduct top-level cybersecurity assessments of cyber risks to critical infrastructure with voluntary participation from private sector entities.

(B) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to give new authority to a Federal agency to require owners or operators to provide information to the Federal Government.

(2) RESPONSIBILITY.—The member agency designated under paragraph (1), in consultation with owners and operators, the Critical Infrastructure Partnership Advisory Council, and appropriate Information Sharing and Analysis Organizations, and in coordination with other member agencies, the intelligence community, and the Department of Commerce, shall—

(A) not later than 180 days after the date of enactment of this Act, conduct a top-level assessment of the cybersecurity threats, vulnerabilities, and consequences and the probability of a catastrophic incident and associated risk across all critical infrastructure sectors to

determine which sectors pose the greatest immediate risk, in order to guide the allocation of resources for the implementation of this Act; and

(B) beginning with the highest priority sectors identified under subparagraph (A), conduct, on an ongoing, sector-by-sector basis, cyber risk assessments of the threats to, vulnerabilities of, and consequences of a cyber attack on critical infrastructure.

(3) VOLUNTARY INPUT OF OWNERS AND OPERATORS.—The member agency designated under paragraph (1) shall—

(A) establish a process under which owners and operators and other relevant private sector experts may provide input into the risk assessments conducted under this section; and

(B) seek and incorporate private sector expertise available through established public-private partnerships, including the Critical Infrastructure Partnership Advisory Council and appropriate Information Sharing and Analysis Organizations.

(4) PROTECTION OF INFORMATION.—Any information submitted as part of the process established

under paragraph (3) shall be protected in accordance with section 106.

(5) SUBMISSION OF RISK ASSESSMENTS.—The Council shall submit each risk assessment conducted under this section, in a classified or unclassified form as necessary, to—

(A) the President;

(B) appropriate Federal agencies; and

(C) appropriate congressional committees.

(b) IDENTIFICATION OF CRITICAL CYBER INFRASTRUCTURE CATEGORIES.—

(1) IN GENERAL.—The Council, in consultation with owners and operators, the Critical Infrastructure Partnership Advisory Council, appropriate Information Sharing and Analysis Organizations, and other appropriate representatives of State and local governments, shall establish procedures to identify categories of critical cyber infrastructure within each sector of critical infrastructure for the purposes of this Act.

(2) DUTIES.—In establishing the procedure under paragraph (1), the Council shall—

(A) prioritize efforts based on the prioritization established under subsection (a);

(B) incorporate, to the extent practicable, the input of owners and operators, the Critical Infrastructure Partnership Advisory Council, appropriate Information Sharing and Analysis Organizations, and other appropriate representatives of the private sector and State and local governments;

(C) develop a voluntary mechanism for owners to submit information to assist the Council in making determinations under this section;

(D) inform owners and operators of the criteria used to identify categories of critical cyber infrastructure;

(E) establish procedures for an owner of critical infrastructure identified as critical cyber infrastructure to challenge the identification;

(F) select a member agency to make recommendations to the Council on the identification of categories of critical cyber infrastructure; and

(G) periodically review and update identifications under this subsection.

(3) IDENTIFICATION REQUIREMENTS.—The Council shall—

(A) identify categories of critical cyber infrastructure within each sector of critical infrastructure and identify owners of critical infrastructure within each category of critical cyber infrastructure;

(B) only identify a category of critical infrastructure as critical cyber infrastructure if damage to or unauthorized access to such critical infrastructure could reasonably result in—

(i) the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause—

(I) a mass casualty event; or

(II) mass evacuations;

(ii) catastrophic economic damage to the United States including—

(I) failure or substantial disruption of a financial market of the United States;

(II) incapacitation or sustained disruption of a transportation system; or

(III) other systemic, long-term damage to the economy of the United States; or

(iii) severe degradation of national security or national security capabilities, including intelligence and defense functions; and

(C) consider the sector-by-sector risk assessments developed in accordance with subsection (a).

(4) INCIDENT REPORTING.—The Council shall establish procedures under which each owner of critical cyber infrastructure shall report significant cyber incidents affecting critical cyber infrastructure.

(5) LIMITATIONS.—The Council may not identify as a category of critical cyber infrastructure under this section—

(A) critical infrastructure based solely on activities protected by the first amendment to the Constitution of the United States;

(B) an information technology product based solely on a finding that the product is capable of, or is actually, being used in critical cyber infrastructure; or

(C) a commercial item that organizes or communicates information electronically.

(6) NOTIFICATION OF IDENTIFICATION OF CATEGORY OF CRITICAL CYBER INFRASTRUCTURE.—Not later than 10 days after the Council identifies a category of critical cyber infrastructure under this section, the Council shall notify the relevant owners of the identified critical cyber infrastructure.

(7) DEFINITION.—In this subsection, the term ''damage'' has the meaning given that term in section 1030(e) of title 18, United States Code.

(c) CONGRESSIONAL NOTICE AND OPPORTUNITY FOR DISAPPROVAL.—

(1) NOTIFICATION.—Not later than 10 days after the date on which the Council identifies a category of critical infrastructure as critical cyber infrastructure under this section, the Council shall—

(A) notify Congress of the identification; and

(B) submit to Congress a report explaining the basis for the identification.

(2) OPPORTUNITY FOR CONGRESSIONAL REVIEW.—The identification of a category of critical infrastructure as critical cyber infrastructure shall not take effect for purposes of this title until the

date that is 60 days after the date on which the Council notifies Congress under paragraph (1).

SEC. 103. VOLUNTARY CYBERSECURITY PRACTICES.

(a) PRIVATE SECTOR DEVELOPMENT OF CYBERSECURITY PRACTICES.—Not later than 180 days after the date of enactment of this Act, each sector coordinating council shall propose to the Council voluntary outcome-based cybersecurity practices (referred to in this section as ''cybersecurity practices'') sufficient to effectively remediate or mitigate cyber risks identified through an assessment conducted under section 102(a) comprised of—

(1) industry best practices, standards, and guidelines; or

(2) practices developed by the sector coordinating council in coordination with owners and operators, voluntary consensus standards development organizations, representatives of State and local governments, the private sector, and appropriate information sharing and analysis organizations.

(b) REVIEW OF CYBERSECURITY PRACTICES.—

(1) IN GENERAL.—The Council shall, in consultation with owners and operators, the Critical Infrastructure Partnership Advisory Council, and appropriate information sharing and analysis organiza-

tions, and in coordination with appropriate representatives from State and local governments—

(A) consult with relevant security experts and institutions of higher education, including university information security centers, appropriate nongovernmental cybersecurity experts, and representatives from national laboratories;

(B) review relevant regulations or compulsory standards or guidelines;

(C) review cybersecurity practices proposed under subsection (a); and

(D) consider any amendments to the cybersecurity practices and any additional cybersecurity practices necessary to ensure adequate remediation or mitigation of the cyber risks identified through an assessment conducted under section 102(a).

(2) ADOPTION.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Council shall—

(i) adopt any cybersecurity practices proposed under subsection (a) that adequately remediate or mitigate identified cyber risks and any associated con-

sequences identified through an assessment conducted under section 102(a); and

(ii) adopt any amended or additional cybersecurity practices necessary to ensure the adequate remediation or mitigation of the cyber risks identified through an assessment conducted under section 102(a).

(B) NO SUBMISSION BY SECTOR COORDINATING COUNCIL.—If a sector coordinating council fails to propose to the Council cybersecurity practices under subsection (a) within 180 days of the date of enactment of this Act, not later than 1 year after the date of enactment of this Act the Council shall adopt cybersecurity practices that adequately remediate or mitigate identified cyber risks and associated consequences identified through an assessment conducted under section 102(a) for the sector.

(c) FLEXIBILITY OF CYBERSECURITY PRACTICES.—Each sector coordinating council and the Council shall periodically assess cybersecurity practices, but not less frequently than once every 3 years, and update or modify cybersecurity practices as necessary to ensure adequate remediation and mitigation of the cyber risks identified through an assessment conducted under section 102(a).

(d) PRIORITIZATION.—Based on the risk assessments performed under section 102(a), the Council shall prioritize the development of cybersecurity practices to ensure the reduction or mitigation of the greatest cyber risks.

(e) PRIVATE SECTOR RECOMMENDED MEASURES.—Each sector coordinating council shall develop voluntary recommended cybersecurity measures that provide owners reasonable and cost-effective methods of meeting any cybersecurity practice.

(f) TECHNOLOGY NEUTRALITY.—No cybersecurity practice shall require—

(1) the use of a specific commercial information technology product; or

(2) that a particular commercial information technology product be designed, developed, or manufactured in a particular manner.

(g) RELATIONSHIP TO EXISTING REGULATIONS.—

(1) INCLUSION IN REGULATORY REGIMES.—

(A) IN GENERAL.—A Federal agency with responsibilities for regulating the security of critical infrastructure may adopt the cybersecurity practices as mandatory requirements.

(B) REPORTS.—If, as of the date that is 1 year after the date of enactment of this Act,

a Federal agency with responsibilities for regulating the security of critical infrastructure has not adopted the cybersecurity practices as mandatory requirements, the agency shall submit to the appropriate congressional committees a report on the reasons the agency did not do so, including a description of whether the critical cyber infrastructure for which the Federal agency has responsibility is maintaining practices sufficient to effectively remediate or mitigate cyber risks identified through an assessment conducted under section 102(a).

(C) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to provide a Federal agency with authority for regulating the security of critical cyber infrastructure in addition or to a greater extent than the authority the Federal agency has under other law.

(2) AVOIDANCE OF CONFLICT.—No cybersecurity practice shall—

(A) prevent an owner (including a certified owner) from complying with any law or regulation; or

(B) require an owner (including a certified owner) to implement cybersecurity measures

that prevent the owner from complying with any law or regulation.

(3) AVOIDANCE OF DUPLICATION.—Where regulations or compulsory standards regulate the security of critical cyber infrastructure, a cybersecurity practice shall, to the greatest extent possible, complement or otherwise improve the regulations or compulsory standards.

(h) INDEPENDENT REVIEW.—

(1) IN GENERAL.—Each cybersecurity practice shall be publicly reviewed by the relevant sector coordinating council and the Critical Infrastructure Partnership Advisory Council, which may include input from relevant institutions of higher education, including university information security centers, national laboratories, and appropriate non-governmental cybersecurity experts.

(2) CONSIDERATION BY COUNCIL.—The Council shall consider any review conducted under paragraph (1).

(i) VOLUNTARY TECHNICAL ASSISTANCE.—At the request of an owner or operator of critical infrastructure, the Council shall provide guidance on the application of cybersecurity practices to the critical infrastructure.

SEC. 104. VOLUNTARY CYBERSECURITY PROGRAM FOR CRITICAL INFRASTRUCTURE.

(a) VOLUNTARY CYBERSECURITY PROGRAM FOR CRITICAL INFRASTRUCTURE.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Council, in consultation with owners and operators and the Critical Infrastructure Partnership Advisory Council, shall establish the Voluntary Cybersecurity Program for Critical Infrastructure in accordance with this section.

(2) ELIGIBILITY.—

(A) IN GENERAL.—An owner of critical cyber infrastructure may apply for certification under the Voluntary Cybersecurity Program for Critical Infrastructure.

(B) CRITERIA.—The Council shall establish criteria for owners of critical infrastructure that is not critical cyber infrastructure to be eligible to apply for certification in the Voluntary Cybersecurity Program for Critical Infrastructure.

(3) APPLICATION FOR CERTIFICATION.—An owner of critical cyber infrastructure or an owner of critical infrastructure that meets the criteria estab-

lished under paragraph (2)(B) that applies for certification under this subsection shall—

(A) select and implement cybersecurity measures of their choosing that satisfy the outcome-based cybersecurity practices established under section 103; and

(B)(i) certify in writing and under penalty of perjury to the Council that the owner has developed and effectively implemented cybersecurity measures sufficient to satisfy the outcome-based cybersecurity practices established under section 103; or

(ii) submit to the Council an assessment verifying that the owner has developed and effectively implemented cybersecurity measures sufficient to satisfy the outcome-based cybersecurity practices established under section 103.

(4) CERTIFICATION.—Upon receipt of a self-certification under paragraph (3)(B)(i) or an assessment under paragraph (3)(B)(ii) the Council shall certify an owner.

(5) NONPERFORMANCE.—If the Council determines that a certified owner is not in compliance with the cybersecurity practices established under section 103, the Council shall—

(A) notify the certified owner of such determination; and

(B) work with the certified owner to remediate promptly any deficiencies.

(6) REVOCATION.—If a certified owner fails to remediate promptly any deficiencies identified by the Council, the Council shall revoke the certification of the certified owner.

(7) REDRESS.—

(A) IN GENERAL.—If the Council revokes a certification under paragraph (6), the Council shall—

(i) notify the owner of such revocation; and

(ii) provide the owner with specific cybersecurity measures that, if implemented, would remediate any deficiencies.

(B) RECERTIFICATION.—If the Council determines that an owner has remedied any deficiencies and is in compliance with the cybersecurity practices, the Council may recertify the owner.

(b) ASSESSMENTS.—

(1) THIRD-PARTY ASSESSMENTS.—The Council, in consultation with owners and operators and the

Critical Infrastructure Protection Advisory Council, shall enter into agreements with qualified third-party private entities, to conduct assessments that use reliable, repeatable, performance-based evaluations and metrics to assess whether an owner certified under subsection (a)(3)(B)(ii) is in compliance with all applicable cybersecurity practices.

(2) TRAINING.—The Council shall ensure that third party assessors described in paragraph (1) undergo regular training and accreditation.

(3) OTHER ASSESSMENTS.—Using the procedures developed under this section, the Council may perform cybersecurity assessments of a certified owner based on actual knowledge or a reasonable suspicion that the certified owner is not in compliance with the cybersecurity practices or any other risk-based factors as identified by the Council.

(4) NOTIFICATION.—The Council shall provide copies of any assessments by the Federal Government to the certified owner.

(5) ACCESS TO INFORMATION.—

(A) IN GENERAL.—For the purposes of an assessment conducted under this subsection, a certified owner shall provide the Council, or a

third party assessor, any reasonable access necessary to complete an assessment.

(B) PROTECTION OF INFORMATION.—Information provided to the Council, the Council's designee, or any assessor during the course of an assessment under this section shall be protected from disclosure in accordance with section 106.

(c) BENEFITS OF CERTIFICATION.—

(1) LIMITATIONS ON CIVIL LIABILITY.—

(A) IN GENERAL.—In any civil action for damages directly caused by an incident related to a cyber risk identified through an assessment conducted under section 102(a), a certified owner shall not be liable for any punitive damages intended to punish or deter if the certified owner is in substantial compliance with the appropriate cybersecurity practices at the time of the incident related to that cyber risk.

(B) LIMITATION.—Subaragraph (A) 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 owner.

(2) EXPEDITED SECURITY CLEARANCE PROCESS.—The Council, in coordination with the Office of the Director of National Intelligence, shall establish a procedure to expedite the provision of security clearances to appropriate personnel employed by a certified owner.

(3) PRIORITIZED TECHNICAL ASSISTANCE.—The Council shall ensure that certified owners are eligible to receive prioritized technical assistance.

(4) PROVISION OF CYBER THREAT INFORMATION.—The Council shall develop, in coordination with certified owners, a procedure for ensuring that certified owners are, to the maximum extent practicable and consistent with the protection of sources and methods, informed of relevant real-time cyber threat information.

(5) PUBLIC RECOGNITION.—With the approval of a certified owner, the Council may publicly recognize the certified owner if the Council determines such recognition does not pose a risk to the security of critical cyber infrastructure.

(6) STUDY TO EXAMINE BENEFITS OF PROCUREMENT PREFERENCE.—

(A) IN GENERAL.—The Federal Acquisition Regulatory Council, in coordination with

the Council and with input from relevant private sector individuals and entities, shall conduct a study examining the potential benefits of establishing a procurement preference for the Federal Government for certified owners.

(B) AREAS.—The study under subparagraph (A) shall include a review of—

(i) potential persons and related property and services that could be eligible for preferential consideration in the procurement process;

(ii) development and management of an approved list of categories of property and services that could be eligible for preferential consideration in the procurement process;

(iii) appropriate mechanisms to implement preferential consideration in the procurement process, including—

(I) establishing a policy encouraging Federal agencies to conduct market research and industry outreach to identify property and services that adhere to relevant cybersecurity practices;

(II) authorizing the use of a mark for the Voluntary Cybersecurity Program for Critical Infrastructure to be used for marketing property or services to the Federal Government;

(III) establishing a policy of encouraging procurement of certain property and services from an approved list;

(IV) authorizing the use of a preference by Federal agencies in the evaluation process; and

(V) authorizing a requirement in certain solicitations that the person providing the property or services be a certified owner; and

(iv) benefits of and impact on the economy and efficiency of the Federal procurement system, if preferential consideration were given in the procurement process to encourage the procurement of property and services that adhere to relevant baseline performance goals establishing under the Voluntary Cybersecurity Program for Critical Infrastructure.

SEC. 105. RULES OF CONSTRUCTION.

Nothing in this title shall be construed to—

(1) limit the ability of a Federal agency with responsibilities for regulating the security of critical infrastructure from requiring that the cybersecurity practices developed under section 103 be met;

(2) provide additional authority for any sector-specific agency or any Federal agency that is not a sector-specific agency with responsibilities for regulating the security of critical infrastructure to establish standards or other cybersecurity measures that are applicable to the security of critical infrastructure not otherwise authorized by law;

(3) limit or restrict the authority of the Department, or any other Federal agency, under any other provision of law; or

(4) permit any owner (including a certified owner) to fail to comply with any other law or regulation, unless specifically authorized.

SEC. 106. PROTECTION OF INFORMATION.

(a) DEFINITIONS.—In this section—

(1) the term ''covered information'' means any information—

(A) submitted as part of the process established under section 102(a)(3);

(B) submitted under section 102(b)(2)(C);

(C) required to be submitted by owners under section 102(b)(4);

(D) provided to the Secretary, the Secretary's designee, or any assessor during the course of an assessment under section 104; or

(E) provided to the Secretary or the Inspector General of the Department through the tip line or another secure channel established under subsection (c); and

(2) the term ''Inspector General'' means an Inspector General described in subparagraph (A), (B), or (I) of section 11(b)(1) of the Inspector General Act of 1978 (5 U.S.C. App.), the Inspector General of the United States Postal Service, the Inspector General of the Central Intelligence Agency, and the Inspector General of the Intelligence Community.

(b) CRITICAL INFRASTRUCTURE INFORMATION.—

(1) IN GENERAL.—Covered information shall be treated as voluntarily shared critical infrastructure information under section 214 of the Homeland Security Act of 2002 (6 U.S.C. 133), except that the requirement of such section 214 that the information be voluntarily submitted shall not be required for protection of information under this section to apply.

(2) SAVINGS CLAUSE FOR EXISTING WHISTLEBLOWER PROTECTIONS.—With respect to covered information, the rights and protections relating to disclosure by individuals of voluntarily shared critical infrastructure information submitted under subtitle B of title II of the Homeland Security Act of 2002 (6 U.S.C. 131 et seq.) shall apply with respect to disclosure of the covered information by individuals.

(c) CRITICAL INFRASTRUCTURE CYBER SECURITY TIP LINE.—

(1) IN GENERAL.—The Secretary shall establish and publicize the availability of a Critical Infrastructure Cyber Security Tip Line (and any other secure means the Secretary determines would be desirable to establish), by which individuals may report—

(A) concerns involving the security of covered critical infrastructure against cyber risks; and

(B) concerns (in addition to any concerns described under subparagraph (A)) with respect to programs and functions authorized or funded under this title involving—

(i) a possible violation of any law, rule, regulation or guideline;

(ii) mismanagement;

(iii) risk to public health, safety, security, or privacy; or

(iv) other misfeasance or nonfeasance.

(2) DESIGNATION OF EMPLOYEES.—The Secretary and the Inspector General of the Department shall each designate employees authorized to receive concerns reported under this subsection that include—

(A) disclosure of covered information; or

(B) any other disclosure of information that is specifically prohibited by law or is specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs.

(3) HANDLING OF CERTAIN CONCERNS.—A concern described in paragraph (1)(B)—

(A) shall be received initially to the Inspector General of the Department;

(B) shall not be provided initially to the Secretary; and

(C) may be provided to the Secretary if determined appropriate by the Inspector General of the Department.

(d) 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 thereto, 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 thereto;

(3) limit or otherwise affect the ability of an entity, agency, or authority of a State, a local government, or the Federal Government or any other individual or entity under applicable law to obtain information that is not covered information (including any information lawfully and properly disclosed generally or broadly to the public) and to use such information in any manner permitted by law, including the disclosure of such information under—

(A) section 552 or 2302(b)(8) of title 5, United States Code;

(B) section 2409 of title 10, United States Code; or

(C) any other Federal, State, or local law, ordinance, or regulation that protects against retaliation an individual who discloses information that the individual reasonably believes evidences a violation of any law, rule, or regulation, gross mismanagement, substantial and specific danger to public health, safety, or security, or other misfeasance or nonfeasance;

(4) prevent the Secretary from using information required to be submitted under this Act for enforcement of this title, including enforcement proceedings subject to appropriate safeguards;

(5) authorize information to be withheld from any committee of Congress, the Comptroller General, or any Inspector General;

(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.

(e) AUDIT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Inspector General of the Department shall conduct an audit of the management of covered information under this

title and report the findings to appropriate congressional committees.

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

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

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

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

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

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

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

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

SEC. 107. ANNUAL ASSESSMENT OF CYBERSECURITY.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, and every year thereafter, the Council shall submit to the appropriate congressional committees a report on the effectiveness of this title in reducing the risk of cyber attack to critical infrastructure.

(b) CONTENTS.—Each report submitted under subsection (a) shall include—

(1) a discussion of cyber risks and associated consequences and whether the cybersecurity practices developed under section 103 are sufficient to effectively remediate and mitigate cyber risks and associated consequences; and

(2) an analysis of—

(A) whether owners of critical cyber infrastructure are successfully implementing the cybersecurity practices adopted under section 103;

(B) whether the critical infrastructure of the United States is effectively secured from cybersecurity threats, vulnerabilities, and consequences;

(C) whether Federal agencies with responsibilities for regulating the security of critical

infrastructure are adequately adopting and enforcing the cybersecurity practices adopted under section 103; and

(D) whether additional legislative authority or other actions are needed to effectively remediate or mitigate cyber risks and associated consequences.

(c) FORM OF REPORT.—A report submitted under this subsection shall be submitted in an unclassified form, but may include a classified annex, if necessary.

SEC. 108. INTERNATIONAL COOPERATION.

(a) IN GENERAL.—The Secretary, in coordination with the Secretary of State, the heads of appropriate sector-specific agencies, and the heads of any appropriate Federal agency with responsibilities for regulating the security of covered critical infrastructure, shall—

(1) 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 within the United States and the government of the country in which the information infrastructure is located of any cyber risks to such information infrastructure; and

(2) coordinate with the government of the country in which such information infrastructure is located and, as appropriate, the owner or operator of the information infrastructure regarding the implementation of cybersecurity measures or other measures to the information infrastructure to mitigate or remediate cyber risks.

(b) INTERNATIONAL AGREEMENTS.—The Secretary, in coordination with the Secretary of State, including in particular with the interpretation of international agreements, shall perform the functions prescribed by this section consistent with applicable international agreements.

SEC. 109. EFFECT ON OTHER LAWS.

Except as expressly provided in section 104(c)(1) and section 106, nothing in this Act shall be construed to preempt the applicability of any State law or requirement.

SEC. 110. DEFINITIONS.

In this title:

(1) CERTIFIED OWNER.—The term ''certified owner'' means an owner of critical cyber infrastructure or an owner of critical infrastructure that is certified by the Council under section 104(a)(4).

(2) CYBER RISK.—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 critical infrastructure.

(3) SECTOR COORDINATING COUNCIL.—The term ''sector coordinating council'' means a private sector coordinating council comprised of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan.

(4) SECTOR-SPECIFIC AGENCY.—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 Act.

TITLE II—FEDERAL INFORMATION SECURITY MANAGEMENT AND CONSOLIDATING RESOURCES

SEC. 201. FISMA REFORM.

(a) 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

"§ 3551. 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 Federal operations and assets;

"(2) recognize the highly networked nature of the Federal computing environment and provide effective governmentwide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

"(3) provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture; and

"(4) provide a mechanism to improve and continuously monitor the security of agency information security programs and systems through a focus on continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

"§ 3552. Definitions

"(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 (including the definitions of the terms 'agency' and 'information system') shall apply to this subchapter.

"(b) OTHER TERMS.—In this subchapter:

"(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and impact resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

"(2) CONTINUOUS MONITORING.—The term 'continuous monitoring' means the ongoing real time or near real-time process used to determine if the

complete set of planned, required, and deployed security controls within an information system continue to be effective over time in light of rapidly changing information technology and threat development. To the maximum extent possible, this also requires automation of that process to enable cost effective, efficient, and consistent monitoring and provide a more dynamic view of the security state of those deployed controls.

"(3) COUNTERMEASURE.—The term 'countermeasure' means automated or manual actions with defensive intent to modify or block data packets associated with electronic or wire communications, Internet traffic, program code, or other system traffic transiting to or from or stored on an information system for the purpose of protecting the information system from cybersecurity threats, conducted on an information system owned or operated by or on behalf of the party to be protected or operated by a private entity acting as a provider of electronic communication services, remote computing services, or cybersecurity services to the party to be protected.

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

"(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

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

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

"(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring nonrepudiation and authenticity;

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

"(C) availability, which means ensuring timely and reliable access to and use of information.

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

"(7) NATIONAL SECURITY SYSTEM.—

"(A) IN GENERAL.—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) EXCLUSION.—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).

"(8) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

"§ 3553. Federal information security authority and coordination

"(a) IN GENERAL.—Except as provided in subsections (f) and (g), the Secretary shall oversee agency information security policies and practices, including the development and oversight of information security policies and directives and compliance with this subchapter.

"(b) DUTIES.—The Secretary shall—

"(1) develop, issue, and oversee the implementation of information security policies and directives, which shall be compulsory and binding on agencies

to the extent determined appropriate by the Secretary, including—

"(A) policies and directives consistent with the standards promulgated under section 11331 of title 40 to identify and provide information security protections that are commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

"(i) information collected, created, processed, stored, disseminated, or otherwise used or maintained by or on behalf of an agency; or

"(ii) information systems used or operated by an agency or by a contractor of an agency or other organization, such as a State government entity, on behalf of an agency;

"(B) minimum operational requirements for network operations centers and security operations centers of agencies to facilitate the protection of and provide common situational awareness for all agency information and information systems;

"(C) reporting requirements, consistent with relevant law, regarding information security incidents;

"(D) requirements for agencywide information security programs, including continuous monitoring of information security;

"(E) performance requirements and metrics for the security of agency information systems;

"(F) training requirements to ensure that agencies are able to fully and timely comply with directions issued by the Secretary under this subchapter;

"(G) training requirements regarding privacy, civil rights, civil liberties, and information oversight for agency information security employees;

"(H) requirements for the annual reports to the Secretary under section 3554(c); and

"(I) any other information security requirements as determined by the Secretary;

"(2) review agency information security programs required to be developed under section 3554(b);

"(3) develop and conduct targeted risk assessments and operational evaluations for agency information and information systems in consultation with the heads of other agencies or governmental and private entities that own and operate such systems, that may include threat, vulnerability, and impact assessments and penetration testing;

"(4) operate consolidated intrusion detection, prevention, or other protective capabilities and use associated countermeasures for the purpose of protecting agency information and information systems from information security threats;

"(5) in conjunction with other agencies and the private sector, assess and foster the development of information security technologies and capabilities for use across multiple agencies;

"(6) designate an entity to receive reports and information about information security incidents, threats, and vulnerabilities affecting agency information systems;

"(7) provide incident detection, analysis, mitigation, and response information and remote or on-site technical assistance to the heads of agencies;

"(8) coordinate with appropriate agencies and officials to ensure, to the maximum extent feasible,

that policies and directives issued under paragraph (1) are complementary with—

"(A) standards and guidelines developed for national security systems; and

"(B) policies and directives issues by the Secretary of Defense, Director of the Central Intelligence Agency, and Director of National Intelligence under subsection (g)(1); and

"(9) not later than March 1 of each year, submit to Congress a report on agency compliance with the requirements of this subchapter, which shall include—

"(A) a summary of the incidents described by the reports required in section 3554(c);

"(B) a summary of the results of assessments required by section 3555;

"(C) a summary of the results of evaluations required by section 3556;

"(D) significant deficiencies in agency information security practices as identified in the reports, assessments, and evaluations referred to in subparagraphs (A), (B), and (C), or otherwise; and

"(E) planned remedial action to address any deficiencies identified under subparagraph (D).

"(c) ISSUING POLICIES AND DIRECTIVES.—When issuing policies and directives under subsection (b), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology and issued by the Secretary of Commerce under section 11331 of title 40. The Secretary shall consult with the Director of the National Institute of Standards and Technology when such policies and directives implement standards or guidelines developed by National Institute of Standards and Technology. To the maximum extent feasible, such standards and guidelines shall be complementary with standards and guidelines developed for national security systems.

"(d) COMMUNICATIONS AND SYSTEM TRAFFIC.—

"(1) IN GENERAL.—Notwithstanding any other provision of law, in carrying out the responsibilities under paragraphs (3) and (4) of subsection (b), if the Secretary makes a certification described in paragraph (2), the Secretary may acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on agency information systems and deploy

countermeasures with regard to the communications and system traffic.

"(2) CERTIFICATION.—A certification described in this paragraph is a certification by the Secretary that—

"(A) the acquisitions, interceptions, and countermeasures are reasonably necessary for the purpose of protecting agency information systems from information security threats;

"(B) the content of communications will be collected and retained only when the communication is associated with a known or reasonably suspected information security threat, and communications and system traffic will not be subject to the operation of a countermeasure unless associated with the threats;

"(C) information obtained under activities authorized under this subsection will only be retained, used, or disclosed to protect agency information systems from information security threats, mitigate against such threats, or, with the approval of the Attorney General, for law enforcement purposes when—

"(i) the information is evidence of a crime that has been, is being, or is about to be committed; and

"(ii) disclosure of the information to a law enforcement agency is not otherwise prohibited by law;

"(D) notice has been provided to users of agency information systems concerning the potential for acquisition, interception, retention, use, and disclosure of communications and other system traffic; and

"(E) the activities are implemented pursuant to policies and procedures governing the acquisition, interception, retention, use, and disclosure of communications and other system traffic that have been reviewed and approved by the Attorney General.

"(3) PRIVATE ENTITIES.—The Secretary may enter into contracts or other agreements, or otherwise request and obtain the assistance of, private entities that provide electronic communication or information security services to acquire, intercept, retain, use, and disclose communications and other system traffic or to deploy countermeasures in accordance with this subsection.

"(e) DIRECTIONS TO AGENCIES.—

"(1) AUTHORITY.—

"(A) IN GENERAL.—Notwithstanding section 3554, and subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may direct other agency heads to take any lawful action with respect to the operation of the information systems, including those owned or operated by another entity on behalf of an agency, that collect, process, store, transmit, disseminate, or otherwise maintain agency information, for the purpose of protecting the information system from or mitigating an information security threat.

"(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a system described in paragraph (2), (3), or (4) of subsection (g).

"(2) PROCEDURES FOR USE OF AUTHORITY.—The Secretary shall—

"(A) in coordination with the Director of the Office of Management and Budget and, as

appropriate, in consultation with operators of information systems, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

"(i) thresholds and other criteria;

"(ii) privacy and civil liberties protections; and

"(iii) providing notice to potentially affected third parties;

"(B) specify the reasons for the required action and the duration of the directive;

"(C) minimize the impact of directives under this subsection by—

"(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and

"(ii) limiting directives to the shortest period practicable; and

"(D) notify the Director of the Office of Management and Budget and head of any affected agency immediately upon the issuance of a directive under this subsection.

"(3) IMMINENT THREATS.—

"(A) IN GENERAL.—If the Secretary determines that there is an imminent threat to agency information systems and a directive under this subsection is not reasonably likely to result in a timely response to the threat, the Secretary may authorize the use of protective capabilities under the control of the Secretary for communications or other system traffic transiting to or from or stored on an agency information system without prior consultation with the affected agency for the purpose of ensuring the security of the information or information system or other agency information systems.

"(B) LIMITATION ON DELEGATION.—The authority under this paragraph may not be delegated to an official in a position lower than Assistant Secretary or Director of the National Cybersecurity and Communications Integration Center.

"(C) NOTICE.—The Secretary or designee of the Secretary shall immediately notify the Director of the Office of Management and Budget and the head and chief information officer (or equivalent official) of each affected agency of—

"(i) any action taken under this subsection; and

"(ii) the reasons for and duration and nature of the action.

"(D) OTHER LAW.—The actions of the Secretary under this paragraph shall be consistent with applicable law.

"(4) LIMITATION.—The Secretary may direct or authorize lawful action or protective capability under this subsection only to—

"(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or

"(B) require the remediation of or protect against identified information security risks with respect to—

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

"(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

"(f) NATIONAL SECURITY SYSTEMS.—

"(1) IN GENERAL.—This section shall not apply to a national security system.

"(2) INFORMATION SECURITY.—Information security policies, directives, standards, and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over national security systems.

"(g) DELEGATION OF AUTHORITIES.—

"(1) IN GENERAL.—The authorities of the Secretary described in paragraphs (1), (2), (3), and (4) of subsection (b) shall be delegated to—

"(A) the Secretary of Defense in the case of systems described in paragraph (2);

"(B) the Director of the Central Intelligence Agency in the case of systems described in paragraph (3); and

"(C) the Director of National Intelligence in the case of systems described in paragraph (4).

"(2) DEPARTMENT OF DEFENSE.—The systems described in this paragraph 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 process any information the unauthorized access, use, disclo-

sure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

"(3) CENTRAL INTELLIGENCE AGENCY.—The systems described in this paragraph 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 process 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.

"(4) OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.—The systems described in this paragraph are systems that are operated by the Office of the Director of National Intelligence, a contractor of the Office of the Director of National Intelligence, or another entity on behalf of the Office of the Director of National Intelligence that process any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Office of the Director of National Intelligence.

"(5) INTEGRATION OF INFORMATION.—The Secretary of Defense, the Director of the Central Intelligence Agency, and the Director of National Intelligence shall carry out their responsibilities under this subsection in coordination with the Secretary and share relevant information in a timely manner with the Secretary relating to the security of agency information and information systems, including systems described in paragraphs (2), (3), and (4), to enable the Secretary to carry out the responsibilities set forth in this section and to maintain comprehensive situational awareness regarding information security incidents, threats, and vulnerabilities affecting agency information systems, consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

"§ 3554. Agency responsibilities

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

"(1) be responsible for—

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

"(i) information collected, created, processed, stored, disseminated, or otherwise used or maintained by or on behalf of the agency; or

"(ii) information systems used or operated by the agency or by a contractor of the agency or other organization, such as a State government entity, on behalf of the agency;

"(B) complying with this subchapter, including—

"(i) the policies and directives issued under section 3553, including any directions under section 3553(e); and

"(ii) information security policies, directives, standards, and guidelines for national security systems issued in accordance with law and as directed by the President;

"(C) complying with the requirements of the information security standards prescribed under section 11331 of title 40, including any required security configuration checklists; and

"(D) ensuring that information security management processes are integrated with

agency strategic and operational planning processes;

"(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 the officials, including through—

"(A) assessing, with a frequency commensurate with risk, the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information or information systems;

"(B) determining the levels of information security appropriate to protect the information and information systems in accordance with the policies and directives issued under section 3553(b) and standards prescribed under section 11331 of title 40;

"(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

"(D) security testing and evaluation, including continuously monitoring the effective implementation of information security controls and techniques, threats, vulnerabilities, assets,

and other aspects of information security as appropriate; and

"(E) reporting information about information security incidents, threats, and vulnerabilities in a timely manner as required under policies and procedures established under subsection (b)(7);

"(3) assess and maintain the resiliency of information systems critical to the mission and operations of the agency;

"(4) delegate to the chief information officer or equivalent official (or to a senior agency official who reports to the chief information officer or equivalent official) the authority to ensure and primary responsibility for ensuring compliance with this subchapter, including—

"(A) overseeing the establishment and maintenance of an agencywide security operations capability that on a continuous basis can—

"(i) detect, report, respond to, contain, and mitigate information security incidents that impair adequate security of the agency information and information systems in a timely manner and in accord-

ance with the policies and directives issued under section 3553(b); and

"(ii) report any information security incident described under clause (i) to the entity designated under section 3553(b)(6);

"(B) developing, maintaining, and overseeing an agencywide information security program as required under subsection (b);

"(C) developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 and section 11331 of title 40;

"(D) training and overseeing employees and contractors of the agency with significant responsibilities for information security with respect to such responsibilities; and

"(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

"(5) the agency has trained and obtained security clearances for an adequate number of employees to assist the agency in complying with this subchapter, including the policies and directives issued under section 3553(b);

"(6) ensure that the chief information officer (or other senior agency official designated under paragraph (4)), in coordination with other senior agency officials, reports to the head of the agency on the effectiveness of the agency information security program, including the progress of remedial actions;

"(7) ensure that the chief information officer (or other senior agency official designated under paragraph (4))—

"(A) possesses the necessary qualifications to administer the duties of the official under this subchapter; and

"(B) has information security duties as a primary duty of the official; and

"(8) ensure that senior agency officials (including component chief information officers or equivalent officials) carry out responsibilities under this subchapter as directed by the official delegated authority under paragraph (4).

"(b) AGENCY PROGRAM.—The head of each agency shall develop, document, and implement an agencywide information security program, which shall be reviewed under section 3553(b)(2), 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, which shall include—

"(1) the development, execution, and maintenance of a risk management strategy for information security that—

"(A) considers information security threats, vulnerabilities, and consequences;

"(B) includes periodic assessments and reporting of risk, with a frequency commensurate with risk and impact;

"(2) policies and procedures that—

"(A) are based on the risk management strategy and assessment results required under paragraph (1);

"(B) reduce information security risks to an acceptable level in a cost-effective manner;

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

"(D) ensure compliance with—

"(i) this subchapter;

"(ii) the information security policies and directives issued under section 3553(b); and

"(iii) any other applicable requirements;

"(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;

"(4) security awareness training developed in accordance with the requirements issued under section 3553(b) to inform individuals with access to agency information systems, including information security employees, contractors, and other users of information systems that support the operations and assets of the agency, of—

"(A) information security risks associated with their activities;

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

"(C) requirements for fulfilling privacy, civil rights, civil liberties, and other information oversight responsibilities; and

"(D) methods for individuals to report risks and incidents to relevant Offices of Inspectors General and the Secretary under section 106 of the Cybersecurity Act of 2012;

"(5) security testing and evaluation commensurate with risk and impact that includes—

"(A) risk-based continuous monitoring of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of management, operational, and technical controls of information systems identified in the inventory required under section 3505(c);

"(B) penetration testing exercises and operational evaluations in accordance with the requirements issued under section 3553(b) to evaluate whether the agency adequately protects against, detects, and responds to incidents;

"(C) vulnerability scanning, intrusion detection and prevention, and penetration testing, in accordance with the requirements issued under section 3553(b); and

"(D) any other periodic testing and evaluation, in accordance with the requirements issued under section 3553(b);

"(6) a process for ensuring that remedial actions are taken to mitigate information security

vulnerabilities commensurate with risk and impact, and otherwise address any deficiencies in the information security policies, procedures, and practices of the agency;

"(7) policies and procedures to ensure detection, mitigation, reporting, and responses to information security incidents, in accordance with the policies and directives issued under section 3553(b), including—

"(A) ensuring timely internal reporting of information security incidents;

"(B) establishing and maintaining appropriate technical capabilities to detect and mitigate risks associated with information security incidents;

"(C) notifying and consulting with the entity designated by the Secretary under section 3553(b)(6); and

"(D) notifying and consulting with—

"(i) law enforcement agencies and relevant Offices of Inspectors General;

"(ii) relevant committees of Congress, as appropriate; and

"(iii) any other entity, in accordance with law and as directed by the President; and

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

"(c) ANNUAL AGENCY REPORTING.—The head of each agency shall—

"(1) report annually to the Committee on Government Reform and the Committee on Science, Space, and Technology of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, any other appropriate committees of Congress, and the Secretary on the adequacy and effectiveness of information security policies, procedures, and practices, including—

"(A) a description of each major information security incident, or set of related incidents, resulting in significant compromise of information security, including a summary of—

"(i) the threats, vulnerabilities, and impact of the incident;

"(ii) the system risk assessment conducted before the incident and required under section 3554(a)(2); and

"(iii) the detection and response actions taken;

"(B) the number of information security incidents within the agency resulting in significant compromise of information security, presented by system impact level, type of incident, and location;

"(C) the total number of information security incidents within the agency, presented by system impact level, type of incident, and location;

"(D) an identification and analysis of, including actions and plans to address, any significant deficiencies identified in such policies, procedures and practices;

"(E) any information or evaluation required under the reporting requirements issued under section 3553(b); and

"(2) address the adequacy and effectiveness of the information security policies, procedures, and practices of the agency as required for management and budget plans and reports, as appropriate.

"(d) COMMUNICATIONS AND SYSTEM TRAFFIC.—Notwithstanding any other provision of law, the head of each agency is authorized to allow the Secretary, or a private entity providing assistance to the Secretary under section 3553, to acquire, intercept, retain, use, and disclose communications, system traffic, records, or other information transiting to or from or stored on an agency information system for the purpose of protecting agency information and information systems from information security threats or mitigating the threats in connection with the implementation of the information security capabilities authorized by paragraph (3) or (4) of section 3553(b).

"§ 3555. Annual assessments

"(a) IN GENERAL.—Except as provided in subsection (c), the Secretary shall conduct periodic assessments of the information security programs and practices of agencies based on the annual agency reports required under section 3554(c), the annual independent evaluations required under section 3556, the results of any continuous monitoring, and other available information.

"(b) CONTENTS.—Each assessment conducted under subsection (a) shall—

"(1) assess the effectiveness of agency information security policies, procedures, and practices;

"(2) provide an assessment of the status of agency information system security for the Federal Government as a whole; and

"(3) include recommendations for improving information system security for an agency or the Federal Government as a whole.

"(c) CERTAIN INFORMATION SYSTEMS.—

"(1) NATIONAL SECURITY SYSTEMS.—A periodic assessment conducted under subsection (a) relating to a national security system shall be prepared as directed by the President.

"(2) SPECIFIC AGENCIES.—Periodic assessments conducted under subsection (a) shall be prepared in accordance with governmentwide reporting requirements by—

"(A) the Secretary of Defense for information systems under the control of the Department of Defense;

"(B) the Director of the Central Intelligence Agency for information systems under the control of the Central Intelligence Agency; and

"(C) the Director of National Intelligence for information systems under the control of

the Office of the Director of National Intelligence.

"(d) AGENCY-SPECIFIC ASSESSMENTS.—Each assessment conducted under subsection (a) that relates, in whole or in part, to the information systems of an agency shall be made available to the head of the agency.

"(e) PROTECTION OF INFORMATION.—In conducting assessments under subsection (a), the Secretary shall take appropriate actions to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and policies.

"(f) REPORT TO CONGRESS.—The Secretary, in coordination with the Secretary of Defense, the Director of the Central Intelligence Agency, and the Director of National Intelligence, shall evaluate and submit to Congress an annual report on the adequacy and effectiveness of the information security programs and practices assessed under this section.

"§ 3556. Independent evaluations

"(a) IN GENERAL.—Not less than annually, an independent evaluation of the information security program and practices of each agency shall be performed to assess the effectiveness of the programs and practices.

"(b) CONTENTS.—Each evaluation performed under subsection (a) shall include—

"(1) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the information systems of the agency; and

"(2) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

"(c) CONDUCT OF INDEPENDENT EVALUATIONS.—Except as provided in subsection (f), an evaluation of an agency under subsection (a) shall be performed by—

"(1) the Inspector General of the agency;

"(2) at the discretion of the Inspector General of the agency, an independent entity entering a contract with the Inspector General to perform the evaluation; or

"(3) if the agency does not have an Inspector General, an independent entity selected by the head of the agency, in consultation with the Secretary.

"(d) PREVIOUSLY CONDUCTED EVALUATIONS.—The evaluation required by this section may be based in whole or in part on a previously conducted audit, evaluation, or report relating to programs or practices of the applicable agency.

"(e) REPORTS.—The official or entity performing an evaluation of an agency under subsection (a) shall submit to Congress, the agency, and the Comptroller General of the United States a report regarding the evaluation. The head of the agency shall provide to the Secretary a report received under this subsection.

"(f) NATIONAL SECURITY SYSTEMS.—An evaluation under subsection (a) of a national security system shall be performed as directed by the President.

"(g) COMPTROLLER GENERAL.—The Comptroller General of the United States shall periodically evaluate and submit to Congress reports on—

"(1) the adequacy and effectiveness of the information security policies and practices of agencies; and

"(2) implementation of this subchapter.

"§ 3557. National security systems

"The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

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

information contained in the national security system;

"(2) implements information security policies and practices as required by standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

"(3) complies with this subchapter.

"§ 3558. Effect on existing law

"Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over the agency.".

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 35 of title 44 is amended by striking the matter relating to subchapters II and III and inserting the following:

"SUBCHAPTER II—INFORMATION SECURITY

"Sec. 3551. Purposes.
"Sec. 3552. Definitions.
"Sec. 3553. Federal information security authority and coordination.
"Sec. 3554. Agency responsibilities.
"Sec. 3555. Annual assessments.
"Sec. 3556. Independent evaluations.
"Sec. 3557. National security systems.
"Sec. 3558. Effect on existing law.".

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

"§ 11331. Responsibilities for Federal information systems standards

"(a) DEFINITIONS.—In this section:

"(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another entity on behalf of an executive agency.

"(2) INFORMATION SECURITY.—The term 'information security' has the meaning given that term in section 3552 of title 44.

"(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given that term in section 3552 of title 44.

"(b) STANDARDS AND GUIDELINES.—

"(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), and based on the standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), the Secretary of Commerce, in consultation with the Secretary of Homeland Security, shall prescribe standards and guidelines relating to Federal information systems.

"(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and over-

seen as otherwise authorized by law and as directed by the President.

"(c) MANDATORY REQUIREMENTS.—

"(1) AUTHORITY TO MAKE MANDATORY.—The Secretary of Commerce may require executive agencies to comply with the standards prescribed under subsection (b)(1) to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

"(2) REQUIRED MANDATORY STANDARDS.—

"(A) IN GENERAL.—The Secretary of Commerce shall require executive agencies to comply with the standards described in subparagraph (B).

"(B) CONTENTS.—The standards described in this subparagraph are information security standards that—

"(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

"(ii) are otherwise necessary to improve the security of Federal information and Federal information systems.

"(d) AUTHORITY TO DISAPPROVE OR MODIFY.—The President may disapprove or modify the standards and guidelines prescribed under subsection (b)(1) if the President determines such action to be in the public interest. The authority of the President to disapprove or modify the standards and guidelines may be delegated to the Director of the Office of Management and Budget. Notice of a disapproval or modification under this subsection shall be published promptly in the Federal Register. Upon receiving notice of a disapproval or modification, the Secretary of Commerce shall immediately rescind or modify the standards or guidelines as directed by the President or the Director of the Office of Management and Budget.

"(e) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority under this section subject to direction by the President and in coordination with the Director of the Office of Management and Budget.

"(f) APPLICATION OF MORE STRINGENT STANDARDS.—The head of an executive agency may employ standards for the cost-effective information security for Federal information systems of that agency that are more

stringent than the standards prescribed by the Secretary of Commerce under subsection (b)(1) if the more stringent standards—

"(1) contain any standards with which the Secretary of Commerce has required the agency to comply; and

"(2) are otherwise consistent with the policies and directives issued under section 3553(b) of title 44.

"(g) DECISIONS ON PROMULGATION OF STANDARDS.—The decision by the Secretary of Commerce regarding the promulgation of any standard under this section shall occur not later than 6 months after the submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).".

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) Section 3502(8)) of title 44, United States Code, is amended by inserting "hosting," after "collection,".

(2) The National Institute of Standards and Technology Act (15 U.S.C. 271 et seq.) is amended—

(A) in section 20(a)(2) (15 U.S.C. 278g–3(a)(2)), by striking ''section 3532(b)(2)'' and inserting ''section 3552(b)''; and

(B) in section 21(b) (15 U.S.C. 278g–4(b))—

(i) in paragraph (2), by inserting '', the Secretary of Homeland Security,'' after ''the Institute''; and

(ii) in paragraph (3), by inserting ''the Secretary of Homeland Security,'' after ''the Secretary of Commerce,''.

(3) 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 3552(b)''.

(4) Part IV of title 10, United States Code, is amended—

(A) in section 2222(j)(5), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)'';

(B) in section 2223(c)(3), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''; and

(C) in section 2315, by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(5) 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 3554(b)''.

SEC. 203. SAVINGS PROVISIONS.

(a) IN GENERAL.—Policies and compliance guidance issued by the Director of the Office of Management and Budget before the date of enactment of this Act under section 3543(a)(1) of title 44 (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed under section 3553(b)(1) of title 44, as added by this Act.

(b) OTHER STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director of the Office of Management and Budget before the date of enactment of this Act under section 11331(b)(1) of title 40 (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed under section 11331(b)(1), as added by this Act.

SEC. 204. CONSOLIDATION OF EXISTING DEPARTMENTAL CYBER RESOURCES AND AUTHORITIES.

(a) IN GENERAL.—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) AGENCY INFORMATION INFRASTRUCTURE.—The term 'agency information infrastructure' means the Federal information infrastructure of a particular Federal agency.

''(2) CENTER.—The term 'Center' means the National Center for Cybersecurity and Communications established under section 242.

''(3) DAMAGE.—The term 'damage' has the meaning given that term in section 1030(e) of title 18, United States Code.

''(4) FEDERAL AGENCY.—The term 'Federal agency' has the meaning given the term 'agency' in section 3502 of title 44, United States Code.

''(5) FEDERAL CYBERSECURITY CENTER.—The term 'Federal cybersecurity center' has the meaning given that term in section 708 of the Cybersecurity Act of 2012.

"(6) FEDERAL ENTITY.—The term 'Federal entity' has the meaning given that term in section 708 of the Cybersecurity Act of 2012.

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

"(A) means information and information systems that are owned, operated, controlled, or licensed solely 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 and information systems that are owned, operated, controlled, or licensed for use solely by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community.

"(8) INCIDENT.—The term 'incident' has the meaning given that term in section 3552 of title 44, United States Code.

"(9) INFORMATION SECURITY.—The term 'information security' has the meaning given that term in section 3552 of title 44, United States Code.

"(10) INFORMATION SYSTEM.—The term 'information system' has the meaning given that term in section 3502 of title 44, United States Code.

"(11) INTELLIGENCE COMMUNITY.—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)).

"(12) NATIONAL SECURITY AND EMERGENCY PREPAREDNESS COMMUNICATIONS INFRASTRUCTURE.—The term 'national security and emergency preparedness communications infrastructure' means the systems supported or covered by the Office of Emergency Communications and the National Communications System on the date of enactment of the Cybersecurity Act of 2012 or otherwise described in Executive Order 12472, or any successor thereto, relating to national security and emergency preparedness communications functions.

"(13) NATIONAL INFORMATION INFRASTRUCTURE.—The term 'national information infrastructure' means information and information systems—

"(A) that are owned, operated, or controlled, in whole or in part, within or from the United States; and

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

"(14) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given that term in section 3552 of title 44, United States Code.

"(15) NON-FEDERAL ENTITY.—The term 'non-Federal entity' has the meaning given that term in section 708 of the Cybersecurity Act of 2012.

"SEC. 242. CONSOLIDATION OF EXISTING RESOURCES.

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

"(b) TRANSFER OF FUNCTIONS.—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.

"(c) DIRECTOR.—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, and who shall report directly to the Secretary.

"(d) DUTIES.—The Director of the Center shall—

"(1) manage Federal efforts to secure, protect, and ensure the resiliency of the Federal information infrastructure, national information infrastructure, and national security and emergency preparedness communications infrastructure of the United States, working cooperatively with appropriate government agencies and the private sector;

"(2) support private sector efforts to secure, protect, and ensure the resiliency of the national information infrastructure;

"(3) prioritize the efforts of the Center to address the most significant risks and incidents that have caused or are likely to cause damage to the Federal information infrastructure, the national information infrastructure, and national security and emergency preparedness communications infrastructure of the United States;

"(4) ensure, in coordination with the privacy officer designated under subsection (j), 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; and

"(5) perform such other duties as the Secretary may require relating to the security and resiliency of the Federal information infrastructure, national information infrastructure, and the national security and emergency preparedness communications infrastructure of the United States.

"(e) AUTHORITIES AND RESPONSIBILITIES OF CENTER.—The Center shall—

"(1) engage in activities and otherwise coordinate Federal efforts to identify, protect against, remediate, and mitigate, respond to, and recover from cybersecurity threats, consequences, vulnerabilities and incidents impacting the Federal information infrastructure and the national information infrastructure, including by providing support to entities that own or operate national information infrastructure, at their request;

"(2) conduct risk-based assessments of the Federal information infrastructure, and risk assessments of critical infrastructure;

"(3) develop, oversee the implementation of, and enforce policies, principles, and guidelines on information security for the Federal information infrastructure, including exercise of the authorities under the Federal Information Security Management Act of 2002 (title III of Public Law 107–347; 116 Stat. 2946);

"(4) evaluate and facilitate the adoption of technologies designed to enhance the protection of information infrastructure, including making such technologies available to entities that own or operate national information infrastructure, with or without reimbursement, as necessary to accomplish the purposes of this section;

"(5) oversee the responsibilities related to national security and emergency preparedness communications infrastructure, including the functions of the Office of Emergency Communications and the National Communications System;

"(6)(A) maintain comprehensive situational awareness of the security of the Federal information infrastructure and the national information infrastructure for the purpose of enabling and supporting activities under subparagraph (e)(1); and

"(B) receive and distribute classified and unclassified information from and to entities that own or operate national information infrastructure to support efforts by such entities to secure such infrastructure and for enhancing overall situational awareness;

"(7) serve as the focal point for, and foster collaboration between, the Federal Government, State and local governments, and private entities on matters relating to the security of the national information infrastructure;

"(8) 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, and coordinate national cyber incident response efforts;

"(9) consult, in coordination with the Secretary of State, 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;

"(10) coordinate the activities undertaken by Federal agencies to—

"(A) protect Federal information infrastructure and national information infrastructure; and

"(B) prepare the Nation to respond to, recover from, and mitigate against risks of incidents involving such infrastructure; and

"(11) perform such other duties as the Secretary may require relating to the security and resiliency of the Federal information infrastructure, national information infrastructure, and national security and emergency preparedness communications infrastructure of the United States.

"(f) USE OF EXISTING MECHANISMS FOR COLLABORATION.—To avoid unnecessary duplication or waste, in carrying out the authorities and responsibilities of the Center under this subtitle, to the maximum extent practicable, the Director of the Center shall make use of existing mechanisms for collaboration and information sharing, including mechanisms relating to the identification and communication of cybersecurity threats, vulnerabilities, and associated consequences, established by other compo-

nents of the Department or other Federal agencies and the information sharing mechanisms established under title VII of the Cybersecurity Act of 2012.

"(g) DEPUTY DIRECTORS.—

"(1) IN GENERAL.—There shall be a Deputy Director appointed by the Secretary, who shall—

"(A) have expertise in infrastructure protection; and

"(B) ensure that 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.

"(2) INTELLIGENCE COMMUNITY.—The Director of National Intelligence, with the concurrence of the Secretary, 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 of the Center and the Director of National Intelligence, and, while serving as Deputy Director, shall report directly to the Director of the Center.

"(h) CYBERSECURITY EXERCISE PROGRAM.—The Director of the Center shall develop and implement a national cybersecurity exercise program with the participation of State and local governments, international partners of the United States, and the private sector.

"(i) LIAISON OFFICERS.—

"(1) REQUIRED DETAIL OF LIAISON OFFICERS.—The Secretary of Defense, the Attorney General, the Secretary of Commerce, and the Director of National Intelligence shall assign personnel to the Center to act as full-time liaisons.

"(2) OPTIONAL DETAIL OF LIAISON OFFICERS.—The head of any Federal agency not described in paragraph (1), with the concurrence of the Director of the Center, may assign personnel to the Center to act as liaisons.

"(3) PRIVATE SECTOR LIAISON.—The Director of the Center shall designate not less than 1 employee of the Center to serve as a liaison with the private sector.

"(j) PRIVACY OFFICER.—The Director of the Center, in consultation with the Secretary, shall designate a full-time privacy officer.

"(k) SUFFICIENCY OF RESOURCES PLAN.—

"(1) REPORT.—Not later than 120 days after the date of enactment of the Cybersecurity Act of 2012, 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, including the availability of existing resources and staff.

"(2) COMPTROLLER GENERAL REVIEW.—The Comptroller General of the United States shall evaluate the reasonableness and adequacy of the report submitted by the Director of the Office of Management and Budget under paragraph (1) and submit to the appropriate committees of Congress a report regarding the same.

"(l) NO RIGHT OR BENEFIT.—The provision of assistance or information under this section to governmental or private entities that own or operate critical infrastructure shall be at the discretion of the Secretary. The provision of certain assistance or information to a governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

"SEC. 243. DEPARTMENT OF HOMELAND SECURITY INFORMATION SHARING.

''(a) INFORMATION SHARING.—The Director of the Center shall establish procedures to—

''(1) ensure the appropriate, regular, and timely sharing of classified and unclassified cybersecurity information, including information relating to threats, vulnerabilities, traffic, trends, incidents, and other anomalous activities that affect the Federal information infrastructure, national information infrastructure, or information systems between and among appropriate Federal and non-Federal entities, including Federal cybersecurity centers, Federal and non-Federal network and security operations centers, cybersecurity exchanges, and non-Federal entities responsible for such information systems;

''(2) expand and enhance the sharing of timely and actionable cybersecurity threat and vulnerability information by the Federal Government with owners and operators of the national information infrastructure;

''(3) establish a method of accessing classified or unclassified information, as appropriate and in accordance with applicable laws protecting trade secrets, that will provide situational awareness of the security of the Federal information infrastructure

and the national information infrastructure relating to cybersecurity threats, and vulnerabilities, including traffic, trends, incidents, damage, and other anomalous activities affecting the Federal information infrastructure or the national information infrastructure;

''(4) develop, in consultation with the Attorney General, the Director of National Intelligence, and the privacy officer established under section 242(j), guidelines to protect the privacy and civil liberties of United States persons and intelligence sources and methods, while carrying out this subsection; and

''(5) ensure, to the extent necessary, that any information sharing under this section is consistent with title VII of the Cybersecurity Act of 2012.

''(b) VOLUNTARILY SHARED INFORMATION.—

''(1) IN GENERAL.—The Director of the Center shall ensure that information submitted in accordance with this section by States and units of local governments, private entities, and international partners of the United States regarding threats, vulnerabilities, incidents, and anomalous activities affecting the national information infrastructure, Federal information infrastructure, or information infrastructure that is owned, operated, controlled, or

licensed solely for use by, or on behalf of, the Department of Defense, a military department, or another element of the intelligence community is treated as voluntarily shared critical infrastructure information under section 214 as requested by submitting entities.

"(2) LIMITATION.—Paragraph (1) shall not apply to information that 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.

"(e) LIMITATION ON USE OF VOLUNTARILY SUBMITTED INFORMATION FOR REGULATORY ENFORCEMENT ACTIONS.—A Federal entity may not use information submitted under this subtitle as evidence in a regulatory enforcement action against the individual or entity that lawfully submitted the information.

"(d) FEDERAL AGENCIES.—

"(1) INFORMATION SHARING PROGRAM.—The Director of the Center, in consultation with the members of the Chief Information Officers Council established under section 3603 of title 44, United

States Code, shall establish a program for sharing information with and between the Center and other Federal agencies that includes processes and procedures—

"(A) under which the Director of the Center regularly shares with each Federal agency analyses and reports regarding the security of such agency information infrastructure and on the overall security 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 means and methods of preventing, responding to, mitigating, and remediating cybersecurity threats and vulnerabilities; and

"(B) under which Federal agencies provide the Director of the Center, upon request, with information 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 of the Center under this subtitle or any other provision of law.

''(2) ACCESS TO INFORMATION.—

''(A) IN GENERAL.—The Director of the Center shall ensure—

''(i) that the head of each Federal agency has timely access to data, including appropriate raw and processed data, regarding the information infrastructure of the Federal agency; and

''(ii) to the greatest extent possible, that the head of each Federal agency is kept apprised of common trends in security compliance as well as the likelihood that a significant cybersecurity risk or incident could cause damage to the agency information infrastructure.

''(B) COMPLIANCE.—The head of a Federal agency shall comply with all processes and procedures established under this subsection regarding notification to the Director of the Center relating to incidents.

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

"SEC. 244. PROHIBITED CONDUCT.

"None of the authorities provided under this subtitle shall authorize the Director of the Center, the Center, the Department, or any other Federal entity to—

"(1) compel the disclosure of information from a private entity relating to an incident unless otherwise authorized by law; or

"(2) 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, or

the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—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 inserting after the item relating to section 237 the following:

''Subtitle E—Cybersecurity

''Sec. 241. Definitions.
''Sec. 242. Consolidation of existing resources.
''Sec. 243. Department of Homeland Security information sharing.
''Sec. 244. Prohibited conduct.''.

TITLE III—RESEARCH AND DEVELOPMENT

SEC. 301. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) FUNDAMENTAL CYBERSECURITY RESEARCH.—The Director of the Office of Science and Technology Policy (referred to in this section as the ''Director''), in coordination with the Secretary and the head of any relevant Federal agency, shall build upon programs and plans in effect as of the date of enactment of this Act to develop a national cybersecurity research and development plan, which shall be updated biennially.

(b) REQUIREMENTS.—The plan required to be developed under subsection (a) shall encourage computer and

information science and engineering research to meet challenges in cybersecurity, including—

(1) how to design and build complex software-intensive systems that are secure and reliable when first deployed;

(2) how to test and verify that software, whether developed locally or obtained from a third party, is free of significant known security flaws;

(3) how to test and verify that software obtained from a third party correctly implements stated functionality, and only that functionality;

(4) how to guarantee the privacy of the identity, information, or lawful transactions of an individual when stored in distributed systems or transmitted over networks;

(5) how to build new protocols to enable the Internet to have robust security as one of the key capabilities of the Internet;

(6) how to determine the origin of a message transmitted over the Internet;

(7) how to support privacy in conjunction with improved security;

(8) how to address the growing problem of insider threat;

(9) how improved consumer education and digital literacy initiatives can address human factors that contribute to cybersecurity;

(10) how to protect information stored through cloud computing or transmitted through wireless services;

(11) conducting research in the areas described in section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)), as amended by subsection (f); and

(12) any additional objectives the Director or Secretary determines appropriate.

(c) CYBERSECURITY PRACTICES RESEARCH.—The Director of the National Science Foundation shall support research—

(1) that develops, evaluates, disseminates, and integrates new cybersecurity practices and concepts into the core curriculum of computer science programs and of other programs where graduates of such programs have a substantial probability of developing software after graduation, including new practices and concepts relating to secure coding education and improvement programs; and

(2) that develops new models for professional development of faculty in cybersecurity education, including secure coding development.

(d) CYBERSECURITY MODELING AND TEST BEDS.—

(1) REVIEW.—Not later than 1 year after the date of enactment of this Act, the Director shall conduct a review of cybersecurity test beds in existence on the date of enactment of this Act to inform the program established under paragraph (2).

(2) ESTABLISHMENT OF PROGRAM.—

(A) IN GENERAL.—The Director of the National Science Foundation, the Secretary, and the Secretary of Commerce shall establish a program for the appropriate Federal agencies to award grants to institutions of higher education or research and development non-profit institutions to establish cybersecurity test beds capable of realistic modeling of real-time cyber attacks and defenses.

(B) REQUIREMENT.—The test beds established under subparagraph (A) shall be sufficiently large in order to model the scale and complexity of real world networks and environments.

(3) PURPOSE.—The purpose of the program established under paragraph (2) shall be to support the rapid development of new cybersecurity defenses, techniques, and processes by improving understanding and assessing the latest technologies in a real-world environment.

(e) COORDINATION WITH OTHER RESEARCH INITIATIVES.—The Director shall to the extent practicable, coordinate research and development activities under this section with other ongoing research and development security-related initiatives, including research being conducted by—

(1) the National Institute of Standards and Technology;

(2) the Department;

(3) other Federal agencies;

(4) other Federal and private research laboratories, research entities, and universities and institutions of higher education, and relevant nonprofit organizations; and

(5) international partners of the United States.

(f) NSF COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking "and" at the end;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

"(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

"(K) secure software engineering and software assurance, including—

"(i) programming languages and systems that include fundamental security features;

"(ii) portable or reusable code that remains secure when deployed in various environments;

"(iii) verification and validation technologies to ensure that requirements and specifications have been implemented; and

"(iv) models for comparison and metrics to assure that required standards have been met;

"(L) holistic system security that—

"(i) addresses the building of secure systems from trusted and untrusted components;

"(ii) proactively reduces vulnerabilities;

"(iii) addresses insider threats; and

"(iv) supports privacy in conjunction with improved security;

"(M) monitoring and detection;

"(N) mitigation and rapid recovery methods;

"(O) security of wireless networks and mobile devices; and

"(P) security of cloud infrastructure and services.".

(g) CYBERSECURITY FACULTY DEVELOPMENT TRAINEESHIP PROGRAM.—Section 5(e)(9) of the Cyber Security Research and Development Act (15 U.S.C. 7404(e)(9)) is amended by striking "2003 through 2007" and inserting "2012 through 2014".

(h) NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM.—Section 204(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5524(a)(1)) is amended—

(1) in subparagraph (B), by striking ''and'' at the end; and

(2) by adding at the end the following:

''(D) develop and propose standards and guidelines, and develop measurement techniques and test methods, for enhanced cybersecurity for computer networks and common user interfaces to systems; and''.

SEC. 302. HOMELAND SECURITY CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—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, test beds, 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 tech-

nologies 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 for Science and Technology—

''(1) shall ensure that the research and development program carried out under subsection (a) is consistent with any strategy to increase the security and resilience of cyberspace;

''(2) shall, to the extent practicable, coordinate the research and development activities of the Department with other ongoing research and develop-

ment 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;

"(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, 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.".

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.), as amended by section 204, is amended by inserting after the item relating to section 237 the following:

"Sec. 238. Cybersecurity research and development.".

SEC. 303. RESEARCH CENTERS FOR CYBERSECURITY.

(a) ESTABLISHMENT.—Not later than 1 year after the date of enactment of this Act, the Director of the National Science Foundation, in coordination with the Secretary, shall establish cybersecurity research centers based at institutions of higher education and other entities that meet the criteria described in subsection (b) to develop solutions and strategies that support the efforts of the Federal government under this Act in—

(1) improving the security and resilience of information infrastructure;

(2) reducing cyber vulnerabilities; and

(3) mitigating the consequences of cyber attacks on critical infrastructure.

(b) CRITERIA FOR SELECTION.—In selecting an institution of higher education or other entity to serve as a Research Center for Cybersecurity, the Director of the National Science Foundation shall consider—

(1) demonstrated expertise in systems security, wireless security, networking and protocols, formal methods and high-performance computing, nanotechnology, and industrial control systems;

(2) demonstrated capability to conduct high performance computation integral to complex cybersecurity research, whether through on-site or off-site computing;

(3) demonstrated expertise in interdisciplinary cybersecurity research;

(4) affiliation with private sector entities involved with industrial research described in paragraph (1) and ready access to testable commercial data;

(5) prior formal research collaboration arrangements with institutions of higher education and Federal research laboratories;

(6) capability to conduct research in a secure environment; and

(7) affiliation with existing research programs of the Federal Government.

SEC. 304. CENTERS OF EXCELLENCE.

The Secretary and the Secretary of Defense may jointly establish academic and professional Centers of Excellence in cybersecurity for the protection of critical infrastructure in conjunction with international academic and professional partners from countries that may include allies of the United States, as determined to be appropriate under title XIX of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53; 121 Stat. 505) in order to research and develop technologies, best practices, and other means to defend critical infrastructure.

TITLE IV—EDUCATION, WORKFORCE, AND AWARENESS

SEC. 401. DEFINITIONS.

In this title:

(1) CYBERSECURITY MISSION.—The term ''cybersecurity mission'' means activities 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) CYBERSECURITY MISSION OF A FEDERAL AGENCY.—The term ''cybersecurity mission of a Federal agency'' means the portion of a cybersecurity mission that is the responsibility of a Federal agency.

SEC. 402. EDUCATION AND AWARENESS.

(a) ASSESSMENT OF CYBERSECURITY EDUCATION IN COLLEGES AND UNIVERSITIES.—

(1) REPORT.—Not later than 1 year after the date of enactment of this Act, the Director of the National Science Foundation shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives a report on the state of cybersecurity education in institutions of higher education in the United States.

(2) CONTENTS OF REPORT.—The report required under paragraph (1) shall include baseline data on—

(A) the state of cybersecurity education in the United States;

(B) the extent of professional development opportunities for faculty in cybersecurity principles and practices;

(C) descriptions of the content of cybersecurity courses in undergraduate computer science curriculum;

(D) the extent of the partnerships and collaborative cybersecurity curriculum development activities that leverage industry and government needs, resources, and tools; and

(E) proposed metrics to assess progress toward improving cybersecurity education.

(b) ENRICHMENT PROGRAMS.—The Director of the National Science Foundation shall—

(1) encourage and support programming, including summer enrichment programs, to be provided by nonprofit organizations, in math, computer programming, science, technology, and engineering, with a goal of increasing cybersecurity skills in students enrolled in kindergarten through grade 12; and

(2) when appropriate, provide opportunities for top-achieving students to participate in the programs described in paragraph (1) at no cost.

(c) NATIONAL EDUCATION AND AWARENESS CAMPAIGN.—The Secretary, in consultation with appropriate Federal agencies shall develop and implement outreach and awareness programs on cybersecurity, including—

(1) in consultation with the Director of the National Institute of Standards and Technology—

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

(B) an education campaign to increase the understanding of State and local governments and private sector entities of the benefits of ensuring effective risk management of the information infrastructure versus the costs of failure to do so and methods to mitigate and remediate vulnerabilities;

(2) in coordination with the Secretary of Commerce, development of a program to publicly recognize or identify products, services, and companies, including owners and operators, that meet the highest standards of cybersecurity; and

(3) in accordance with subsection (d), a program for carrying out collaborative education and

training activities for cybersecurity through a consortium or other appropriate entity.

(d) COLLABORATIVE EDUCATION AND TRAINING.—

(1) IN GENERAL.—The consortium or other entity established under subsection (c)(3) shall—

(A) provide training to State and local first responders and officials specifically for preparing and responding to cyber attacks;

(B) develop and update a curriculum and training models for State and local first responders and officials;

(C) provide technical assistance services to build and sustain capabilities in support of cybersecurity preparedness and response; and

(D) conduct cybersecurity training and simulation exercises to defend from and respond to cyber attacks.

(2) MEMBERS.—The Consortium or other entity established under subsection (c)(3) shall consist of academic, nonprofit, Federal Government, and State and local government partners that develop, update, and deliver cybersecurity training in support of homeland security.

(e) CONSIDERATIONS.—In carrying out the authority described in subsection (c), the Secretary of Commerce,

the Secretary, and the Director of the National Institute of Standards and Technology shall leverage existing programs designed to inform the public of safety and security of products or services, including self-certifications and independently-verified assessments regarding the quantification and valuation of information security risk.

SEC. 403. NATIONAL CYBERSECURITY COMPETITION AND CHALLENGE.

(a) TALENT COMPETITION AND CHALLENGE.—

(1) IN GENERAL.—The Secretary and the Secretary of Commerce shall establish a program to conduct competitions and challenges and 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) PARTICIPATION.—Participants in the competitions and challenges of the program established under paragraph (1) shall include—

(A) students enrolled in grades 9 through 12;

(B) students enrolled in a postsecondary program of study leading to a baccalaureate degree at an institution of higher education;

(C) students enrolled in a postbaccalaureate program of study at an institution of higher education;

(D) institutions of higher education and research institutions;

(E) veterans; and

(F) other groups or individuals as the Secretary and the Secretary of Commerce determine appropriate.

(3) SUPPORT OF OTHER COMPETITIONS AND CHALLENGES.—The program established under paragraph (1) may support other competitions and challenges not established under this subsection through affiliation and cooperative agreements with—

(A) Federal agencies;

(B) regional, State, or school programs supporting the development of cyber professionals;

(C) State, local, and tribal governments; or

(D) other private sector organizations.

(4) AREAS OF TALENT.—The program established under paragraph (1) 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;

(F) offensive and defensive cyber operations; and

(G) other areas to fulfill the cybersecurity mission as the Secretary determines appropriate.

(5) INTERNSHIPS.—The Director of the Office of Personnel Management shall establish, in coordination with the Director of the National Center for Cybersecurity and Communications, a program to provide, where appropriate, internships or other work experience in the Federal government to the winners of the competitions and challenges.

(b) NATIONAL RESEARCH AND DEVELOPMENT COMPETITION AND CHALLENGE.—

(1) IN GENERAL.—The Director of the National Science Foundation, in consultation with appropriate Federal agencies, shall establish a program of cyber-

security competitions and challenges to stimulate innovation in basic and applied cybersecurity research, technology development, and prototype demonstration that has the potential for application to the information technology activities of the Federal Government.

(2) PARTICIPATION.—Participants in the competitions and challenges of the program established under paragraph (1) shall include—

(A) students enrolled in grades 9 through 12;

(B) students enrolled in a postsecondary program of study leading to a baccalaureate degree at an institution of higher education;

(C) students enrolled in a postbaccalaureate program of study at an institution of higher education;

(D) institutions of higher education and research institutions;

(E) veterans; and

(F) other groups or individuals as the Director of the National Science Foundation determines appropriate.

(3) TOPICS.—In selecting topics for competitions and challenges held as part of the program established under paragraph (1), the Director—

(A) shall consult widely both within and outside the Federal Government; and

(B) may empanel advisory committees.

(4) INTERNSHIPS.—The Director of the Office of Personnel Management shall establish, in coordination with the Director of the National Science Foundation, a program to provide, where appropriate, internships or other work experience in the Federal government to the winners of the competitions and challenges held as part of the program established under paragraph (1).

SEC. 404. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary, shall establish a Federal Cyber Scholarship-for-Service program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for the Federal Government and State, local, and tribal governments.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program established under subsection (a) shall—

(1) incorporate findings from the assessment and development of the strategy under section 405;

(2) provide not more than 1,000 scholarships per year, to students who are enrolled in a program of study at an institution of higher education leading to a degree or specialized program certification in the cybersecurity field, in an amount that covers each student's tuition and fees at the institution and provides the student with an additional stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to enter into an agreement under which the recipient agrees to work in the cybersecurity mission of a Federal, State, local, or tribal agency for a period equal to the length of the scholarship following receipt of the student's degree if offered employment in that field by a Federal, State, local, or tribal agency;

(4) provide a procedure by which the National Science Foundation or a Federal agency may, consistent with regulations of the Office of Personnel Management, request and fund security clearances for scholarship recipients, including providing for

clearances during summer internships and after the recipient receives the degree; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the cybersecurity mission of a Federal agency during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of individuals in the Federal civil service, upon receiving a degree for which an individual received a scholarship under this section, the individual shall be—

(A) hired under the authority provided for in section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) exempt from competitive service.

(2) COMPETITIVE SERVICE POSITION.—Upon satisfactory fulfillment of the service term of an individual hired under paragraph (1), the individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—To be eligible to receive a scholarship under this section, an individual shall—

(1) be a citizen or lawful permanent resident of the United States;

(2) demonstrate a commitment to a career in improving the security of information infrastructure; and

(3) have demonstrated a high level of proficiency in mathematics, engineering, or computer sciences.

(e) REPAYMENT.—If a recipient of a scholarship under this section does not meet the terms of the scholarship program, the recipient shall refund the scholarship payments in accordance with rules established by the Director of the National Science Foundation, in coordination with the Secretary.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall evaluate and report periodically to Congress on the success of recruiting individuals for the scholarships and on hiring and retaining those individuals in the public sector workforce.

SEC. 405. ASSESSMENT OF CYBERSECURITY FEDERAL WORKFORCE.

(a) IN GENERAL.—The Director of the Office of Personnel Management and the Secretary, in coordination with the Director of National Intelligence, the Secretary of Defense, and the Chief Information Officers Council es-

tablished under section 3603 of title 44, United States Code, 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, in consultation with the Director of the National Center for Cybersecurity and Communications 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 cybersecurity personnel of the Federal Government.

(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) a 10-year projections of Federal workforce needs.

(c) UPDATES.—The Director of the Office of Personnel Management, in consultation with the Director of the National Center for Cybersecurity and Communications and the Director of the Office of Management and

Budget, shall update the strategy developed under subsection (b) as needed.

SEC. 406. FEDERAL 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 of the National Center for Cybersecurity and Communications, 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. 407. TRAINING AND EDUCATION OF FEDERAL EMPLOYEES.

(a) DEFINITION.—In this section, the term ''agency information infrastructure'' means the Federal information infrastructure of a Federal agency.

(b) TRAINING.—

(1) FEDERAL GOVERNMENT EMPLOYEES AND FEDERAL CONTRACTORS.—The Director of the Office of Personnel Management, in coordination with

the Secretary, 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 an agency information infrastructure or the Federal information infrastructure.

(2) CONTENTS.—The curriculum established under paragraph (1) shall include, at a minimum—

(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 contractors; and

(K) the responsibilities of Federal employees and contractors 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 Secretary, 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 Ex-

ecutive Schedule, the Secretary and the Director of National Intelligence 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 3554(c) of title 44, United States Code, as amended by this Act, a certification regarding whether all employees and contractors of the Federal agency have completed the training required under this subsection.

(c) RECRUITMENT.—The Director of the Office of Personnel Management, in coordination with the Director of the National Center for Cybersecurity and Communications, shall develop strategies and programs to recruit students enrolled in institutions of higher education and students enrolled in career and technical institutions in the United States to serve as Federal employees engaged in cybersecurity missions.

(d) LEADERSHIP IN CYBERSECURITY.—The head of each Federal agency shall adopt best practices, developed by the Office of Personnel Management, 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. NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS ACQUISITION AUTHORITIES.

(a) IN GENERAL.—Subtitle E of title II of the Homeland Security Act of 2002, as added by section 204, is amended by adding at the end the following:

"SEC. 245. 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 (a)(1) and (b)(2) of section 3304 of title 41, United States Code, subject to all other requirements of sections 3301 and 3304 of title 41, United States Code.

"(b) GUIDELINES.—Not later than 90 days after the date of enactment of the Cybersecurity Act of 2012, the

chief procurement officer of the Department 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 Center 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 3304(e) of title 41, United States Code.

"(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. 246. RECRUITMENT AND RETENTION PROGRAM FOR THE NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.

"(a) DEFINITIONS.—In this section:

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

"(2) QUALIFIED EMPLOYEE.—The term 'qualified employee' means an employee who performs functions relating to the security of Federal systems and critical information infrastructure.

"(b) GENERAL AUTHORITY.—

"(1) ESTABLISH POSITIONS, APPOINT PERSONNEL, AND FIX RATES OF PAY.—The Secretary may exercise with respect to qualified employees of the Department the same authority of that the Secretary of Defense has with respect to civilian intelligence personnel under sections 1601, 1602, and 1603 of title 10, United States Code, to establish as positions in the excepted service, to appoint individuals to those positions, and fix pay. Such authority shall be exercised subject to the same conditions and limitations applicable to the Secretary of Defense with respect to civilian intelligence personnel of the Department of Defense.

"(2) SCHOLARSHIP PROGRAM.—The Secretary may exercise with respect to qualified employees of the Department the same authority of the Secretary of Defense has with respect to civilian personnel under section 2200a of title 10, United States Code, to the same extent, and subject to the same conditions and limitations, that the Secretary of Defense may exercise such authority with respect to civilian personnel of the Department of Defense.

"(3) PLAN FOR EXECUTION OF AUTHORITIES.—Not later than 120 days after the date of enactment of this subtitle, the Secretary shall submit

a report to the appropriate committees of Congress with a plan for the use of the authorities provided under this subsection.

"(4) COLLECTIVE BARGAINING AGREEMENTS.—Nothing in paragraph (1) may be construed to impair the continued effectiveness of a collective bargaining agreement with respect to an office, component, subcomponent, or equivalent of the Department that is a successor to an office, component, subcomponent, or equivalent of the Department covered by the agreement before the succession.

"(5) REQUIRED REGULATIONS.—The Secretary, in coordination with the Director of the Center and the Director of the Office of Personnel Management, shall prescribe regulations for the administration of this section.

"(c) MERIT SYSTEM PRINCIPLES AND CIVIL SERVICE PROTECTIONS: APPLICABILITY.—

"(1) APPLICABILITY OF MERIT SYSTEM PRINCIPLES.—The Secretary shall exercise the authority under subsection (b) in a manner consistent with the merit system principles set forth in section 2301 of title 5, United States Code.

"(2) CIVIL SERVICE PROTECTIONS.—Section 1221, section 2302, and chapter 75 of title 5,

United States Code, shall apply to the positions established under subsection (b)(1).

"(d) REQUIREMENTS.—Before the initial exercise of any authority authorized under subsection (b)(1) the Secretary shall—

"(1) seek input from affected employees, and the union representatives of affected employees as applicable, and Federal manager and professional associations into the design and implementation of a fair, credible, and transparent system for exercising any authority under subsection (b)(1);

"(2) make a good faith attempt to resolve any employee concerns regarding proposed changes in conditions of employment through discussions with the groups described in paragraph (1);

"(3) develop a program to provide training to supervisors of cybersecurity employees at the Department on the use of the new authorities, including actions, options, and strategies a supervisor may use in—

"(A) developing and discussing relevant goals and objectives with the employee, communicating and discussing progress relative to performance goals and objectives, and conducting performance appraisals;

"(B) mentoring and motivating employees, and improving employee performance and productivity;

"(C) fostering a work environment characterized by fairness, respect, equal opportunity, and attention to the quality of work of the employees;

"(D) effectively managing employees with unacceptable performance;

"(E) addressing reports of a hostile work environment, reprisal, or harassment of or by another supervisor or employee; and

"(F) otherwise carrying out the duties and responsibilities of a supervisor;

"(4) develop a program to provide training to supervisors of cybersecurity employees at the Department on the prohibited personnel practices under section 2302 of title 5, United States Code, (particularly with respect to the practices described in paragraphs (1) and (8) of section 2302(b) of title 5, United States Code), employee collective bargaining and union participation rights, and the procedures and processes used to enforce employee rights; and

"(5) develop a program under which experienced supervisors mentor new supervisors by—

"(A) sharing knowledge and advice in areas such as communication, critical thinking, responsibility, flexibility, motivating employees, teamwork, leadership, and professional development; and

"(B) pointing out strengths and areas for development.

"(e) SUPERVISOR REQUIREMENT.—

"(1) IN GENERAL.—Except as provided in paragraph (2), not later than 1 year after the date of enactment of the Cybersecurity Act of 2012 and every 3 years thereafter, every supervisor of cybersecurity employees at the Department shall complete the programs established under paragraphs (3) and (4) of subsection (d).

"(2) EXCEPTION.—A supervisor of cybersecurity employees at the Department who is appointed after the date of enactment of the Cybersecurity Act of 2012 shall complete the programs established under paragraphs (3) and (4) of subsection (d) not later than 1 year after the date on which the supervisor is appointed to the position, and every 3 years thereafter.

"(3) ONGOING PARTICIPATION.—Participation by supervisors of cybersecurity employees at the Department in the program established under subsection (d)(5) shall be ongoing.

"(f) CONVERSION TO COMPETITIVE SERVICE.—In consultation with the Director of the Center, the Secretary may grant competitive civil service status to a qualified employee appointed to the excepted service under subsection (b) if that employee is employed in the Center or is transferring to the Center.

"(g) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this subtitle, and every year thereafter for 4 years, the Secretary shall submit to the appropriate committees of Congress a detailed report that—

"(1) discusses the process used by the Secretary in accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by a qualified employee;

"(2) describes—

"(A) how the Secretary plans to fulfill the critical need of the Department to recruit and retain qualified employees;

"(B) the measures that will be used to measure progress; and

"(C) any actions taken during the reporting period to fulfill such critical need;

"(3) discusses how the planning and actions taken under paragraph (2) are integrated into the strategic workforce planning of the Department;

"(4) provides metrics on actions occurring during the reporting period, including—

"(A) the number of qualified employees hired by occupation and grade and level or pay band;

"(B) the total number of veterans hired;

"(C) the number of separations of qualified employees by occupation and grade and level or pay band;

"(D) the number of retirements of qualified employees by occupation and grade and level or pay band; and

"(E) the number and amounts of recruitment, relocation, and retention incentives paid to qualified employees by occupation and grade and level or pay band.".

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Se-

curity Act of 2002 (6 U.S.C. 101 et seq.), as amended by section 204, is amended by inserting after the item relating to section 244 the following:

"Sec. 245. National Center for Cybersecurity and Communications acquisition authorities.
"Sec. 246. Recruitment and retention program for the national center for cybersecurity and communications.".

SEC. 409. REPORTS ON CYBER INCIDENTS AGAINST GOVERNMENT NETWORKS.

(a) DEPARTMENT OF HOMELAND SECURITY.—Not later than 180 days after the date of enactment of this Act, and annually thereafter, the Secretary shall submit to Congress a report that—

(1) summarizes major cyber incidents involving networks of Executive agencies (as defined in section 105 of title 5, United States Code), except for the Department of Defense;

(2) provides aggregate statistics on the number of breaches of networks of Executive agencies, the volume of data exfiltrated, and the estimated cost of remedying the breaches; and

(3) discusses the risk of cyber sabotage.

(b) DEPARTMENT OF DEFENSE.—Not later than 180 days after the date of enactment of this Act, and annually thereafter, the Secretary of Defense shall submit to Congress a report that—

(1) summarizes major cyber incidents against networks of the Department of Defense and the military departments;

(2) provides aggregate statistics on the number of breaches against networks of the Department of Defense and the military departments, the volume of data exfiltrated, and the estimated cost of remedying the breaches; and

(3) discusses the risk of cyber sabotage.

(c) FORM OF REPORTS.—Each report submitted under this section shall be in unclassified form, but may include a classified annex as necessary to protect sources, methods, and national security.

(d) CONTENTS OF REPORTS.—Each report submitted under this section may be based in whole or in part on the reporting requirements under section 3553 of chapter 35 of title 44, United States Code, as amended by this Act.

SEC. 410. REPORTS ON PROSECUTION FOR CYBERCRIME.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General and the Directors of the Federal Bureau of Investigation and the United States Secret Service shall submit to Congress reports—

(1) describing investigations and prosecutions relating to cyber intrusions or other cybercrimes the preceding year, including—

(A) the number of investigations initiated relating to such crimes;

(B) the number of arrests relating to such crimes;

(C) the number and description of instances in which investigations or prosecutions relating to such crimes have been delayed or prevented because of an inability to extradite a criminal defendant in a timely manner; and

(D) the number of prosecutions for such crimes, including—

(i) the number of defendants prosecuted;

(ii) whether the prosecutions resulted in a conviction;

(iii) the sentence imposed and the statutory maximum for each such crime for which a defendant was convicted; and

(iv) the average sentence imposed for a conviction of such crimes;

(2) identifying the number of employees, financial resources, and other resources (such as tech-

nology and training) devoted to the enforcement, investigation, and prosecution of cyber intrusions or other cybercrimes, including the number of investigators, prosecutors, and forensic specialists dedicated to investigating and prosecuting cyber intrusions or other cybercrimes; and

(3) discussing any impediments under the laws of the United States or international law to prosecutions for cyber intrusions or other cybercrimes.

(b) UPDATES.—The Attorney General and the Directors of the Federal Bureau of Investigation and the United States Secret Service shall annually submit to Congress reports updating the reports submitted under subsection (a) at the same time the Attorney General and the Directors submit annual reports under section 404 of the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (42 U.S.C. 3713d).

SEC. 411. REPORT ON RESEARCH RELATING TO SECURE DOMAIN.

(a) IN GENERAL.—The Secretary shall enter into a contract with the National Research Council, or another federally funded research and development corporation, under which the Council or corporation shall submit to Congress reports on available technical options, consistent with constitutional and statutory privacy rights, for en-

hancing the security of the information networks of entities that own or manage critical infrastructure through—

(1) technical improvements, including developing a secure domain; or

(2) increased notice of and consent to the use of technologies to scan for, detect, and defeat cyber security threats, such as technologies used in a secure domain.

(b) TIMING.—The contract entered into under subsection (a) shall require that the report described in subsection (a) be submitted—

(1) not later than 180 days after the date of enactment of this Act;

(2) annually, after the first report submitted under subsection (a), for 3 years; and

(3) more frequently, as determined appropriate by the Secretary in response to new risks or technologies that emerge.

SEC. 412. REPORT ON PREPAREDNESS OF FEDERAL COURTS TO PROMOTE CYBERSECURITY.

Not later than 180 days after the date of enactment of this Act, the Attorney General, in coordination with the Administrative Office of the United States Courts, shall submit to Congress a report—

(1) on whether Federal courts have granted timely relief in matters relating to botnets and other cybercrime and cyber security threats; and

(2) that includes, as appropriate, recommendations on changes or improvements to—

(A) the Federal Rules of Civil Procedure or the Federal Rules of Criminal Procedure;

(B) the training and other resources available to support the Federal judiciary;

(C) the capabilities and specialization of courts to which such cases may be assigned; and

(D) Federal civil and criminal laws.

SEC. 413. REPORT ON IMPEDIMENTS TO PUBLIC AWARENESS.

Not later than 180 days after the date of enactment of this Act, and annually thereafter for 3 years (or more frequently if determined appropriate by the Secretary) the Secretary shall submit to Congress a report on—

(1) legal or other impediments to appropriate public awareness of—

(A) the nature of, methods of propagation of, and damage caused by common cyber security threats such as computer viruses, phishing techniques, and malware;

(B) the minimal standards of computer security necessary for responsible Internet use; and

(C) the availability of commercial off the shelf technology that allows consumers to meet such levels of computer security;

(2) a summary of the plans of the Secretary to enhance public awareness of common cyber security threats, including a description of the metrics used by the Department for evaluating the efficacy of public awareness campaigns; and

(3) recommendations for congressional actions to address these impediments to appropriate public awareness of common cyber security threats.

SEC. 414. REPORT ON PROTECTING THE ELECTRICAL GRID OF THE UNITED STATES.

Not later than 180 days after the date of enactment of this Act, the Secretary, in consultation with the Secretary of Defense and the Director of National Intelligence, shall submit to Congress a report on—

(1) the threat of a cyber attack disrupting the electrical grid of the United States;

(2) the implications for the national security of the United States if the electrical grid is disrupted;

(3) the options available to the United States and private sector entities to quickly reconstitute electrical service to provide for the national security of the United States, and, within a reasonable time frame, the reconstitution of all electrical service within the United States; and

(4) a plan to prevent disruption of the electric grid of the United States caused by a cyber attack.

SEC. 415. MARKETPLACE INFORMATION.

(a) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) registrants that file reports with the Securities and Exchange Commission have an obligation to disclose material risks to investors; and

(2) as with longstanding rules regarding other material risks, information security risks and related events that are material to investors should be disclosed on a regular basis to provide quality information to the marketplace and enable informed investor decisions.

(b) DEFINITION OF INFORMATION SECURITY RISK.—In this section, the term ''information security risk and related events'' means the risk to a registrant's business operations, assets, financial condition, strategy, competitive positioning, and reputation, due to the potential for

unauthorized access, use, disclosure, disruption, modification, or destruction of registrant information, information of third parties collected by the registrant, or information systems of the registrant.

(c) GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Securities and Exchange Commission (referred to in this section as the ''Commission'') shall evaluate existing guidance to registrants related to disclosures by registrants of information security risks and related events (including Securities and Exchange Commission Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity) to determine whether such guidance, in light of the evaluation, should be—

(1) updated by the Division of Corporation Finance; or

(2) issued as Commission interpretive guidance.

(d) ANNUAL REPORTS.—For 5 years following the evaluation under subsection (b), the Commission shall submit to Congress, on an annual basis, a report that reviews—

(1) the types of information security risks and related events that registrants disclosed in the previous year;

(2) whether the staff of the Commission has requested registrants to provide additional information on the disclosures under paragraph (1);

(3) any awareness or education activities for registrants or investors, on the subject of information security risks and related events disclosure requirements, sponsored by the Commission or attended by a Commissioner or staff of the Commission; and

(4) any public actions commenced by the Commission relating to the enforcement of disclosure requirements pertaining to the information security risks and related events.

TITLE V—FEDERAL ACQUISITION RISK MANAGEMENT STRATEGY

SEC. 501. FEDERAL ACQUISITION RISK MANAGEMENT STRATEGY.

(a) IN GENERAL.—The Secretary, in coordination with relevant private sector and academic experts and each Federal entity described in paragraphs (1) through (9) of subsection (b), shall develop and periodically update an acquisition risk management strategy designed to ensure, based on mission criticality and cost effectiveness, the security of the Federal information infrastructure.

(b) COORDINATION.—In developing the acquisition risk management strategy required under subsection (a), the Secretary shall coordinate with—

(1) the Secretary of Defense;

(2) the Secretary of Commerce;

(3) the Secretary of State;

(4) the Director of National Intelligence;

(5) the Administrator of General Services;

(6) the Administrator for Federal Procurement Policy;

(7) the members of the Chief Information Officers Council established under section 3603 of title 44, United States Code;

(8) the Chief Acquisition Officers Council established under section 1311 of title 41, United States Code; and

(9) the Chief Financial Officers Council established under section 302 of the Chief Financial Officers Act of 1990 (31 U.S.C. 901 note).

(c) ELEMENTS.—The risk management strategy developed under subsection (a) shall—

(1) address risks in the acquisition of any part of the Federal information infrastructure; and

(2) include developing processes that—

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

(B) incorporate internationally recognized standards, guidelines, and best practices, including those developed by the private sector, for supply chain integrity;

(C) enhance capabilities to test and evaluate software and hardware within or for use in the Federal information infrastructure, and, where appropriate, make the capabilities available for use by the private sector;

(D) protect the intellectual property and trade secrets of suppliers of information and communications technology products and services;

(E) share with the private sector, to the fullest extent possible, the risks identified in the supply chain and working with the private sector to mitigate those threats as identified;

(F) identify specific acquisition practices of Federal agencies that increase risks to the supply chain and develop a process to provide rec-

ommendations for revisions to those processes; and

(G) 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, consistent with the preferences for the acquisition of commercial items under section 2377 of title 10, United States Code, and section 3307 of title 41, United States Code.

SEC. 502. AMENDMENTS TO CLINGER-COHEN PROVISIONS TO ENHANCE AGENCY PLANNING FOR INFORMATION SECURITY NEEDS.

Chapter 113 of title 40, United States Code, is amended—

(1) in section 11302—

(A) in subsection (f), by striking ''technology.'' and inserting ''technology, including information technology or network information security requirements.'';

(B) in subsection (i)—

(i) by inserting '', including information security requirements,'' after ''information resources management''; and

(ii) by adding at the end the following: ''The Administrator for Federal Procurement Policy, in coordination with the Chief Information Officers Council and the Federal Acquisition Institute, shall ensure that contracting officers and the individuals preparing descriptions of the Government requirements and statements of work have adequate training in information security requirements, including in information technology security contracts.'';

(C) in subsection (j), by adding at the end the following: ''The Director shall review and report on possible impediments in the acquisition process or elsewhere that are acting to slow agency uptake of the newest, most secure technologies.''; and

(D) by adding at the end the following:

''(l) MULTIPLE AWARD SCHEDULE FOR INFORMATION SECURITY.—The Administrator of General Services shall develop a special item number under Schedule 70 for information security products and services and consolidate those products and services under that special item number to promote acquisition.

"(m) REDUCING THE USE OF COUNTERFEIT PRODUCTS.—Not later than 180 days after the date of enactment of the Cybersecurity Act of 2012, the Director shall issue guidance requiring, to the extent practicable, Federal agencies to purchase information technology products only through the authorized channels or distributors of a supplier."; and

(2) in section 11312(b)(3), by inserting ", information security improvement," after "risk-adjusted return on investment".

TITLE VI—INTERNATIONAL COOPERATION

SEC. 601. DEFINITIONS.

In this title:

(1) COMPUTER SYSTEM; COMPUTER DATA.—The terms "computer system" and "computer data" have the meanings given those terms in chapter I of the Convention on Cybercrime.

(2) CONVENTION ON CYBERCRIME.—The term "Convention on Cybercrime" means the Council of Europe's Convention on Cybercrime, done at Budapest November 23, 2001 as ratified by the United States Senate on August 3, 2006 (Treaty 108–11) with any relevant reservations of declarations.

(3) CYBER ISSUES.—The term ''cyber issues'' means the full range of international policies designed to ensure an open, interoperable, secure, and reliable global information and communications infrastructure.

(4) CYBERCRIME.—The term ''cybercrime'' refers to criminal offenses relating to computer systems of computer data described in the Convention of Cybercrime.

(5) RELEVANT FEDERAL AGENCIES.—The term ''relevant Federal agencies'' means any Federal agency that has responsibility for combating cybercrime globally, including the Department of Commerce, the Department of Homeland Security, the Department of Justice, the Department of State, the Department of the Treasury, and the Office of the United States Trade Representative.

SEC. 602. FINDINGS.

Congress finds the following:

(1) On February 2, 2010, Admiral Dennis C. Blair, the Director of National Intelligence, testified before the Select Committee on Intelligence of the Senate regarding the Annual Threat Assessment of the U.S. Intelligence Community, stating ''The national security of the United States, our economic

prosperity, and the daily functioning of our government are dependent on a dynamic public and private information infrastructure, which includes tele-communications, computer networks and systems, and the information residing within. This critical infrastructure is severely threatened. . . . We cannot protect cyberspace without a coordinated and collaborative effort that incorporates both the US private sector and our international partners.''

(2) In a January 2010 speech on Internet freedom, Secretary of State Hillary Clinton stated: ''Those who disrupt the free flow of information in our society, or any other, pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyber attacks should face consequences and international condemnation. In an Internet-connected world, an attack on one nation's networks can be an attack on all. And by reinforcing that message, we can create norms of behavior among states and encourage respect for the global networked commons.''

(3) November 2011 marked the tenth anniversary of the Convention on Cybercrime, the only multilateral agreement on cybercrime, to which the Sen-

ate provided advice and consent on August 3, 2006, and is currently ratified by over 30 countries.

(4) The May 2009 White House Cyberspace Policy Review asserts ''[t]he Nation also needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force. International norms are critical to establishing a secure and thriving digital infrastructure.''

SEC. 603. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) engagement with other countries to advance the cyberspace objectives of the United States should be an integral part of the conduct of United States foreign relations and diplomacy;

(2) the cyberspace objectives of the United States include the full range of cyber issues, including issues related to governance, standards, cybersecurity, cybercrime, international security, human rights, and the free flow of information;

(3) it is in the interest of the United States to work with other countries to build consensus on principles and standards of conduct that protect

computer systems and users that rely on them, prevent and punish acts of cybercrime, and promote the free flow of information;

(4) a comprehensive national cyberspace strategy must include tools for addressing threats to computer systems and acts of cybercrime from sources and by persons outside the United States;

(5) developing effective solutions to international cyberspace threats requires engagement with foreign countries on a bilateral basis and through relevant regional and multilateral fora;

(6) it is in the interest of the United States to encourage the development of effective frameworks for international cooperation to combat cyberthreats, and the development of foreign government capabilities to combat cyberthreats; and

(7) the Secretary of State, in consultation with other relevant Federal agencies, should develop and lead Federal Government efforts to engage with other countries to advance the cyberspace objectives of the United States, including efforts to bolster an international framework of cyber norms, governance and deterrence.

SEC. 604. COORDINATION OF INTERNATIONAL CYBER ISSUES WITHIN THE UNITED STATES GOVERNMENT.

The Secretary of State is authorized to designate a senior level official at the Department of State, to carry out the Secretary's responsibilities to—

(1) coordinate the United States global diplomatic engagement on the full range of international cyber issues, including building multilateral cooperation and developing international norms, common policies, and responses to secure the integrity of cyberspace;

(2) provide strategic direction and coordination for United States Government policy and programs aimed at addressing and responding to cyber issues overseas, especially in relation to issues that affect United States foreign policy and related national security concerns;

(3) coordinate with relevant Federal agencies, including the Department, the Department of Defense, the Department of the Treasury, the Department of Justice, the Department of Commerce, and the intelligence community to develop interagency plans regarding international cyberspace, cybersecurity, and cybercrime issues; and

(4) ensure that cyber issues, including cybersecurity and cybercrime, are included in the responsibilities of overseas Embassies and consulates of the United States, as appropriate.

SEC. 605. CONSIDERATION OF CYBERCRIME IN FOREIGN POLICY AND FOREIGN ASSISTANCE PROGRAMS.

(a) BRIEFING.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary of State, after consultation with the heads of the relevant Federal agencies, shall provide a comprehensive briefing to relevant congressional committees—

(A) assessing global issues, trends, and actors considered to be significant with respect to cybercrime;

(B) assessing, after consultation with private industry groups, civil society organizations, and other relevant domestic or multilateral organizations, which shall be selected by the President based on an interest in combating cybercrime, means of enhancing multilateral or bilateral efforts in areas of significance—

(i) to prevent and investigate cybercrime;

(ii) to develop and share best practices with respect to directly or indirectly combating cybercrime; and

(iii) to cooperate and take action with respect to the prevention, investigation, and prosecution of cybercrime; and

(C) describing the steps taken by the United States to promote the multilateral or bilateral efforts described in subparagraph (B).

(2) CONTRIBUTIONS FROM RELEVANT FEDERAL AGENCIES.—Not later than 30 days before the date on which the briefing is to be provided under paragraph (1), the head of each relevant Federal agency shall consult with and provide to the Secretary of State relevant information appropriate for the briefing.

(b) PERIODIC UPDATES.—The Secretary of State shall provide updated information highlighting significant developments relating to the issues described in subsection (a), through periodic briefings to Congress.

(c) USE OF FOREIGN ASSISTANCE PROGRAMS.—

(1) FOREIGN ASSISTANCE PROGRAMS TO COMBAT CYBERCRIME.—The Secretary of State is authorized to accord priority in foreign assistance to programs designed to combat cybercrime in a region

or program of significance in order to better combat cybercrime by, among other things, improving the effectiveness and capacity of the legal and judicial systems and the capabilities of law enforcement agencies with respect to cybercrime.

(2) SENSE OF THE CONGRESS WITH RESPECT TO BILATERAL AND MULTILATERAL ASSISTANCE.—It is the sense of Congress that the Secretary of State should include programs designed to combat cybercrime in relevant bilateral or multilateral assistance programs administered or supported by the United States Government.

TITLE VII—INFORMATION SHARING

SEC. 701. AFFIRMATIVE AUTHORITY TO MONITOR AND DEFEND AGAINST CYBERSECURITY THREATS.

(a) IN GENERAL.—Notwithstanding chapter 119, 121, or 206 of title 18, United States Code, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and sections 222 and 705 of the Communications Act of 1934 (47 U.S.C. 222 and 605), any private entity may—

(1) monitor its information systems and information that is stored on, processed by, or transiting such information systems for—

(A) malicious reconnaissance;

(B) efforts to defeat a technical control or an operational control;

(C) technical vulnerabilities;

(D) efforts to cause a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a technical control or an operational control;

(E) malicious cyber command and control;

(F) information exfiltrated as a result of defeating a technical control or an operational control;

(G) any other attribute of a cybersecurity threat, if monitoring for such attribute is not otherwise prohibited by law; or

(H) any combination of subparagraphs (A) through (G);

(2) operate countermeasures on its information systems to protect its rights or property from cybersecurity threats;

(3) consent to another private entity monitoring or operating countermeasures on its information systems and information that is stored on, processed

by, or transiting such information systems in accordance with this section;

(4) monitor a third party's information systems and information that is stored on, processed by, or transiting such information systems for the information listed in subparagraphs (A) through (H) of paragraph (1), if—

(A) the third party provides express prior consent to such monitoring; and

(B) such monitoring would be lawful under paragraph (1) or under any other provision of law if the third party were to perform such monitoring of its own networks; and

(5) operate countermeasures on a third party's information systems to protect the third party's rights or property from cybersecurity threats, if—

(A) the third party provides express prior consent to such countermeasures; and

(B) operating such countermeasures would be lawful under paragraph (2) or under any other provision of law if the third party were to operate such countermeasures on its own information systems to protect its own rights or property.

(b) USE AND PROTECTION OF INFORMATION.—A private entity performing monitoring or operating countermeasures under subsection (a)—

(1) may use cybersecurity threat indicators acquired under this title, provided such use is solely for the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from cybersecurity threats or mitigating such threats;

(2) shall make reasonable efforts to safeguard communications, records, system traffic, or other information that may be used to identify specific persons acquired in the course of such monitoring from unauthorized access or acquisition;

(3) shall comply with any lawful restrictions placed on the use of cybersecurity threat indicators, including, if requested, the removal or destruction of information that can be used to identify specific persons from such indicators;

(4) may not use cybersecurity threat indicators to gain an unfair competitive advantage to the detriment of the entity that authorized such monitoring or operation of countermeasures; and

(5) may use information obtained under any other provision of law.

SEC. 702. VOLUNTARY DISCLOSURE OF CYBERSECURITY THREAT INDICATORS AMONG PRIVATE ENTITIES.

(a) AUTHORITY TO DISCLOSE.—Notwithstanding any other provision of law, any private entity may disclose lawfully obtained cybersecurity threat indicators to any other private entity in accordance with this section.

(b) USE AND PROTECTION OF INFORMATION.—A private entity disclosing or receiving cybersecurity threat indicators pursuant to subsection (a)—

(1) may use, retain, or further disclose such cybersecurity threat indicators solely for the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from cybersecurity threats or mitigating such threats;

(2) shall make reasonable efforts to safeguard communications, records, system traffic, or other information that can be used to identify specific persons from unauthorized access or acquisition;

(3) shall comply with any lawful restrictions placed on the disclosure or use of cybersecurity threat indicators, including, if requested, the removal of information that may be used to identify specific persons from such indicators; and

(4) may not use the cybersecurity threat indicators to gain an unfair competitive advantage to the detriment of the entity that authorized such sharing.

(c) TRANSFERS TO UNRELIABLE PRIVATE ENTITIES PROHIBITED.—A private entity may not disclose cybersecurity threat indicators to another private entity that the disclosing entity knows—

(1) has intentionally or willfully violated the requirements of subsection (b); and

(2) is reasonably likely to violate such requirements.

SEC. 703. CYBERSECURITY EXCHANGES.

(a) DESIGNATION OF CYBERSECURITY EXCHANGES.—The Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall establish—

(1) a process for designating one or more appropriate civilian Federal entities or non-Federal entities to serve as cybersecurity exchanges to receive and distribute cybersecurity threat indicators;

(2) procedures to facilitate and ensure the sharing of classified and unclassified cybersecurity threat indicators in as close to real time as possible with

appropriate Federal entities and non-Federal entities in accordance with this title; and

(3) a process for identifying certified entities to receive classified cybersecurity threat indicators in accordance with paragraph (2).

(b) PURPOSE.—The purpose of a cybersecurity exchange is to receive and distribute, in as close to real time as possible, cybersecurity threat indicators, and to thereby avoid unnecessary and duplicative Federal bureaucracy for information sharing as provided in this title.

(c) REQUIREMENT FOR A LEAD FEDERAL CIVILIAN CYBERSECURITY EXCHANGE.—

(1) IN GENERAL.—The Secretary, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall designate a civilian Federal entity as the lead cybersecurity exchange to serve as a focal point within the Federal Government for cybersecurity information sharing among Federal entities and with non-Federal entities.

(2) RESPONSIBILITIES.—The lead Federal civilian cybersecurity exchange designated under paragraph (1) shall—

(A) receive and distribute, in as close to real time as possible, cybersecurity threat indicators in accordance with this title;

(B) facilitate information sharing, interaction, and collaboration among and between—

(i) Federal entities;

(ii) State, local, tribal, and territorial governments;

(iii) private entities;

(iv) academia;

(v) international partners, in consultation with the Secretary of State; and

(vi) other cybersecurity exchanges;

(C) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information lawfully obtained from any source, including alerts, advisories, indicators, signatures, and mitigation and response measures, to appropriate Federal and non-Federal entities in as close to real time as possible, to improve the security and protection of information systems;

(D) coordinate with other Federal and non-Federal entities, as appropriate, to integrate information from Federal and non-Fed-

eral entities, including Federal cybersecurity centers, non-Federal network or security operation centers, other cybersecurity exchanges, and non-Federal entities that disclose cybersecurity threat indicators under section 704(a), in as close to real time as possible, to provide situational awareness of the United States information security posture and foster information security collaboration among information system owners and operators;

(E) conduct, in consultation with private entities and relevant Federal and other governmental entities, regular assessments of existing and proposed information sharing models to eliminate bureaucratic obstacles to information sharing and identify best practices for such sharing; and

(F) coordinate with other Federal entities, as appropriate, to compile and analyze information about risks and incidents that threaten information systems, including information voluntarily submitted in accordance with section 704(a) or otherwise in accordance with applicable laws.

(3) SCHEDULE FOR DESIGNATION.—The designation of a lead Federal civilian cybersecurity exchange under paragraph (1) shall be made concurrently with the issuance of the interim policies and procedures under section 704(g)(3)(D).

(d) ADDITIONAL CIVILIAN FEDERAL CYBERSECURITY EXCHANGES.—In accordance with the process and procedures established in subsection (a), the Secretary, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, may designate additional civilian Federal entities to receive and distribute cybersecurity threat indicators, if such entities are subject to the requirements for use, retention, and disclosure of information by a cybersecurity exchange under section 704(b) and the special requirements for Federal entities under section 704(g).

(e) REQUIREMENTS FOR NON-FEDERAL CYBERSECURITY EXCHANGES.—

(1) IN GENERAL.—In considering whether to designate a private entity or any other non-Federal entity as a cybersecurity exchange to receive and distribute cybersecurity threat indicators under section 704, and what entity to designate, the Secretary shall consider the following factors:

(A) The net effect that such designation would have on the overall cybersecurity of the United States.

(B) Whether such designation could substantially improve such overall cybersecurity by serving as a hub for receiving and sharing cybersecurity threat indicators in as close to real time as possible, including the capacity of the non-Federal entity for performing those functions.

(C) The capacity of such non-Federal entity to safeguard cybersecurity threat indicators from unauthorized disclosure and use.

(D) The adequacy of the policies and procedures of such non-Federal entity to protect personally identifiable information from unauthorized disclosure and use.

(E) The ability of the non-Federal entity to sustain operations using entirely non-Federal sources of funding.

(2) REGULATIONS.—The Secretary may promulgate regulations as may be necessary to carry out this subsection.

(f) CONSTRUCTION WITH OTHER AUTHORITIES.—Nothing in this section may be construed to alter the au-

thorities of a Federal cybersecurity center, unless such cybersecurity center is acting in its capacity as a designated cybersecurity exchange.

(g) CONGRESSIONAL NOTIFICATION OF DESIGNATION OF CYBERSECURITY EXCHANGES.—

(1) IN GENERAL.—The Secretary, in coordination with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall promptly notify Congress, in writing, of any designation of a cybersecurity exchange under this title.

(2) REQUIREMENT.—Written notification under paragraph (1) shall include a description of the criteria and processes used to make the designation.

SEC. 704. VOLUNTARY DISCLOSURE OF CYBERSECURITY THREAT INDICATORS TO A CYBERSECURITY EXCHANGE.

(a) AUTHORITY TO DISCLOSE.—Notwithstanding any other provision of law, a non-Federal entity may disclose lawfully obtained cybersecurity threat indicators to a cybersecurity exchange in accordance with this section.

(b) USE, RETENTION, AND DISCLOSURE OF INFORMATION BY A CYBERSECURITY EXCHANGE.—A cybersecurity exchange may only use, retain, or further disclose information provided pursuant to subsection (a)—

(1) in order to protect information systems from cybersecurity threats and to mitigate cybersecurity threats; or

(2) to law enforcement pursuant to subsection (g)(2).

(c) USE AND PROTECTION OF INFORMATION RECEIVED FROM A CYBERSECURITY EXCHANGE.—A non-Federal entity receiving cybersecurity threat indicators from a cybersecurity exchange—

(1) may use, retain, or further disclose such cybersecurity threat indicators solely for the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from cybersecurity threats or mitigating such threats;

(2) shall make reasonable efforts to safeguard communications, records, system traffic, or other information that can be used to identify specific persons from unauthorized access or acquisition;

(3) shall comply with any lawful restrictions placed on the disclosure or use of cybersecurity threat indicators by the cybersecurity exchange or a third party, if the cybersecurity exchange received such information from the third party, including, if requested, the removal of information that can be

used to identify specific persons from such indicators; and

(4) may not use the cybersecurity threat indicators to gain an unfair competitive advantage to the detriment of the third party that authorized such sharing.

(d) EXEMPTION FROM PUBLIC DISCLOSURE.—Any cybersecurity threat indicator disclosed by a non-Federal entity to a cybersecurity exchange pursuant to subsection (a) shall be—

(1) exempt from disclosure under section 552(b)(3) of title 5, United States Code, or any comparable State law; and

(2) treated as voluntarily shared information under section 552 of title 5, United States Code, or any comparable State law.

(e) EXEMPTION FROM EX PARTE LIMITATIONS.—Any cybersecurity threat indicator disclosed by a non-Federal entity to a cybersecurity exchange pursuant to subsection (a) shall not be subject to the rules of any governmental entity or judicial doctrine regarding ex parte communications with a decision making official.

(f) EXEMPTION FROM WAIVER OF PRIVILEGE.—Any cybersecurity threat indicator disclosed by a non-Federal entity to a cybersecurity exchange pursuant to subsection

(a) may not be construed to be a waiver of any applicable privilege or protection provided under Federal, State, tribal, or territorial law, including any trade secret protection.

(g) SPECIAL REQUIREMENTS FOR FEDERAL AND LAW ENFORCEMENT ENTITIES.—

(1) RECEIPT, DISCLOSURE AND USE OF CYBERSECURITY THREAT INDICATORS BY A FEDERAL ENTITY.—

(A) AUTHORITY TO RECEIVE AND USE CYBERSECURITY THREAT INDICATORS.—A Federal entity that is not a cybersecurity exchange may receive, retain, and use cybersecurity threat indicators from a cybersecurity exchange in order—

(i) to protect information systems from cybersecurity threats and to mitigate cybersecurity threats; and

(ii) to disclose such cybersecurity threat indicators to law enforcement in accordance with paragraph (2).

(B) AUTHORITY TO DISCLOSE CYBERSECURITY THREAT INDICATORS.—A Federal entity that is not a cybersecurity exchange shall ensure that if disclosing cybersecurity threat indicators to a non-Federal entity under this sec-

tion, such non-Federal entity shall use or retain such cybersecurity threat indicators in a manner that is consistent with the requirements in—

(i) subsection (b) on the use and protection of information; and

(ii) paragraph (2).

(2) LAW ENFORCEMENT ACCESS AND USE OF CYBERSECURITY THREAT INDICATORS.—

(A) DISCLOSURE TO LAW ENFORCEMENT.—A Federal entity may disclose cybersecurity threat indicators received under this title to a law enforcement entity if—

(i) the disclosure is permitted under the procedures developed by the Secretary and approved by the Attorney General under paragraph (3); and

(ii) the information appears to pertain—

(I) to a cybersecurity crime which has been, is being, or is about to be committed;

(II) to an imminent threat of death or serious bodily harm; or

(III) to a serious threat to minors, including sexual exploitation and threats to physical safety.

(B) USE BY LAW ENFORCEMENT.—A law enforcement entity may only use cybersecurity threat indicators received by a Federal entity under paragraph (A) in order—

(i) to protect information systems from a cybersecurity threat or investigate, prosecute, or disrupt a cybersecurity crime;

(ii) to protect individuals from an imminent threat of death or serious bodily harm; or

(iii) to protect minors from any serious threat, including sexual exploitation and threats to physical safety.

(3) PRIVACY AND CIVIL LIBERTIES.—

(A) REQUIREMENT FOR POLICIES AND PROCEDURES.—The Secretary, in consultation with privacy and civil liberties experts, the Director of National Intelligence, and the Secretary of Defense, shall develop and periodically review policies and procedures governing the receipt, retention, use, and disclosure of cybersecurity threat indicators by a Federal entity ob-

tained in connection with activities authorized in this title. Such policies and procedures shall—

(i) minimize the impact on privacy and civil liberties, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats;

(ii) reasonably limit the receipt, retention, use and disclosure of cybersecurity threat indicators associated with specific persons consistent with the need to carry out the responsibilities of this title, including establishing a process for the timely destruction of cybersecurity threat indicators that are received pursuant to this section that do not reasonably appear to be related to the purposes identified in paragraph (1)(A);

(iii) include requirements to safeguard cybersecurity threat indicators that may be used to identify specific persons from unauthorized access or acquisition;

(iv) include procedures for notifying entities, as appropriate, if information re-

ceived pursuant to this section is not a cybersecurity threat indicator; and

(v) protect the confidentiality of cybersecurity threat indicators associated with specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for the purposes identified in paragraph (1)(A).

(B) ADOPTION OF POLICIES AND PROCEDURES.—The head of an agency responsible for a Federal entity designated as a cybersecurity exchange under section 703 shall adopt and comply with the policies and procedures developed under this paragraph.

(C) REVIEW BY THE ATTORNEY GENERAL.—The policies and procedures developed under this subsection shall be provided to the Attorney General for review not later than 1 year after the date of the enactment of this title, and shall not be issued without the Attorney General's approval.

(D) REQUIREMENT FOR INTERIM POLICIES AND PROCEDURES.—The Secretary shall issue interim policies and procedures not later than

60 days after the date of the enactment of this title.

(E) PROVISION TO CONGRESS.—The policies and procedures issued under this title and any amendments to such policies and procedures shall be provided to Congress in an unclassified form and be made public, but may include a classified annex.

(4) OVERSIGHT.—

(A) REQUIREMENT FOR OVERSIGHT.—The Secretary and the Attorney General shall establish a mandatory program to monitor and oversee compliance with the policies and procedures issued under this subsection.

(B) NOTIFICATION OF THE ATTORNEY GENERAL.—The head of each Federal entity that receives information under this title shall—

(i) comply with the policies and procedures developed by the Secretary and approved by the Attorney General under paragraph (3);

(ii) promptly notify the Attorney General of significant violations of such policies and procedures; and

(iii) provide to the Attorney General any information relevant to the violation that the Attorney General requires.

(C) ANNUAL REPORT.—On an annual basis, the Chief Privacy and Civil Liberties Officer of the Department of Justice and the Chief Privacy Officer of the Department, in consultation with the most senior privacy and civil liberties officer or officers of any appropriate agencies, shall jointly submit to Congress a report assessing the privacy and civil liberties impact of the governmental activities conducted pursuant to this title.

(5) REPORTS ON INFORMATION SHARING.—

(A) PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD REPORT.—Not later than 2 years after the date of the enactment of this title, and every 2 years thereafter, the Privacy and Civil Liberties Oversight Board shall submit to Congress and the President a report providing—

(i) an analysis of the practices of private entities that are performing, monitoring, operating countermeasures, or disclosing cybersecurity threat indicators pursuant to this title;

(ii) an assessment of the privacy and civil liberties impact of the activities carried out by the Federal entities under this title; and

(iii) recommendations for improvements to or modifications of the law and the policies and procedures established pursuant to paragraph (3) in order to address privacy and civil liberties concerns.

(B) INSPECTORS GENERAL ANNUAL REPORT.—The Inspector General of the Department, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, and the Inspector General of the Department of Defense shall, on an annual basis, jointly submit to Congress a report on the receipt, use and disclosure of information shared with a Federal cybersecurity exchange under this title, including—

(i) a review of the use by Federal entities of such information for a purpose other than to protect information systems from cybersecurity threats and to mitigate cybersecurity threats, including law en-

1 forcement access and use pursuant to
2 paragraph (2);
3 (ii) a review of the type of information
4 shared with a Federal cybersecurity ex-
5 change;
6 (iii) a review of the actions taken by
7 Federal entities based on such information;
8 (iv) appropriate metrics to determine
9 the impact of the sharing of such informa-
10 tion with a Federal cybersecurity exchange
11 on privacy and civil liberties;
12 (v) a list of Federal entities receiving
13 such information;
14 (vi) a review of the sharing of such in-
15 formation among Federal entities to iden-
16 tify inappropriate stovepiping of shared in-
17 formation; and
18 (vii) any recommendations of the in-
19 spectors general for improvements or modi-
20 fications to the authorities under this title.
21 (C) FORM.—Each report required under
22 this paragraph shall be submitted in unclassi-
23 fied form, but may include a classified annex.
24 (6) SANCTIONS.—The head of each Federal en-
25 tity that conducts activities under this title shall de-

velop and enforce appropriate sanctions for officers, employees, or agents of such entities who conducts such activities—

(A) outside the normal course of their specified duties;

(B) in a manner inconsistent with the discharge of the responsibilities of such entity; or

(C) in contravention of the requirements, policies, and procedures required by this subsection.

(7) FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF THIS TITLE.—

(A) IN GENERAL.—If a Federal entity intentionally or willfully violates a provision of this title or a regulation promulgated under this title, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—

(i) the actual damages sustained by the person as a result of the violation or $1,000, whichever is greater; and

(ii) the costs of the action together with reasonable attorney fees as determined by the court.

(B) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

(i) the district in which the complainant resides;

(ii) the district in which the principal place of business of the complainant is located;

(iii) the district in which the Federal entity that disclosed the information is located; or

(iv) the District of Columbia.

(C) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than 2 years after the date of the violation that is the basis for the action.

(D) EXCLUSIVE CAUSE OF ACTION.—A cause of action under this subsection shall be the exclusive means available to a complainant seeking a remedy for a disclosure of information in violation of this title by a Federal entity.

SEC. 705. SHARING OF CLASSIFIED CYBERSECURITY THREAT INDICATORS.

(a) SHARING OF CLASSIFIED CYBERSECURITY THREAT INDICATORS.—The procedures established under section 703(a)(2) shall provide that classified cybersecurity threat indicators may only be—

(1) shared with certified entities;

(2) shared in a manner that is consistent with the need to protect the national security of the United States;

(3) shared with a person with an appropriate security clearance to receive such cybersecurity threat indicators; and

(4) used by a certified entity in a manner that protects such cybersecurity threat indicators from unauthorized disclosure.

(b) REQUIREMENT FOR GUIDELINES.—Not later than 60 days after the date of the enactment of this title, the Director of National Intelligence shall issue guidelines providing that appropriate Federal officials may, as the Director considers necessary to carry out this title—

(1) grant a security clearance on a temporary or permanent basis to an employee of a certified entity;

(2) grant a security clearance on a temporary or permanent basis to a certified entity and approval to use appropriate facilities; or

(3) expedite the security clearance process for such an employee or entity, if appropriate, in a manner consistent with the need to protect the national security of the United States.

(c) DISTRIBUTION OF PROCEDURES AND GUIDELINES.—Following the establishment of the procedures under section 703(a)(2) and the issuance of the guidelines under subsection (b), the Secretary and the Director of National Intelligence shall expeditiously distribute such procedures and guidelines to—

(1) appropriate governmental entities and private entities;

(2) the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, and the Select Committee on Intelligence of the Senate; and

(3) the Committee on Armed Services, the Committee on Energy and Commerce, the Committee on Homeland Security, the Committee on the

Judiciary, and the Permanent Select Committee on Intelligence of the House of Representatives.

SEC. 706. LIMITATION ON LIABILITY AND GOOD FAITH DEFENSE FOR CYBERSECURITY ACTIVITIES.

(a) IN GENERAL.—No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any entity acting as authorized by this title, and any such action shall be dismissed promptly for activities authorized by this title consisting of—

(1) the cybersecurity monitoring activities authorized by paragraph (1), (3) or (4) of section 701(a); or

(2) the voluntary disclosure of a lawfully obtained cybersecurity threat indicator—

(A) to a cybersecurity exchange pursuant to section 704(a);

(B) by a provider of cybersecurity services to a customer of that provider;

(C) to a private entity or governmental entity that provides or manages critical infrastructure (as that term is used in section 1016 of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c)); or

(D) to any other private entity under section 702(a), if the cybersecurity threat indicator

is also disclosed within a reasonable time to a cybersecurity exchange.

(b) GOOD FAITH DEFENSE.—If a civil or criminal cause of action is not barred under subsection (a), a reasonable good faith reliance that this title permitted the conduct complained of is a complete defense against any civil or criminal action brought under this title or any other law.

(c) LIMITATION ON USE OF CYBERSECURITY THREAT INDICATORS FOR REGULATORY ENFORCEMENT ACTIONS.—No Federal entity may use a cybersecurity threat indicator received pursuant to this title as evidence in a regulatory enforcement action against the entity that lawfully shared the cybersecurity threat indicator with a cybersecurity exchange that is a Federal entity.

(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT, NATIONAL SECURITY, OR HOMELAND SECURITY PURPOSES.—No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any entity, and any such action shall be dismissed promptly, for a failure to disclose a cybersecurity threat indicator if—

(1) the Attorney General or the Secretary determines that disclosure of a cybersecurity threat indicator would impede a civil or criminal investigation

and submits a written request to delay notification for up to 30 days, except that the Attorney General or the Secretary may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary; or

(2) the Secretary, the Attorney General, or the Director of National Intelligence determines that disclosure of a cybersecurity threat indicator would threaten national or homeland security and submits a written request to delay notification, except that the Secretary, the Attorney General, or the Director, may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary.

(e) LIMITATION ON LIABILITY FOR FAILURE TO ACT.—No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any private entity, or any officer, employee, or agent of such an entity, and any such action shall be dismissed promptly, for the reasonable failure to act on information received under this title.

(f) DEFENSE FOR BREACH OF CONTRACT.—Compliance with lawful restrictions placed on the disclosure or

use of cybersecurity threat indicators is a complete defense to any tort or breach of contract claim originating in a failure to disclose cybersecurity threat indicators to a third party.

(g) LIMITATION ON LIABILITY PROTECTIONS.—Any person who, knowingly or acting in gross negligence, violates a provision of this title or a regulation promulgated under this title shall—

(1) not receive the protections of this title; and

(2) be subject to any criminal or civil cause of action that may arise under any other State or Federal law prohibiting the conduct in question.

SEC. 707. CONSTRUCTION AND FEDERAL PREEMPTION.

(a) CONSTRUCTION.—Nothing in this title may be construed—

(1) to limit any other existing authority or lawful requirement to monitor information systems and information that is stored on, processed by, or transiting such information systems, operate countermeasures, and retain, use or disclose lawfully obtained information;

(2) to permit the unauthorized disclosure of—

(A) information that has been determined by the Federal Government pursuant to an Executive order or statute to require protection

against unauthorized disclosure for reasons of national defense or foreign relations;

(B) any restricted data (as that term is defined in paragraph (y) of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014));

(C) information related to intelligence sources and methods; or

(D) information that is specifically subject to a court order or a certification, directive, or other authorization by the Attorney General precluding such disclosure;

(3) to provide additional authority to, or modify an existing authority of, the Department of Defense or the National Security Agency or any other element of the intelligence community to control, modify, require, or otherwise direct the cybersecurity efforts of a non-Federal entity or a Federal entity;

(4) to limit or modify an existing information sharing relationship;

(5) to prohibit a new information sharing relationship;

(6) to require a new information sharing relationship between a Federal entity and a private entity;

(7) to limit the ability of a non-Federal entity or a Federal entity to receive data about its information systems, including lawfully obtained cybersecurity threat indicators;

(8) to authorize or prohibit any law enforcement, homeland security, or intelligence activities not otherwise authorized or prohibited under another provision of law;

(9) to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning;

(10) to authorize or limit liability for actions that would violate the regulations adopted by the Federal Communications Commission on preserving the open Internet, or any successor regulations thereto, nor to modify or alter the obligations of private entities under such regulations; or

(11) to prevent a governmental entity from using information not acquired through a cybersecurity exchange for regulatory purposes.

(b) FEDERAL PREEMPTION.—This title supersedes any law or requirement of a State or political subdivision of a State that restricts or otherwise expressly regulates

the provision of cybersecurity services or the acquisition, interception, retention, use or disclosure of communications, records, or other information by private entities to the extent such law contains requirements inconsistent with this title.

(c) PRESERVATION OF OTHER STATE LAW.—Except as expressly provided, nothing in this title shall be construed to preempt the applicability of any other State law or requirement.

(d) NO CREATION OF A RIGHT TO INFORMATION.—The provision of information to a non-Federal entity under this title does not create a right or benefit to similar information by any other non-Federal entity.

(e) PROHIBITION ON REQUIREMENT TO PROVIDE INFORMATION TO THE FEDERAL GOVERNMENT.—Nothing in this title may be construed to permit a Federal entity—

(1) to require a non-Federal entity to share information with the Federal Government;

(2) to condition the disclosure of unclassified or classified cybersecurity threat indicators pursuant to this title with a non-Federal entity on the provision of cybersecurity threat information to the Federal Government; or

(3) to condition the award of any Federal grant, contract or purchase on the provision of cy-

bersecurity threat indicators to a Federal entity, if the provision of such indicators does not reasonably relate to the nature of activities, goods, or services covered by the award.

(f) LIMITATION ON USE OF INFORMATION.—No cybersecurity threat indicators obtained pursuant to this title may be used, retained, or disclosed by a Federal entity or non-Federal entity, except as authorized under this title.

(g) DECLASSIFICATION AND SHARING OF INFORMATION.—Consistent with the exemptions from public disclosure of section 704(d), the Director of National Intelligence, in consultation with the Secretary and the head of the Federal entity in possession of the information, shall facilitate the declassification and sharing of information in the possession of a Federal entity that is related to cybersecurity threats, as the Director deems appropriate.

(h) REPORT ON IMPLEMENTATION.—Not later than 2 years after the date of the enactment of this title, the Secretary, the Director of National Intelligence, the Attorney General, and the Secretary of Defense shall jointly submit to Congress a report that—

(1) describes the extent to which the authorities conferred by this title have enabled the Federal Gov-

ernment and the private sector to mitigate cybersecurity threats;

(2) discloses any significant acts of noncompliance by a non-Federal entity with this title, with special emphasis on privacy and civil liberties, and any measures taken by the Federal Government to uncover such noncompliance;

(3) describes in general terms the nature and quantity of information disclosed and received by governmental entities and private entities under this title; and

(4) identifies the emergence of new threats or technologies that challenge the adequacy of the law, including the definitions, authorities and requirements of this title, for keeping pace with the threat.

(i) REQUIREMENT FOR ANNUAL REPORT.—On an annual basis, the Director of National Intelligence shall provide a report to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives on the implementation of section 705. Such report, which shall be submitted in a classified and in an unclassified form, shall include a list of private entities that receive classified cybersecurity threat indicators under this title, except that the unclassified report shall not contain information that

may be used to identify specific private entities unless such private entities consent to such identification.

SEC. 708. DEFINITIONS.

In this title:

(1) CERTIFIED ENTITY.—The term ''certified entity'' means a protected entity, a self-protected entity, or a provider of cybersecurity services that—

(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and

(B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately protect and use classified cybersecurity threat indicators.

(2) COUNTERMEASURE.—The term ''countermeasure'' means automated or manual actions to modify, redirect, or block information that is stored on, processed by, or transiting an information system that is known or suspected to contain cybersecurity threat indicators for the purpose of protecting an information system from cybersecurity threats, conducted on an information system owned or operated by or on behalf of the party to be protected or operated by a private entity acting as a provider of electronic communication services, remote computing

1 services, or cybersecurity services to the party to be
2 protected.

3 (3) CYBERSECURITY CRIME.—The term ''cyber-
4 security crime'' means the violation of a provision of
5 State or Federal law relating to computer crimes, in-
6 cluding a violation of any provision of title 18,
7 United States Code, enacted or amended by the
8 Computer Fraud and Abuse Act of 1986 (Public
9 Law 99–474; 100 Stat. 1213).

10 (4) CYBERSECURITY EXCHANGE.—The term
11 ''cybersecurity exchange'' means any governmental
12 entity or private entity designated by the Secretary
13 of Homeland Security, in consultation with the Di-
14 rector of National Intelligence, the Attorney Gen-
15 eral, and the Secretary of Defense, to receive and
16 distribute cybersecurity threat indicators under sec-
17 tion 703(a).

18 (5) CYBERSECURITY SERVICES.—The term ''cy-
19 bersecurity services'' means products, goods, or serv-
20 ices intended to detect, mitigate, or prevent cybersec-
21 urity threats.

22 (6) CYBERSECURITY THREAT.—The term ''cy-
23 bersecurity threat'' means any action that may re-
24 sult in unauthorized access to, exfiltration of, manip-
25 ulation of, harm of, or impairment to the integrity,

confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system, except that none of the following shall be considered a cybersecurity threat—

(A) actions protected by the first amendment to the Constitution of the United States; and

(B) exceeding authorized access of an information system, if such access solely involves a violation of consumer terms of service or consumer licensing agreements.

(7) CYBERSECURITY THREAT INDICATOR.—The term ''cybersecurity threat indicator'' means information—

(A) that is reasonably necessary to describe—

(i) malicious reconnaissance, including anomalous patterns of communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(ii) a method of defeating a technical control;

(iii) a technical vulnerability;

(iv) a method of defeating an operational control;

(v) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a technical control or an operational control;

(vi) malicious cyber command and control;

(vii) the actual or potential harm caused by an incident, including information exfiltrated as a result of defeating a technical control or an operational control when it is necessary in order to identify or describe a cybersecurity threat;

(viii) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(ix) any combination thereof; and

(B) from which reasonable efforts have been made to remove information that can be used to identify specific persons unrelated to the cybersecurity threat.

(8) FEDERAL CYBERSECURITY CENTER.—The term ''Federal cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the United States Computer Emergency Readiness Team, or successors to such centers.

(9) FEDERAL ENTITY.—The term ''Federal entity'' means an agency or department of the United States, or any component, officer, employee, or agent of such an agency or department.

(10) GOVERNMENTAL ENTITY.—The term ''governmental entity'' means any Federal entity and agency or department of a State, local, tribal, or territorial government other than an educational institution, or any component, officer, employee, or agent of such an agency or department.

(11) INFORMATION SYSTEM.—The term ''information system'' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, including communications with,

or commands to, specialized systems such as industrial and process control systems, telephone switching and private branch exchanges, and environmental control systems.

(12) MALICIOUS CYBER COMMAND AND CONTROL.—The term ''malicious cyber command and control'' means a method for remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system associated with a known or suspected cybersecurity threat.

(13) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(14) MONITOR.—The term ''monitor'' means the interception, acquisition, or collection of information that is stored on, processed by, or transiting an information system for the purpose of identifying cybersecurity threats.

(15) NON-FEDERAL ENTITY.—The term ''non-Federal entity'' means a private entity or a governmental entity other than a Federal entity.

(16) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(17) PRIVATE ENTITY.—The term ''private entity'' has the meaning given the term ''person'' in section 1 of title 1, United States Code, and does not include a governmental entity.

(18) PROTECT.—The term ''protect'' means actions undertaken to secure, defend, or reduce the vulnerabilities of an information system, mitigate cybersecurity threats, or otherwise enhance information security or the resiliency of information systems or assets.

(19) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(20) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(21) THIRD PARTY.—The term ''third party'' includes Federal entities and non-Federal entities.

Calendar No. 470

112th CONGRESS
2d Session

S. 3414

A BILL

To enhance the security and resiliency of the cyber and communications infrastructure of the United States.

July 23, 2012

Read the second time and placed on the calendar